

# Understanding Quantum Technologies

**Fourth edition**

Balestro  
2021

10



11

le lab quantique

cover back page

# **Understanding Quantum Technologies**

**Fourth edition**

**2021**

**Olivier Ezratty**

## About the author

Olivier Ezratty

consultant and author

[olivier \(at\) oezratty.net](mailto:olivier(at)oezratty.net), [www.oezratty.net](http://www.oezratty.net), @olivez

+33 6 67 37 92 41

Olivier Ezratty advises and trains businesses and public services in the development of their innovation strategies around deep techs and, in particular, quantum technologies. He brings them a 360° understanding of scientific, technology, marketing as well as ecosystems development.

Since 2005, he carried out various missions in different verticals such as the **media and telecoms** (Orange, Bouygues Télécom, TDF, Médiamétrie, BVA, Astra), **finance and insurance** (BPCE group, Caisse des Dépôts, Société Générale, Swiss Life, Crédit Agricole, Crédit Mutuel-CIC, Generali, MAIF), **industry and services** (Schneider, Camfil, Vinci, NTN-STR, Econocom, ADP, Air France, Airbus) and in the **public sector** (Ministry of Defense, CEA, Météo France, Bpifrance, Business France, Douanes Françaises, Inria, European Union).

His contributions are also based on a strong investment in the innovation ecosystem particularly in the entrepreneurial world:

- Quantum computing and artificial intelligence trainer at **Capgemini Institut**.
- Member of the Scientific Council of **ARCEP** (telecommunication regulator) since 2015.
- Expert and speaker at **IHEDN** in the 2019/2020 and 2020/2021 promotions.
- Expert with **Bpifrance**, particularly for quantum technologies projects due diligences.
- Started teaching quantum technologies in an elective at **EPITA** (computer science school) in 2021.

He lectures in various universities such as CentraleSupélec, Ecole des Mines de Paris, Télécom Paristech, EPITA, Les Gobelins, HEC, Neoma Rouen and SciencesPo, on quantum technologies, artificial intelligence as well as innovation and product management, in French and English as needed.

Olivier Ezratty is the author of the ebook **Understanding Quantum Technologies** (September 2021) the fourth edition of **Comprendre l'Informatique Quantique** (September 2018, 2019 and 2020), **Les usages de l'intelligence artificielle** (2017, 2018, 2019 and 2021) as well as the **CES Las Vegas Report**, that was published each January from 2006 to 2020, and the **Startup Guide**, which became a reference in France with more than 400,000 downloads, updated every year since 2016 (23rd edition and 13th year in 2019). All of this was and is still published for free on his blog "Opinions Libres" ([www.oezratty.net](http://www.oezratty.net)) which deals with technological innovation from the scientific, technological, entrepreneurial and innovation public policies.

Olivier Ezratty is also the co-initiator in 2012 of **Quelques Femmes du Numérique !** ("some digital women", [www.qfdn.net](http://www.qfdn.net)) which became an association in 2016, and aims to increase gender balance in digital professions, by raising awareness among young people about these professions. He is the portraits photographer for the initiative and developed their new site launched in April 2021.

Olivier Ezratty was a software engineer and developer. He started in 1985 at **Sogitec**, a subsidiary of the Dassault group, where he was consecutively Software Engineer, then Head of the Research Department in the Communication Division. He initialized developments under Windows 1.0 in the field of editorial computing as well as on SGML, the ancestor of HTML and XML.

Joining **Microsoft France** in 1990, he gained experience in many areas of the marketing mix. He launched the first version of Visual Basic in 1991 and Windows NT in 1993. In 1998, he became Marketing and Communication Director of Microsoft France and in 2001, Director of the Developer Division, which he created in France to launch the .NET platform and promote it to developers, higher education and research, as well as to startups.

Olivier Ezratty is a software engineer from **Centrale Paris** (1985), which became CentraleSupélec in 2015.

**This document is provided to you free of charge and is licensed under a "Creative Commons" license.**  
in the variant "Attribution-Noncommercial-No Derivative Works 2.0".



see <http://creativecommons.org/licenses/by-nc-nd/2.0/> - web site [ISSN 2680-0527](http://issn2680-0527)

## Credits

Cover illustration: personal creation associating a Bloch sphere describing a qubit and the symbol of peace (my creation, done in 2018) above a long list of over 400 scientists and entrepreneurs who are mentioned in the ebook.

A note on image credits: this document contains over 1600 illustrations. I have managed to give credits to their creators as much as possible. Most sources are credited in footnotes or in the text. Only scientists' portraits are not since it's quite hard to track it. I have added my own credit in most of the illustrations I have created. In some cases, I have redrawn some third-party illustrations to create clean vector versions or used existing third party illustrations and added my own text comments. The originals are still credited.

# Table of contents

<b>Foreword .....</b>	<b>9</b>
<b>Why.....</b>	<b>10</b>
A complex domain in search of pedagogy .....	12
A new computing wave .....	13
Summary and abstract .....	13
Reading guide.....	17
First and second quantum revolutions applications .....	19
Why quantum computing? .....	21
<b>History and scientists .....</b>	<b>29</b>
Precursors .....	32
Founders .....	38
Post-war.....	56
Quantum computing physicists .....	61
Quantum information science and algorithms creators .....	71
Research for dummies .....	78
<b>Quantum physics 101 .....</b>	<b>88</b>
Postulates.....	89
Quantization .....	92
Wave-particle duality .....	95
Superposition and entanglement .....	101
Indetermination .....	104
Measurement .....	105
No-cloning.....	106
Tunnel effect.....	107
Quantum matter and fluids.....	108
Extreme quantum .....	119
<b>Gate-based quantum computing.....</b>	<b>128</b>
In a nutshell .....	128
Linear algebra.....	130
Qubits .....	146
Bloch sphere.....	149
Registers .....	153
Gates.....	156
Inputs and outputs .....	165
Qubit lifecycle .....	167
Measurement .....	168
<b>Quantum computing engineering .....</b>	<b>179</b>
Key parameters.....	180
Quantum computers segmentation .....	183
Qubit types .....	187
Architecture overview .....	196
Processor layout .....	198
Error correction .....	200
Quantum memory.....	218
Non-linearities.....	222

Energetic cost of quantum computing.....	223
Economics .....	231
Quantum uncertainty .....	233
<b>Quantum computing hardware.....</b>	<b>239</b>
Quantum annealing .....	241
Superconducting qubits .....	252
Electron spins qubits .....	281
NV centers qubits .....	296
Topological qubits .....	301
Trapped ions qubits .....	307
Cold atoms qubits.....	323
Photons qubits .....	331
<b>Quantum enabling technologies.....</b>	<b>361</b>
Cryogenics.....	361
Cabling and filters .....	379
Qubits control and readout electronics .....	382
Thermometers.....	393
Vacuum.....	394
Lasers .....	395
Photonics .....	400
Other enabling technologies vendors .....	405
Raw materials.....	408
Alternatives to quantum computing .....	417
<b>Quantum algorithms .....</b>	<b>442</b>
Algorithms classes.....	445
Basic algorithms toolbox.....	451
Higher level algorithms .....	462
Hybrid algorithms .....	483
Quantum inspired algorithms .....	485
Complexity theories .....	485
Quantum speedups .....	495
<b>Quantum software development tools .....</b>	<b>499</b>
Development tool classes .....	500
Research-originated quantum development tools .....	508
Quantum vendors development tools.....	513
Cloud quantum computing .....	523
Certification and verification .....	525
Debugging .....	527
Benchmarking .....	528
<b>Quantum computing business applications .....</b>	<b>538</b>
Market forecasts .....	538
Healthcare.....	543
Energy and chemistry .....	549
Transportation and logistics .....	552
Telecommunications.....	555
Finance .....	556
Insurance .....	561
Marketing .....	562
Content .....	562

Defense and aerospace .....	563
Intelligence services .....	564
Industry.....	565
Science .....	565
Software and tools vendors .....	566
<b>Quantum telecommunications and cryptography.....</b>	<b>588</b>
Public key cryptography.....	589
Quantum cryptography.....	591
Quantum Random Numbers Generators .....	597
Quantum Key Distribution.....	605
Post-quantum cryptography .....	616
Quantum homomorphic cryptography .....	625
Quantum telecommunications.....	625
Quantum Physical Unclonable Functions .....	630
Quantum telecommunications and cryptography vendors .....	631
<b>Quantum sensing.....</b>	<b>644</b>
Quantum gravimeters .....	646
Quantum clocks.....	650
Quantum magnetometers.....	654
Quantum thermometers .....	658
Imaging and microscopes.....	658
Quantum radars .....	664
Quantum chemical sensors.....	666
Quantum NEMS and MEMS .....	667
Radio frequencies sensing.....	667
<b>Quantum technologies around the world.....</b>	<b>669</b>
Quantum computing startups and SMEs.....	670
Global investments .....	675
North America .....	678
Europe .....	687
Russia .....	720
Near and Middle East .....	721
Asia-Pacific .....	722
What industry strategies? .....	735
<b>Corporate adoption .....</b>	<b>737</b>
Technology screening.....	737
Customer needs analysis .....	738
Training .....	738
Evaluation.....	739
<b>Quantum technologies and society.....</b>	<b>740</b>
Human ambition.....	740
Science fiction.....	741
Quantum foundations and the philosophy of quantum physics .....	744
Ethical quantum.....	751
Religions and mysticism .....	755
Public education .....	756
Scientific education .....	757
Jobs impact.....	761
Gender balance.....	762

Quantum technologies marketing.....	765
<b>Quantum fake sciences.....</b>	<b>768</b>
Quantum biology.....	768
Quantum medicine .....	777
Quantum management.....	784
Other exaggerations.....	787
<b>Conclusion.....</b>	<b>792</b>
<b>Bibliography .....</b>	<b>794</b>
Books and ebooks.....	794
Comics.....	797
Presentations.....	798
Events .....	798
Training .....	800
Websites .....	800
Podcasts .....	800
Reports .....	801
Miscellaneous.....	801
<b>Glossary.....</b>	<b>802</b>
<b>Index .....</b>	<b>822</b>
<b>Revisions history.....</b>	<b>832</b>

# **Foreword**

Quantum technologies hold promises of major disruptions in computing, communications and sensing. But scientific and technological challenges to their large-scale deployment are still important, and it is quite difficult for public decision makers, users, investors, professionals, and the public at large to anticipate when these will happen. This is of paramount importance for companies to stay competitive, for governments to position their country in this technology race, or for students to make decisions about their career. While some quantum devices are already in use with practical impact, e.g. sophisticated microscopes taking benefit of the exquisite sensitivity of the spin of point defects in diamonds, other technologies will take years if not decades to reach the markets.

But the situation is changing fast. When I co-founded the Quantonation investment fund in 2018, most of the fund's presentation was about the promises of quantum, and about the science. Today, with 15 seed investments made in startups in Europe and North America, the situation has already radically changed since, for the most mature, we are talking about products and customers, and, at least, proofs of concepts. Consulting firms are busy assessing future markets, their size keeps increasing and the horizon is getting closer with significant practical achievements not much further down the road. I'm often asked whether there is not too much "hype" in the field. I don't think so, particularly when I am comparing quantum technologies with other sectors. This is the beginning of market recognition, for a sector which impact is slowly being assessed properly.

But to do that, make proper assessments and keep control of the quantum narrative, we need deep experts who have a proper understanding of all the facets of the technology, from the fundamentals of the science to its applications, including questions about their deployment, their funding, how to teach them, and more. It is necessary to be able to mobilize academic experts to provide an opinion on the science at the base of the innovation, on the ability to make robust products, but we must also be able to imagine their use cases, and scientists alone are not equipped to do so. There is a need for a multidisciplinary collaboration involving scientists, engineers and users capable of taking a forward-looking posture. And here enters my friend Olivier Ezratty, the author of this most wonderful book "Understanding Quantum Technologies", who embodies multidisciplinarity. He has the unique ability to listen, question, gather facts, and synthesize his learnings in a book that stands out as unique in the whole world, as far as I know.

I've met Olivier when I came back to France to start Quantonation. From the start I was impressed by his extremely methodic approach that he had applied with success on an earlier publication on artificial intelligence, and his very unique ambition. The book was first published, in French, in 2018 and then grew with the field he was "decoding" to use the title of Olivier's famous podcast with Fanny Bouton on quantum technologies. With each new edition, the page number was growing, Olivier was making the book better, adding whole new sections, researching complex scientific and technology aspects, so that, with this first edition in English, the public now has access to an outstanding reference book on quantum technologies. Olivier has also been among the very first supporters of the not-for profit that I co-founded and chaired, Le Lab Quantique. Le Lab Quantique is proud to promote "Understanding Quantum Technologies", an instrument that will benefit its ecosystem building mission.

I am convinced that this book will become a primer for professionals, from scientists to engineers, technicians, investors, and also for teachers, students, and the public at large. We're all extremely lucky to see the second quantum revolution happening before our eyes, science and technology are progressing at an amazing pace and it is essential to invent a new model of knowledge sharing, of collaboration. Olivier Ezratty's book is an indispensable instrument to read this revolution.

**Christophe Jurczak, Partner at Quantonation, Paris and co-founder, Le Lab Quantique**

# Why

This ebook is the fourth edition of a book originally compiling a series of 18 articles that I published in French between June and September 2018. A second richer edition followed in September 2019 and a third one in September 2020. This fourth edition is yet another significant update of this ebook and, above all, a shift to English to expand its readership.

It provides a 360° perspective of quantum technologies and quantum computing encompassing historical, scientific, technological, engineering, entrepreneurial, geopolitical, philosophical and societal dimensions. It also ambitions to be accessible to computer science engineers who may easily be lost with quantum physics and its underlying mathematics formalism. This book also investigates rarely covered aspects of quantum technologies and quantum engineering like various enabling technologies (cryogenics, cryo-electronics, new materials design, semiconductors, cabling and lasers), their thermodynamic and energetic dimension and what raw materials are used and where they come from. I also extensively cover quantum sensing, telecommunications and cryptography.

Compared to many specialists, I am a relative newbie in the field. I started to write short pieces on quantum computing back in 2015 and seriously began my quantum journey in 2018. This field intrigued me a lot since being very promising and, meanwhile, rather difficult to apprehend. I was puzzled by all the media covering vendor announcements without them having a real clue about what they were writing about. Google, IBM and Honeywell announcements are hard to interpret, but they did set the stage. A few years later, quantum technologies are more commonplace, but still largely misunderstood by general audiences as well as by many IT professionals. This ebook aims to fill these misunderstanding gaps.

These large vendors have elevated quantum technologies to the rank of strategic sectors for developed countries. Most governments have launched their quantum plans, starting with Singapore, the UK, China and the USA, and then Germany, Japan, Australia, Russia, Israel, Taiwan, France, The Netherlands and Italy. The worldwide quantum technologies race is on. Countries are embattled to acquire or preserve their technological sovereignty, like if it was the last chance to achieve it, particularly for those countries who felt they lost the digital battle against the USA and Asia (mostly China, South Korea and Taiwan). Also, like many deep techs, quantum technologies are dual-use ones, with both civilian and military use cases, therefore increasing the strategic stakes.

While it has not yet reached the volume and funding of other sectors such as artificial intelligence or the digital cloud, the quantum startups and SMEs ecosystem continues to expand worldwide. In this ebook, I mention over 450 such companies in many different categories (computing hardware and software, telecommunications, cryptography, sensing, enabling technologies). We are here in the deep techs realm if not in hard tech territory, with many startups still at an applied research stage with a rather low technology readiness level. Being still very uncertain, this market remains quite open to opportunities for scientists and creative innovators, while in other markets like with semiconductors and large consumer Internet players, the game looks like it is nearly over.

Quantum technologies are also surrounded by a fair share of hype. A few scientists, their laboratory's communication department, startups and large vendors frequently exaggerate the impact of their work<sup>1</sup>.

---

<sup>1</sup> See the creation of the "Quantum Bullshit Detector" Twitter account in the spring of 2019, which is used to binary identify what is bullshit and what is not. They ceased tweeting in February 2021, reporting being "*acquired by a successful quantum startup preparing for IPO*". In [Revolt! Scientists Say They're Sick of Quantum Computing's Hype](#) by Sophia Chen, December 2019. See also [Quantum Computing Hype is Bad for Science](#) by Victor Galitski, University of Maryland, July 2021.

Many companies also integrate “quantum” into their positioning if not branding in many fancy ways. Either in a totally artificial way, or based on using technologies from the first quantum revolution.

Transistors, lasers and image sensors are quantum, so most digital technologies can claim to be quantum. As a consequence, we must learn to distinguish the old (first quantum revolution related) from the new (second quantum revolution related). However, the real bullshit is elsewhere, with false science-based quantum medicine and other charlatanism. I showcase it in a section dedicated to quantum hoaxes and scams.

This book has another flavor. It is the result of an unprecedented human adventure at the heart of the quantum ecosystem. I started the journey back in 2016. I had then decided to select the theme of quantum computing for my usual techno-screening activities, ranging from preparing conferences and training to writing educational ebooks for professionals. I was joined by my friend **Fanny Bouton** to run a popularization conference on quantum computing in Nantes. She brought and still brings a different perspective, including some science fiction derived inspirations. This led to the conference **Le quantique, c'est fantastique** on June 14, 2018 ([video](#)) and to numerous subsequent presentations. On top of that, we launched two series of podcasts (in French) covering the news of quantum techs and with interviews with researchers and entrepreneurs. We also worked on gender balance and contributed as early as possible to this sector feminization and attract new talents<sup>2</sup>.

We've had the opportunity to meet with top researchers and entrepreneurs in France: **Alain Aspect**, **Philippe Grangier**, co-author of Alain Aspect's experiment and one of the founders of continuous variables quantum key distribution, **Daniel Esteve**, a pioneer of superconducting qubits at the CEA, **Patrice Bertet** who works in his laboratory, **Maud Vinet** from CEA-Leti in Grenoble and **Tristan Meunier** of the CNRS Institut Néel who drive the Grenoble silicon qubit project, **Eleni Diamanti** from CNRS LIP6, a specialist in quantum communications and coordinator with **Iordanis Kerenidis** of the Paris quantum hub, **Pascale Senellart** from CNRS C2N, a specialist in single photons generation, co-founder of Quandela, **Elham Kashefi** from CNRS LIP6, a specialist in quantum software and telecommunications and co-founder of VeriQloud, **Alexia Auffèves** from CNRS Institut Néel, a specialist in quantum thermodynamics and on the energetics of quantum technologies, **Philippe Duluc** and **Cyril Allouche** from Atos, the quantum sensing teams of **Thales** and many others afterwards. We also toured almost all quantum **startups** in France. And of course, **Christophe Jurczak** from Quantonation and Le Lab Quantique, who kindly wrote this book foreword.

Then, progressively, we expanded our reach to international researchers and entrepreneurs, particularly in Canada, the USA, the UK, Austria and The Netherlands). I had the opportunity to discuss with **Artur Ekert**, **Peter Knight**, **Tommaso Calarco** and many startup founders, from **PsiQuantum**, **IQM**, **ParityQC**, **ProteinQure**, **Qilimanjaro**, **Qblox** and others.

In short, during these years, we have been "embedded" in the scientific and entrepreneurial ecosystem. We also applied one of Heisenberg's principles derivatives, namely that the measurement tool may influence the measured quantity. But it can't be documented at this stage. It was and remains a beautiful adventure with real people, passions, convictions, ups and downs, and in the end, a nice result with French and European research and entrepreneurship in quantum technologies that are more dynamic and better positioned than a few years ago. And the adventure is just beginning!

---

<sup>2</sup> With a one-day training session with Roland Berger and Axelle Lemaire in April 2019, with high school students at Magic Makers in September 2019, with young people and parents at the Startup4Teens event in February 2020, and a debate in early March 2020 with Alexia Auffèves, Elham Kashefi and Pascale Senellart hosted by Fanny Bouton and organized at Talan, another event with a dominant female audience of all ages in the Tech4All event organized by Ecole 42 and Digital Ladies in March 2020, each time in partnership with the association *Quelques Femmes du Numérique ! (Some Digital Women)*.

You may wonder why this ebook is free and what is its business model. I have published all my ebooks like this since 2006 and fared well so far (on entrepreneurship, artificial intelligence and other technology and science related topics). I favor distribution breadth over revenue. It makes knowledge easily accessible to broad audiences, particularly with students. Also, being distributed in digital format, such ebooks are easy to correct and update. It is quite practical when you mention hundreds of people and organizations, and deal with complicated scientific matters. Afterwards, I sell my time in a rather traditional way with speaking and consulting missions.

## A complex domain in search of pedagogy

After having swept through many areas of science and deep techs, I can definitively position quantum physics and quantum computing at the complexity scale apex. Quantum physics is difficult to apprehend since relying on counter-intuitive phenomena like wave-particle duality and entanglement, and on a mathematical formalism that is not obvious to most people, including IT specialists, one of the key audiences for this ebook. It is still an open challenge to translate this scientific field lingua into natura language for most people, even with a strong engineering background.

As **Richard Feynman** famously pointed out, when you study quantum physics, if you think you understood everything, you are making a fool of yourself. **Alain Aspect** confirms this, always expressing doubts about his own understanding of the quantum entanglement that he demonstrated with photons in his famous 1982 experiment.

Explaining quantum computing is thus a new and difficult art. When reading quantum physics books, you discover a mathematical formalism and many terms like observables, degeneracy, gentle measurement, Hermitian operators and the likes and wonder how they relate to the physical world. Sometimes, it takes quite a while before being able to make this connection! On the other hand, you hear simplistic descriptions of quantum physics, noticeably on superposition and entanglement, and quantum computing, some coming from quantum computing vendors themselves<sup>3</sup>.

Once you think you understand it after having created a mental view of how it works, your explanations become quickly inaccessible for the profane. How do you avoid this side effect? Probably with finding analogies and use more visual tools to explain things than too much mathematics. I try this in many sections of this ebook, but, still, mathematics will be useful in some parts. Also, to make sure it does not lose its scientific soundness in the process, many parts of this ebook have been fact-checked and proof-read by quantum scientists. I'd say not enough. You'll be the judge.

This ebook frequently responds to questions like what, why, where and how? Particularly with linking theory, maths and the real world. Has Moore's law really stalled? What being "quantum" means for a product or technology? Why are we using this convoluted mathematical formalism? Do we really have objects sitting simultaneously at two different locations? Why parallel opposite vectors in the Bloch sphere are mathematically orthogonal? Why and where density matrices are useful? What are pure and mixed states describing in the physical world? Why superposition and entanglement are the two sides of the same coin? Why do we need to cool many qubit types? How are cryostats working? What is the energy consumption of a quantum computer? How much data sits in quantum registers? How is data loaded in a quantum program? What data is generated by a quantum algorithm and how is it decoded? Are quantum computers made for big data applications? How can you compare such and such quantum computer technology? Is Shor algorithm a serious threat for cybersecurity? When will we have a "real" quantum computer? Have we really achieved quantum supremacy? What is the real speedup of quantum algorithms? Are the case studies from D-Wave and the like real production grade applications? Will a quantum Internet replace the existing Internet? Why do many physicists dislike D-Wave and say it is not quantum?

---

<sup>3</sup> See the interesting point in [What Makes Quantum Computing So Hard to Explain?](#) by Scott Aaronson, June 2021.

Why do they still argue on the interpretation of quantum mechanics? How are classical computing technologies competing with quantum computers? Why are quantum random number generators not that random? Are the Chinese going to kill us (metaphorically) with their huge R&D investments in quantum technologies? Can Europe take its fair share in this new market? Oh, and if I'm in an organization... what should I do? Am I late in the game by doing nothing?

In order to properly address this broad laundry list of questions, this ebook is positioned above the average media coverage of quantum computing, as well as analyst reports, and below classical scientific publications that are generally largely inaccessible to non-specialists, or to specialists from other domains.

## A new computing wave

Quantum computing stays on top of the various applications of the second quantum revolution. Quantum sensing is more exotic and quantum telecommunications and cryptography are less fascinating. Why is quantum computing becoming an important topic? Firstly, because large IT companies such as IBM, Google, Intel and Microsoft are making headlines with impressive announcements that we must, however, take with a grain of salt, with a lot of hindsight, and decipher calmly. There's also the obvious impact of Peter Shor's factoring algorithm. It drives fuzzy fears on the future of Internet security and for your own digital privacy.

Above all, it is linked to the broad impact that quantum technologies could have on many scientific fields and digital markets. It may theoretically make it possible to solve problems belonging to classes of complexity that even the largest giant supercomputers will never be able to tackle with.

The other reason for this sudden interest is that we are still at the beginning of the story. New leaders will show up. A new ecosystem is being built. This in a field where there are still enormous scientific and technology challenges to overcome. It is a land of opportunities for science, technology and innovation.

It is quite difficult to evaluate the feasibility of large-scale quantum computing. For most scientists, we are still many decades away from it. Some believe it will never show up. Others are more optimistic. The main enemy is quantum decoherence and qubits errors happening during computing and which are difficult to avoid and correct. The plan is to fix that with quantum error corrections and logical qubits made of physical qubits. It then becomes a physical scalability issue with a bunch of complex engineering issues related to cooling, cryo-electronics, cabling, classical computing, miniaturization, as well as fundamental thermodynamic and energetic dimensions.

It is a very interesting living case study of how mankind builds upon scientific progress and addresses the most difficult challenges around.

## Summary and abstract

Here is a linear list of the topics covered in this ebook, which can also serve as an executive summary with key related messages and questions asked and answered. You won't probably read all the book straightforwardly but chunks by chunks as you learn the domain. As a student interested by quantum technologies, you'll start with the scientific parts. As a business person, you'll jump onto the various list of companies included per technology domain and look at what countries are doing in quantum technologies.

### Why Quantum Computing?

- Quantum computing's prospect is to overcome the limitations of traditional computing for solving specific problems whose complexity grows exponentially with their size.

- Why are conventional computing technologies and even other unconventional computing ones currently insufficient to achieve this goal?

## History and scientists

- This is the hall of fame of the subject where I highlight the efforts of dozens of renowned scientists who defined the fields of quantum physics and quantum computing. It establishes an approximate chronology of the field and showcases its history of ideas. Who inspired whom? The links between theories and experiments.
- It is also a didactic approach to the great discoveries of quantum physics, with the associated debates that confronted scientists, particularly around the 1920s and 1930s.

## Quantum physics 101

- What are the foundations of quantum physics that are used in quantum technologies and in particular in quantum computing? Entanglement, superposition, wave-particle duality and measurement. This will not be a complete course in quantum mechanics, but just the basics to better understand the rest. I decompose some well-known quantum equations, including the famous Schrödinger wave function.
- We also look at weird quantum matter and how it is used in quantum technologies: superconductivity, superfluidity, supersolidity and polaritons.
- Another section on extreme quantum describes branches of quantum physics that go beyond the current uses of quantum technologies and instead relate to particle physics and astrophysics. We also cover vacuum quantum fluctuations and the Casimir effect.

## Gate-based quantum computing

- We cover here the logical and mathematical part of gate-based quantum computing.
- Quantum computers exploit physical entities with two simultaneous states thanks to superposition and can be combined via quantum gates and entanglement. Quantum gates modify these qubits states. At the end of the computation, qubits values are read in the form of 0 and 1. Quantum computation is only digital at its beginning and with its results, but analog in the middle.
- We take a look at the main linear algebra concepts that are used in quantum physics and quantum computing. Complex numbers, Hilbert spaces, bras and kets, unitary and Hermitian matrices, state vectors, density matrices, matrix traces and their roles in understanding quantum computing and the power of quantum computing.
- We detail the mathematical models used to describe qubits and register states, the famous Bloch sphere that embodies it to visualize it in three dimensions. What is the role of this geometric description of a qubit and why is it so strange with orthogonal states not being geometrically orthogonal?
- We detail how we manipulated qubits with qubits registers, quantum gates and measurement.

## Quantum computing engineering

- We define the key comparison elements of quantum computers, even beyond DiVincenzo's famous criteria.
- We scan the types of qubits that use three main types of elementary particles: controlled **atoms** (trapped ions, cold atoms), **collective electrons** or **electron spins** (Josephson superconducting junctions, silicon qubits, Majorana fermions or NV centers) and flying qubits, including **photons** and **flying electrons**.

- We describe the overall engineering of a quantum computing, taking the example of superconducting qubits.
- We cover the way noise affects qubits and how it could be mitigated or corrected with Quantum Error Corrections.
- With current techniques such as superconducting qubits, a quantum computer fits in a few cubic meters and consumes about 25 kW, which is very reasonable considering the computing power provided. We are studying the energy aspects of quantum computing. Is there an energetic advantage to quantum computing? Is it sustainable as we scale the number of qubits?
- We also look at the cost structure of a quantum computer that will influence their actual price.
- At last, we mention the optimists and pessimists of the outcome of a scalable quantum computer. Why is there so much controversy on the feasibility of scalable quantum computers? Turning problems into solutions, what is the associated roadmap ahead for scientists and engineers?

### **Quantum computing hardware**

- This part covers the details of the main commercial qubit technologies around: superconducting, electron spins, NV centers, Majorana fermions, cold atoms, trapped ions and photons.
- We take a look at research labs and vendors, covering both large IT companies like IBM, Google and Intel and all the known startups.

### **Quantum enabling technologies**

- We look here at all the classical technologies that are being used to build quantum computers and other quantum products.
- Some of today's quantum computers processors need to be cooled down to 15 mK. We are studying the associated cryogenic systems and their engineering, based on dry dilution refrigerators.
- We also cover cabling, micro-wave generation and electronics, lasers and photonics.
- I take a look at the many raw materials used in quantum technologies, their origin, transformation processes and potential procurement issues. We will see that the dependency on China is quite moderate compared with other IT technologies.
- A section on unconventional computing covers computing technologies competing with or complementing quantum computing: supercomputers, superconducting processors, adiabatic and reversible computing, probabilistic computing and optical computing.

### **Quantum algorithms**

- Quantum computers use quantum algorithms to solve complex computational problems. These are very different in scope and design compared with classical computing algorithms. They were invented quite recently, starting in the early 1990s.
- I describe the algorithm toolbox including the important field of data preparation.
- The major applications of quantum computing include materials physics simulation, molecular biology, complex optimizations and machine learning.
- Quantum algorithms are often hybrid, combining traditional and quantum computation.
- I also describe the famous qubit state teleportation algorithm which may disappoint you since it has nothing to do with Star Trek teleportation.
- Quantum performance gains and the notion of algorithm verification and certification.

- Problem complexity theories, classical and quantum complexity classes, and limitations of quantum computers.

## **Quantum Software Development tools**

- Development tools classification.
- Tools coming from research laboratories and from industry vendors.
- Cloud access to quantum computers.
- Quantum code emulation.
- Quantum code verification, debugging.
- Quantum computing benchmarking with IBM's quantum volume, Atos's Q-score and the likes.
- The notions of quantum supremacy and quantum advantage.

## **Quantum Computing Business applications**

- Tour of the potential quantum computing applications in various market segments such as transportation, healthcare, energy utilities, chemistry, finance, marketing, defense and aerospace, intelligence and research.
- We describe some documented case studies of prototype solutions piloted with large companies in these different markets. Many come from D-Wave, a few from IBM and other vendors. Are these applications running in production or just low-scale proof of concepts?
- We cover the many startups in this field.

## **Quantum telecommunications and cryptography**

- This is a more mature market for quantum computing, a direct consequence of the long-term threats that quantum computing creates to public key cryptography-based systems.
- The market comprises two components: quantum cryptography, which allows security keys to be transported without being tampered with during transport, and post-quantum cryptography, which protects against Shor algorithm-based code breaking capabilities.
- Quantum cryptography is part of the broader field of quantum telecommunications, which can be used to link quantum computers to each other or to link quantum sensors to quantum computers. It is sometimes associated with the notion of the quantum Internet and distributed quantum computing.

## **Quantum Sensing**

- What are the quantum applications and industry vendors in quantum sensing for measuring time, light frequencies, gravity and magnetism?

## **Quantum technologies around the world**

- We start with venture funds more or less specialized in quantum technologies and with the quantum startups' ecosystem shape and form around the world.
- I cover the organization of quantum ecosystems in many countries with their major laboratories and state initiatives in the USA, Canada, the UK, Austria, Switzerland, the Netherlands, China, Japan, Singapore, Australia, Germany and France. This covers their public research, government initiatives and vendors ecosystem.

## Corporate adoption

- How can corporations adopt quantum technologies and how fast should they do it?

## Quantum technologies and society

- What are the philosophical and ethical issues raised by quantum computing? The biases and explicability of algorithms in the age of quantum computing, the great differences with these same questions when applied to deep learning. Is there a risk of seeing quantum computing concentrated in the hands of a few actors or countries? We deal with the philosophy of quantum physics. We also give some perspectives on gender balance in quantum technologies.
- Quantum jargon and its drifts. The desire for power over data, nature and understanding of the world. The education challenges. How are quantum technologies marketed?

## Quantum Fake Sciences

- Quantum medicine with some of its scientific fundamentals that deserve a low-level detour and then the high-level approaches belonging mostly to the realm of charlatanism.
- I cover various other quantum fakes, whatever you call it with quantum management and quantum marketing.

## Glossary

- A glossary of over 200 terms defines many technical terms used in the ebook. It's a good way to test your knowledge on the subject, including for the author!

## Reading guide

Here is a tentative to prioritize which parts of this ebook you could read according to your business and scientific level.

Physicists can find a state-of-the-art tour covering all dimensions of quantum technologies beyond the field they already master.

Computer scientists, engineers and students in various scientific fields are the core target audience for this book, as it presents, popularizes and contextualizes the various scientific, mathematical and engineering concepts used in quantum technologies.

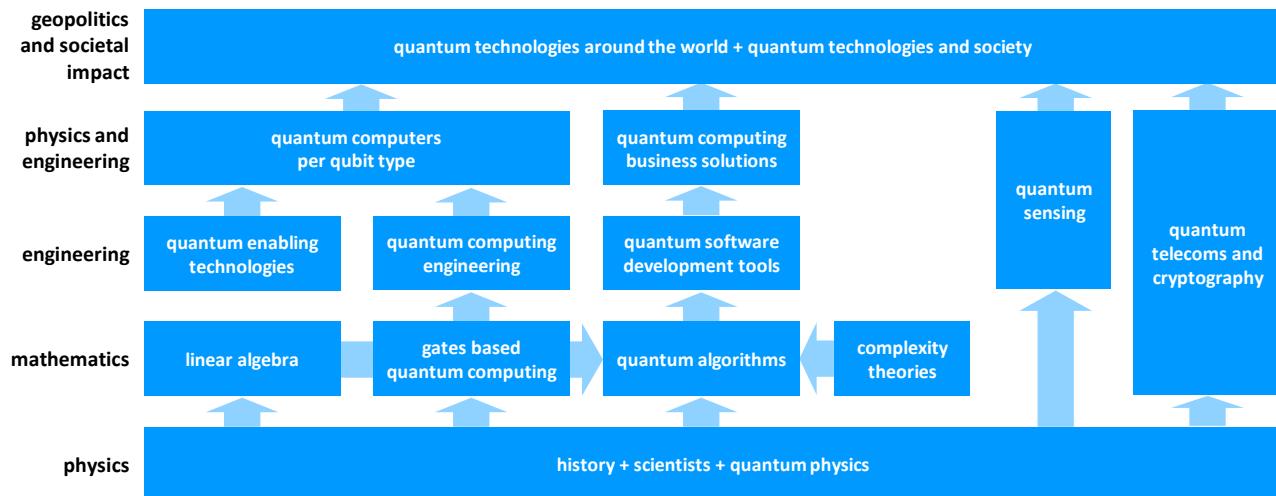
The required mathematical and computer basics level is at the Bachelor's degree level for most parts. Afterwards, it can also depend on your age since many of these concepts were not in current programs a couple decades ago unless you were already specialized in quantum physics.

Non-technical and decision-makers can still read the sections dealing with usages as well as with how countries are faring and societal issues.

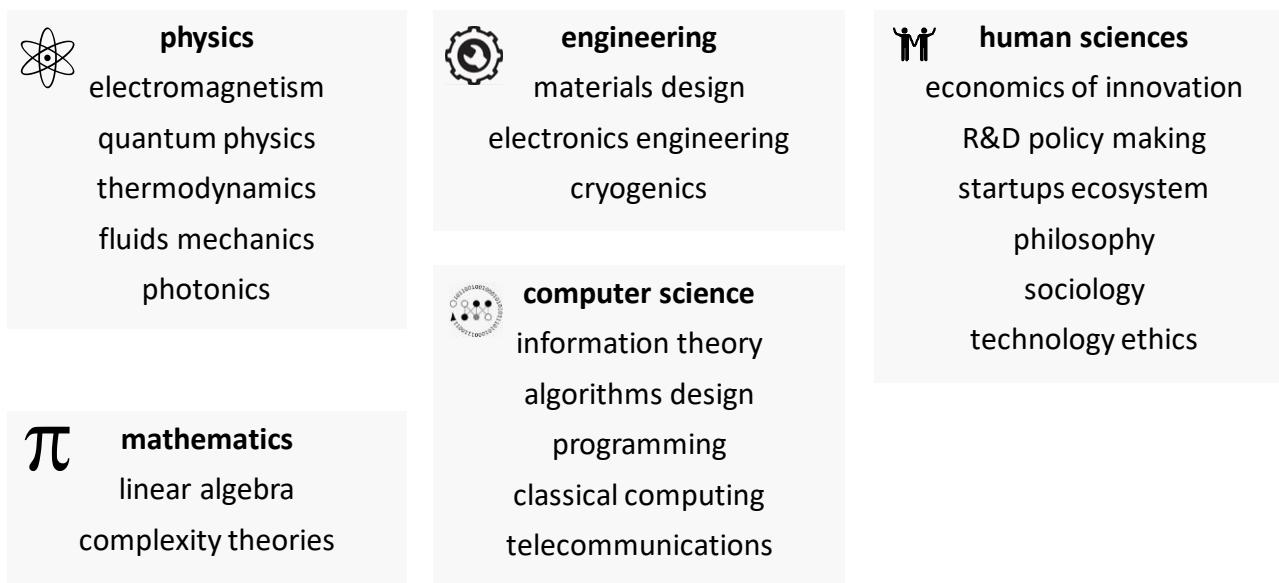
Book sections	Physicists	Computer scientists	Engineers and scientific students	Non technicians	Business audiences
Why					
History and scientists					
Quantum Physics 101					
Gate-based Quantum Computing					

Quantum Computing Engineering					
Quantum Enabling Technologies					
Quantum Computing Hardware					
Quantum Algorithms					
Quantum Software Development tools					
Quantum Computing Business applications					
Quantum Telecommunications and Cryptography					
Quantum Sensing					
Quantum Technologies around the world					
Corporate Adoption					
Quantum technologies in society					
Quantum Fake Sciences					

Here's another view of the table of contents showcasing the logic between the lower « physics » layers and the upper hardware, software and solutions layers.



At last, let's mention one of the reasons why a curious mind may like quantum technologies: they encourage you to explore many scientific disciplines, even human and social sciences.



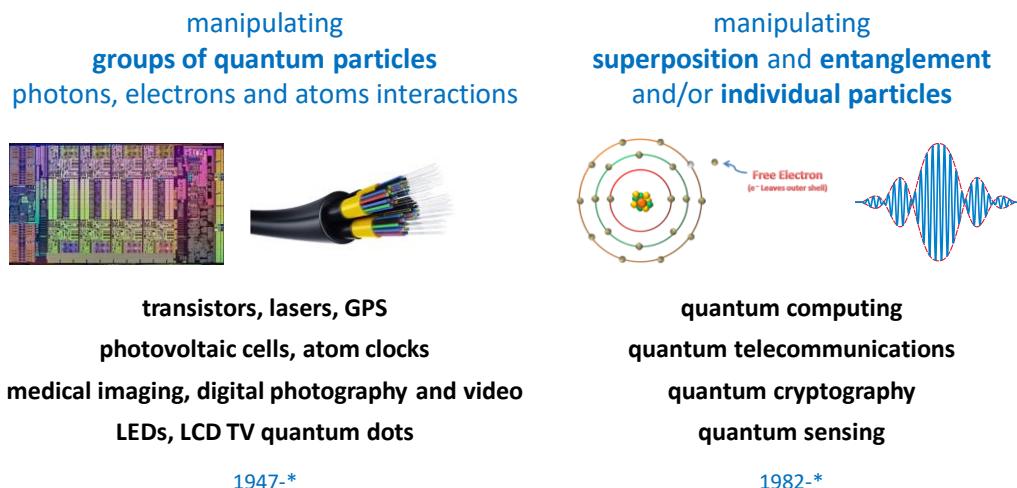
If you have some scientific background, you'll play in familiar territory but if you've had your degree a couple decades ago, this overview will provide you with some interesting intellectual upgrades. On top of that, learning quantum science is probably more efficient than Sudoku or crosswords to train your brain muscle as it ages!

## First and second quantum revolutions applications

Quantum physics has been implemented since the post-war period in almost all products and technologies in electronics, computing and telecommunications.

This corresponds to the **first quantum revolution**. It includes transistors, invented in 1947, which use the tunnel effect and are the basis of all our existing digital world, photovoltaic cells which rely on the photoelectric effect, and lasers which also exploit the interaction of light and matter and are used in a very large number of applications, particularly in telecommunications.

## 1<sup>st</sup> and 2<sup>nd</sup> quantum revolutions



Many medical imaging solutions rely on various quantum effects, including nuclear magnetic resonance imaging (MRI). LEDs are also based on quantum effects. The GPS is relying on atomic clocks synchronization. Quantum dots used in high-end LCD displays and Smart TVs also use variations of the photoelectric effect. The list is long and we will not detail all these use cases!

The **second quantum revolution** covers the technologies combining all or part of the ability to control individual quantum objects (atoms, electrons, photons), use quantum superposition and/or entanglement.

We owe the names of the first and second quantum revolution to Alain Aspect, Jonathan Dowling and Gerard Milburn in 2003<sup>4</sup>. The first and the two following ones created it simultaneously and independently. In the United States, the paternity is attributed to the latter, while in France, it is attributed to the former! Who knows why?

(cc) Olivier Ezratty, June 2021

<sup>4</sup> See [Speakable and unspeakable in quantum mechanics](#) by John S. Bell, June 2004 edition (289 pages) which contains a preface by Alain Aspect on the second quantum revolution, dated February 2003, pages 18 to 40. We find the expression in [Quantum technology: the second quantum revolution](#) by Jonathan P. Dowling and Gerard J. Milburn, June 2003 (20 pages) as well as in [Quantum Technology Second Quantum Revolution](#) by Jonathan Dowling, 2011 (60 pages). Dowling's writings make a very large inventory of various quantum technologies embedded in this second quantum revolution. [The Second Quantum Revolution: From Entanglement to Quantum Computing and Other Super-Technologies](#) by Lars Jaeger, 2018 (331 pages) is a broader overview of the different sides of the second quantum revolution.

The scope of the second revolution covers various recent applications of quantum physics as well as those of quantum computing that integrate quantum computing, quantum telecommunications and quantum cryptography. Said simply, it's about improving our digital world performance and security, and to increase the precision of all sorts of sensors.

- **Quantum cryptography** is a mean of communicating inviolable public cryptography keys thanks to the principle of photons entanglement and non-cloning theorem. It relies either on fiber optic communications or on space links with satellites as China has tested with its Micius satellite since 2017. This is a different field from **post-quantum cryptography**, which is intended to replace current classical cryptographic solutions with new solutions that are resistant to attacks carried out with the Shor and Grover algorithms running in quantum computers.
- **Quantum telecommunications** enables distributed computing, connecting quantum computers and potentially quantum sensors, enabling qubit to qubit distant connections. It is a field that is still in the making. It could become the base for a very secure quantum Internet and quantum cloud infrastructure. Although quantum information could be transmitted instantaneously, we cannot exploit this for transmitting classic information<sup>5</sup>. However, it can be used to distribute quantum processing on several quantum processors and in particular for "blind computing", which we also mention in various places in this ebook. It could provide a mean to "scale-out" quantum computers, when it's becoming difficult to "scale-in". This requires a lot of engineering, particularly to convert solid qubits into photon qubits. Photons are the only way to communicate with long distances.
- **Quantum sensing** makes it possible to measure dimensions with several orders of magnitude better precision than existing technologies. It is a vast scientific field that is the subject of numerous research projects and industrial solutions. It includes ultra-precise atomic clocks<sup>6</sup>, cold atom accelerometers and gyroscopes that use atomic interferometry, SQUIDs (superconducting based) and diamond cavity magnetometers such as those from Thales.

Table 1. Quantum Metrology and Sensing Technologies

Technology	Technological Readiness <sup>a</sup>	Potential Market
Measurement		
Atomic clocks	Commercial	\$50-\$500 million
Meters for voltage, current, and resistance	Commercial	—
Sensors		
Gravimeters and other atomic interferometers	Commercial	< \$50 million
Quantum inertial motion units	Medium-term	\$50-\$500 million
Atomic magnetometers	Commercial	\$50-\$500 million
Magnetoencephalography	Commercial	\$50-\$500 million
Quantum electron microscopes	Medium-term	\$50-\$500 million
Quantum-assisted nuclear spin imaging	Long-term	< \$50 million
Signal measurement	Medium-term	—

Sources: European Commission (2017) United States Air Force Scientific Advisory Board 2015; interviews.

Microgravimeters measure gravity with precision, such as those from **Muquans** (Bordeaux, France). This also includes various advanced medical imaging systems<sup>7</sup>. A dedicated section of this ebook is covering quantum sensing, starting page 588.

<sup>5</sup> But..." Entangled states cannot be used to communicate from one point to another in space-time faster than light. Indeed, the states of these two particles are only coordinated and do not allow to transmit any information: the result of the measurement relative to the first particle is always random. This is valid in the case of entangled states as well as in the case of non-entangled states. The modification of the state of the other particle, however instantaneous it may be, leads to a result that is just as random. Correlations between the two measurements can only be detected once the results have been compared, which necessarily implies a classical exchange of information, respectful of relativity. Quantum mechanics thus respects the principle of causality". Source: [https://fr.wikipedia.org/wiki/Intrication\\_quantique](https://fr.wikipedia.org/wiki/Intrication_quantique).

<sup>6</sup> See for example this NIST work on an atomic clock based on rubidium, the element most frequently used in atomic clocks. NIST [Team Demonstrates Heart Of Next-Generation Chip-Scale Atomic Clock](#), May 2019.

<sup>7</sup> See [Quantum camera snaps objects it cannot 'see'](#), by Belle Dume, May 2018. This is a variant of [Diffraction Free Light Source for Ghost Imaging of Objects Viewed Through Obscuring Media](#) by Ronald Meyers, 2010 (22 pages). Yanhua Shih (University of Maryland) US Army Research Laboratory, has been working on the subject since 2005. [Quantum Imaging](#) by Yanhua Shih, 2007 (25 pages). Also, see [Quantum Imaging - UMBC](#) (47 slides).

# Why quantum computing?

The main goal for using quantum computing is to solve complex problems that are and will stay inaccessible to classical computers. This happens when these problems solutions scale exponentially in computing time on classical machines. Problems that scale polynomially on classical hardware are not interesting for quantum computing.

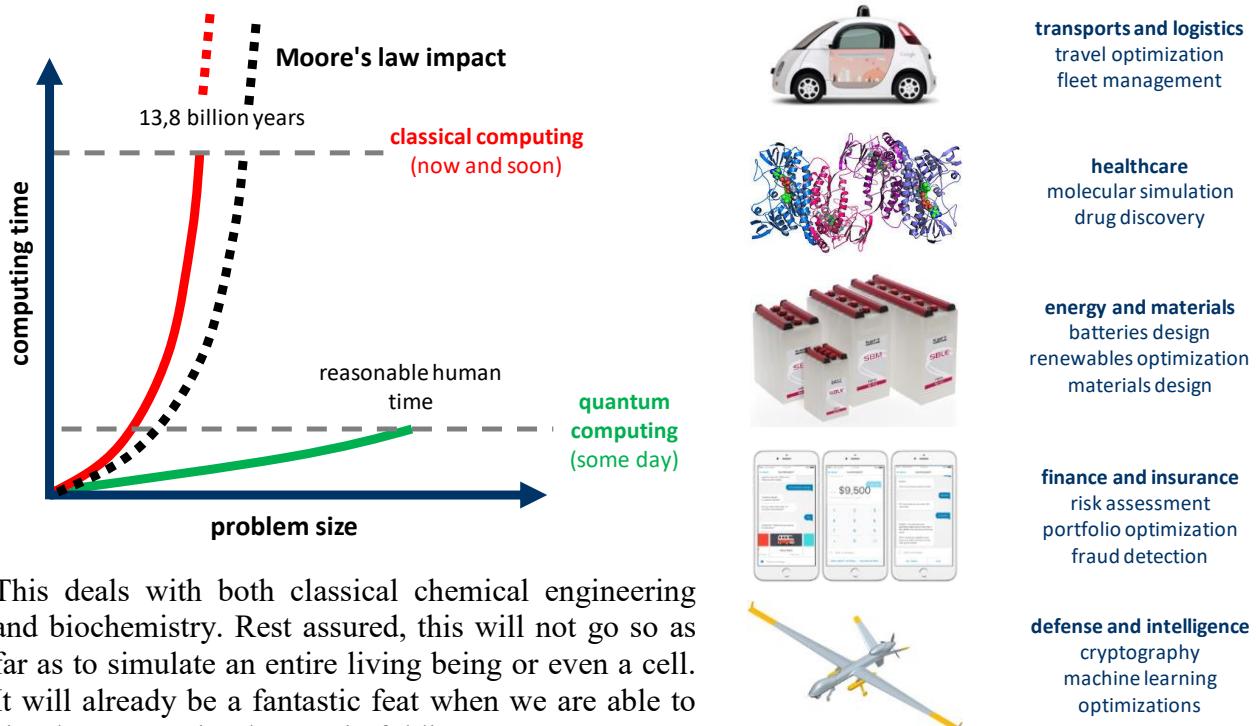
## Intractable problems

Typical exponential problems are combinatorial optimization searches and chemical simulations. Their size is usually expressed in a number of items like a number of steps for solving a travelling salesperson problem. Exponential problems are said to be "intractable" because their computation time evolves in crazy proportions with their size.

It starts with various optimization problems such as the above-mentioned traveling salesperson problem, with its contemporary equivalents applied to product delivery or autonomous vehicles routing. Today, you optimize your route with Google Maps or Waze, based on traffic conditions. Traffic conditions are variable and your actual journey time is not always what was planned nor optimal.

With fully autonomous fleets, it may theoretically be possible to optimize the individual path of each and every vehicle based on their departure and destination locations. Conventional algorithms could work with a limited number of vehicles, but beyond a few hundred vehicles and trips, traditional computing capacities would be largely saturated. Quantum computing may then come to the rescue!

Secondly, we have physics and molecular simulations, themselves governed by quantum mechanics equations. It usually boils down to finding the minimum energy configuration of a system, in order to simulate the interaction of atoms in molecules, complex crystal structures or even how magnetism works in various materials.



This deals with both classical chemical engineering and biochemistry. Rest assured, this will not go so as far as to simulate an entire living being or even a cell. It will already be a fantastic feat when we are able to simulate some simple protein folding.

A third area for quantum computing is the training and inferences of machine learning models and neural networks. It is now within the reach of conventional computers equipped with GPGPUs (general purpose GPUs) such as Nvidia's V100 and A100 and their tensor processing specialized units, optimizing matrix based operations. Quantum advantage is less obvious in this field, particularly since machine learning must usually be trained with a lot of data.

Finally, you can't avoid integer factorization, which is of particular interest to the NSA and their peers to break RSA-type public-key encryption security. We'll dig into this in details.

Other applications are investigated for different markets such as finance, insurance and even marketing. Many businesses have complex optimization problems to solve. Like with most technology-driven disruptions, businesses will progressively discover quantum computing use case as its market and related skills grow.

In extreme cases, computing times on conventional computers for exponential problems, even with the most powerful supercomputers of the moment, would exceed the age of the Universe, i.e. 13.85 billion years.

*“Building a quantum computer is a race between humans and nature, not between countries”*

Lu Chaoyang, China  
December 2020.

### Moore's law limitations

Moore's law, or “More than Moore” as its successor is now labelled, would have a marginal impact, dotted in the graph. First of all, it has been slowing down since 2006, and even if it did not slow down, it would not bring the capacity to solve exponential problems. Computation times for exponential problems would remain exponential despite the supposed doubling of machine power every 18 months to two years. The addition of a single qubit theoretically doubles quantum computers power, both in terms of internal memory space and computing parallelism capacity<sup>8</sup>.

In comparison, quantum computers could theoretically, one of these days, solve these same problems within a reasonable time span on the scale of a human life, in hours, days, weeks or months. Reasonableness obviously depends on the nature of the problem to be solved.

The main benefit of quantum computation is to modify the time scales for solving a problem and turn problems whose classical solution requires some exponential time into quantum solutions requiring at most some polynomial time. It can become useful when the size of the problem is large, sometimes with only about fifty items in a combinatorial optimization search! Quantum computation also makes it possible to gain space, particularly memory, to perform these calculations.

However, the scientific and technological barriers to overcome to make this real are still immense. Some of these use case promises may even be frequently oversold.

Meanwhile, quantum computing is not a “jack of all trades” solution. It is not a replacement tool but more a complement to current High Performance Computers (HPC). Many, if not most of today's classical computing problems and software are not at all relevant use cases for quantum computing.

From an economy historical perspective, the consequence is that quantum computing won't probably be a **Schumpeterian innovation**. It will not entirely replace classical legacy technologies. It will complement it. It's an incremental instead of being a replacement technology. You probably won't have a quantum desktop, laptop or smartphone to run your usual digital tasks although quantum technologies can be embedded in these devices like quantum sensors and quantum random numbers generators.

---

<sup>8</sup> One could though argue that adding a single functional qubit to a quantum computer appears to be exponentially difficult with the number of qubits.

Quantum computers will be hidden from users and sit in cloud data centers, like Nvidia GPGPUs racks. This will be even amplified by the progress we can anticipate with wireless telecoms.

When quantum computers will scale after 2030, we'll probably use 6G or 7G networks with even better latency and bandwidth! Of course, it's still hard to anticipate the usages brought by quantum computers when they will scale. Let's still boil in the fact that, as we'll see later, quantum computers are not excellent to handle big data nor for real-time computing. This makes it less relevant to use a local quantum processor, as it makes sense today to have local neural networks capacities to handle your in-camera image recognition processing and voice recognition in smartphones. Less data means more relevance for distant quantum computation done in the cloud.

## Classical computing technology developments

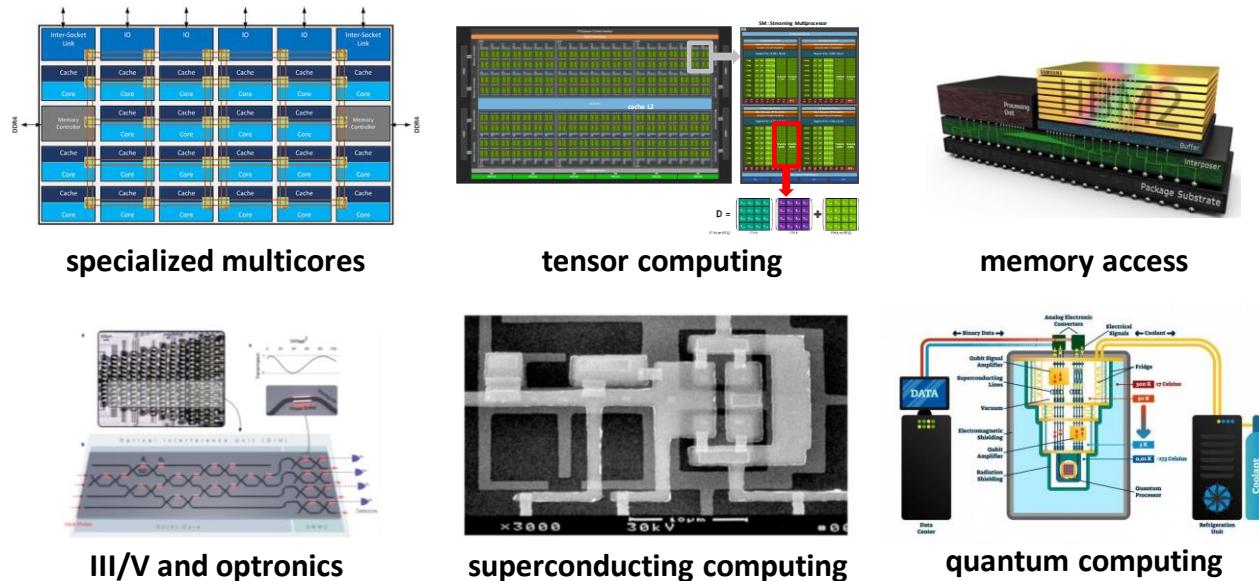
How are we currently making progress with conventional computing? We rely on a few known techniques, some of which have not yet been fully explored.

Multi-core architectures enable parallel processing but with limits formalized by **Amdahl's law**, which describes the upper limits of parallel computing systems acceleration.

We have the ongoing sluggish increase of transistors density in processors coupled with so-called **Domain Specific Architectures** using ad-hoc circuits like tensors (matrix multipliers) used to run specialized algorithms like neural networks. One key technology development is to make sure memory is as close as possible to processing units.

**Neuromorphic processors** mimick biological neurons features with integrated memory and processing using memristors.

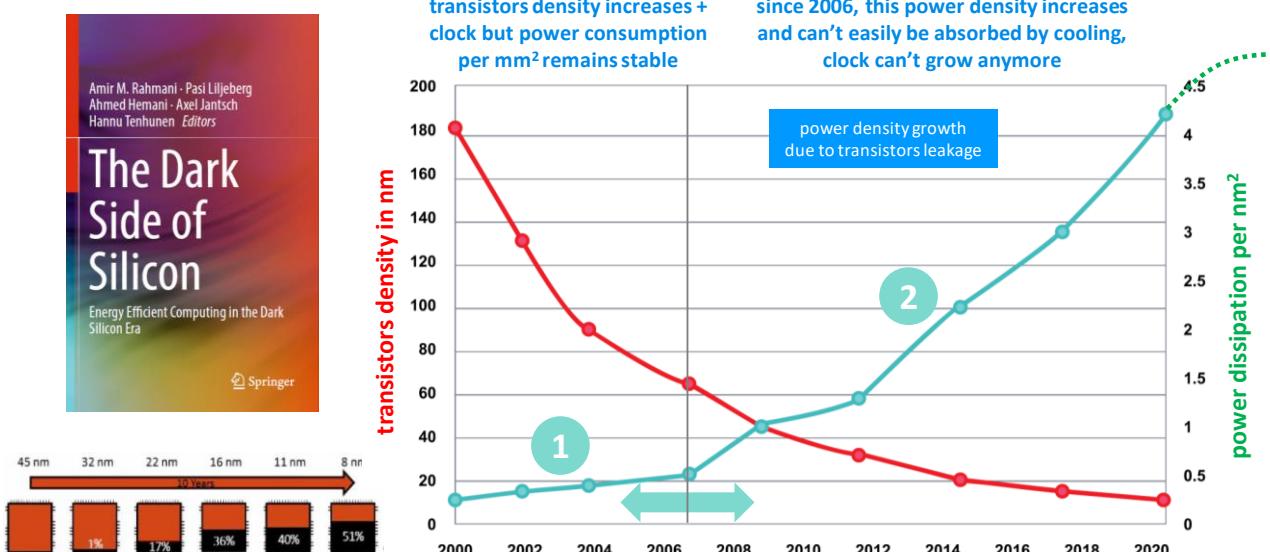
**Optronics** can replace electrons with photons to process information. It could theoretically enable processors running 20 to 25 times faster than current CMOS processors and reach 100 GHz. But these processors are difficult to develop and integrate. The materials used are different from those of CMOS processors. Manufacturing processes must switch from silicon to III-V materials like indium and gallium.



The heat barrier limits our capacity to increase processor clock speed beyond 5 GHz. It can reach 6 GHz with liquid cooling<sup>9</sup>. This is due to the end, in 2006, of **Robert Dennard's** (1932, American) scale established in 1974.

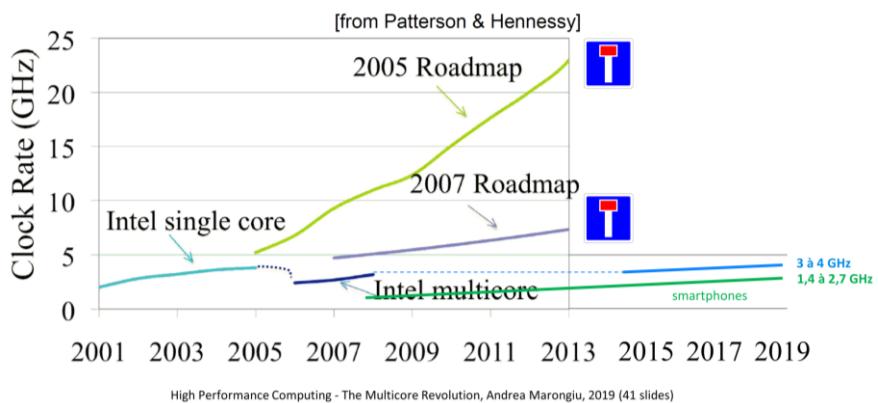
According to this scale or rule, as the transistors density increased, the power consumed per unit area of the chipsets was stable. This happened since the transistors voltage and current could decrease with their density, while increasing the clock frequency. Starting with 65 nm integration, this rule was broken.

## end of Dennard scale in 2006



The transistors current leaks started to grow and power consumption soared. This is what prevents the growth of processors clock. At the beginning of the 2000s, Intel planned in its roadmaps to raise their CPU clock frequency up to 20 GHz. It then stopped playing this game and instead entered the multicore realm.

However, the clock quest is still in play. In June 2021, Intel released a new micro-processor for high-end laptops running at a 2.9 GHz base clock but with a 5 GHz turbo mode for a single core, the 4-core i7-1195G7, etched in 10 nm, and with a TDP of 28 W (thermal dissipation power).



The semiconductor demand switched in 2007 towards low-power multi-functions chipsets for smartphones. This opened up a boulevard for Arm core-based processors and growth for corporations like **Qualcomm**.

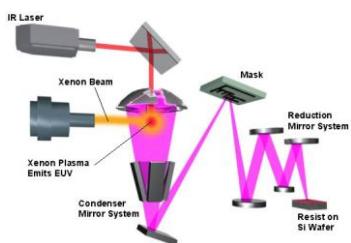
<sup>9</sup> See on this subject [Minimum Energy of Computing, Fundamental Considerations](#) by Victor Zhirnov, Ralph Cavin and Luca Gamaitoni, 2014 (40 pages) which compares the energy efficiency of living things and electronics.

The available computing power per consumed kW increased steadily, doubling every 1.57 years between 1946 and 2009, according to **Jonathan Koomey**'s empirical law enacted in 2010. However, this doubling slowed down to 2.6 years after 2000, due to the end of Dennard's scale.

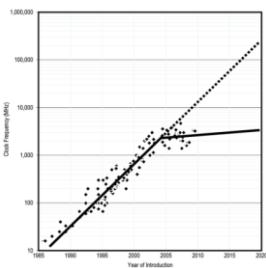
There are many techniques used to optimize classical computing footprint, particularly around memory management, with making sure memory is as close as possible to computing, including in-memory processing<sup>10</sup>.

After 2006, transistors density still continued to increase. However, the end of Dennard's scale led to the rarely mentioned **dark silicon** phenomenon. As the chipsets get too hot, it becomes difficult to use it entirely.

Various methods are then combined: on-demand cores or functions deactivations according to usage needs, or a shutdown of certain portions or cores, or a voltage drop, or a selective clock frequency adjustment. This is what is used in the Arm core-based processors of smartphone chipsets, whose cores do not use the same clock rates, in the so-called big.LITTLE architectures<sup>11</sup>.

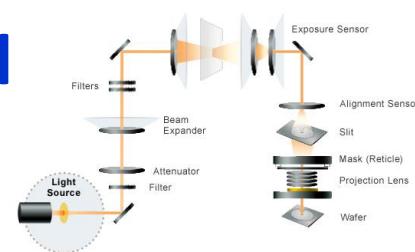


**Extreme Ultra Violet (EUV)**  
for <= 10 nm density

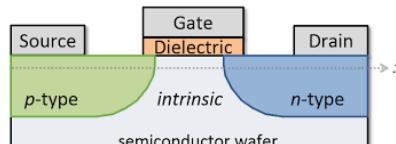


**heat barrier**  
limiting processor clocks

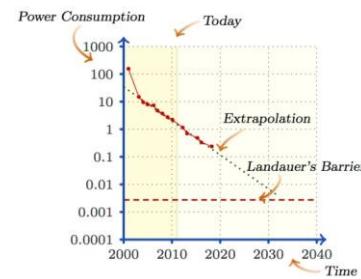
## CMOS technical challenges



**reticules size limit**  
chipsets die size limit



**indesirable quantum effects <2 nm**  
dielectric = 6 atoms thick



**Landauer barrier**  
lower power consumption limit

To lower transistors density below 10 nm, etching systems using extreme ultraviolet are required, coming from **ASML**. Etching resolution depends on the wavelength of the light used to project a mask on a photoresist.

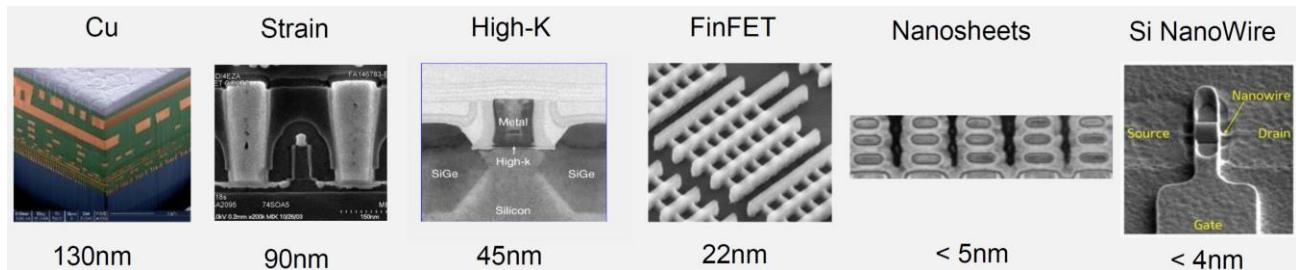
Lowering the transistors size requires increasing this frequency to decrease the wavelength, and thus go from the current deep ultra-violet to extreme ultra-violet. It took more than 10 years to develop these EUV lithography systems. It is in production since 2019 in TSMC and Samsung 5 nm nodes fabs. One of key benefits of EUV etching is to reduce the usage of the costly multiple patterning process in order to improve lithography resolution.

<sup>10</sup> See [Energy Efficient Computing Systems: Architectures, Abstractions and Modeling to Techniques and Standards](#) by Rajeev Muralidhar et al, July 2020 (35 pages) which makes a good inventory of the various ways to save energy with classical computing. And [Processing-in-memory: A workload-driven perspective](#) by S. Ghose et al, IBM Research, 2019 (19 pages).

<sup>11</sup> There are many other techniques to improve classical processors energy efficiency. See for example [Energy Efficient Computing Systems: Architectures, Abstractions and Modeling to Techniques and Standards](#) by Rajeev Muralidhar et al, AWS and Melbourne University, July 2020 (35 pages).

For a while, scientists warned about undesirable quantum effects appearing below 10 nm nodes. But it didn't prevent going down to 5 nm. Samsung and TSMC roadmaps are still predicting to reach 3 nm by 2025 and 2 nm beyond this, thanks to nanowires and nanosheets techniques<sup>12</sup>. In July 2021, Intel even announced a new density scale using angstrom sized transistors, with 20A and 18A by 2025 (meaning... about 2 nm).

In August 2020, TSMC announced that it would start 3 nm production as early as 2022, combining EUV etching with the traditional FinFET technology that has been in use for more than 10 years. In May 2021, IBM announced it had prototyped 2 nm nanosheet-based chipsets, manufactured by Samsung, and also using EUV lithography<sup>13</sup>.



As far as integration is concerned, two other limits must be taken care of, such as **Rolf Landauer's** (researcher at IBM in 1961) principle which defines the minimum energy required to erase a bit of information. It is a theoretical barrier contested by some physicists<sup>14</sup>. And it can be circumvented as we will see with the technique of [adiabatic and reversible computing](#) that is covered page 427.



Finally, there is a limit coming from the reticles size, these optical systems used in lithography whose size is physically limited, especially optically. It's explained in this illustration, coming from **ASML**, the world leader in semiconductor lithography. This limit has been reached with the largest recent processors. The largest single-die processors of 2020 were the **Nvidia A100** with its 54.4 billion transistors etched in 7 nm, superseded closely in size by the **Graphcore GC200** with its 59.4 billion transistors and 1,472 cores, launched in July 2020.

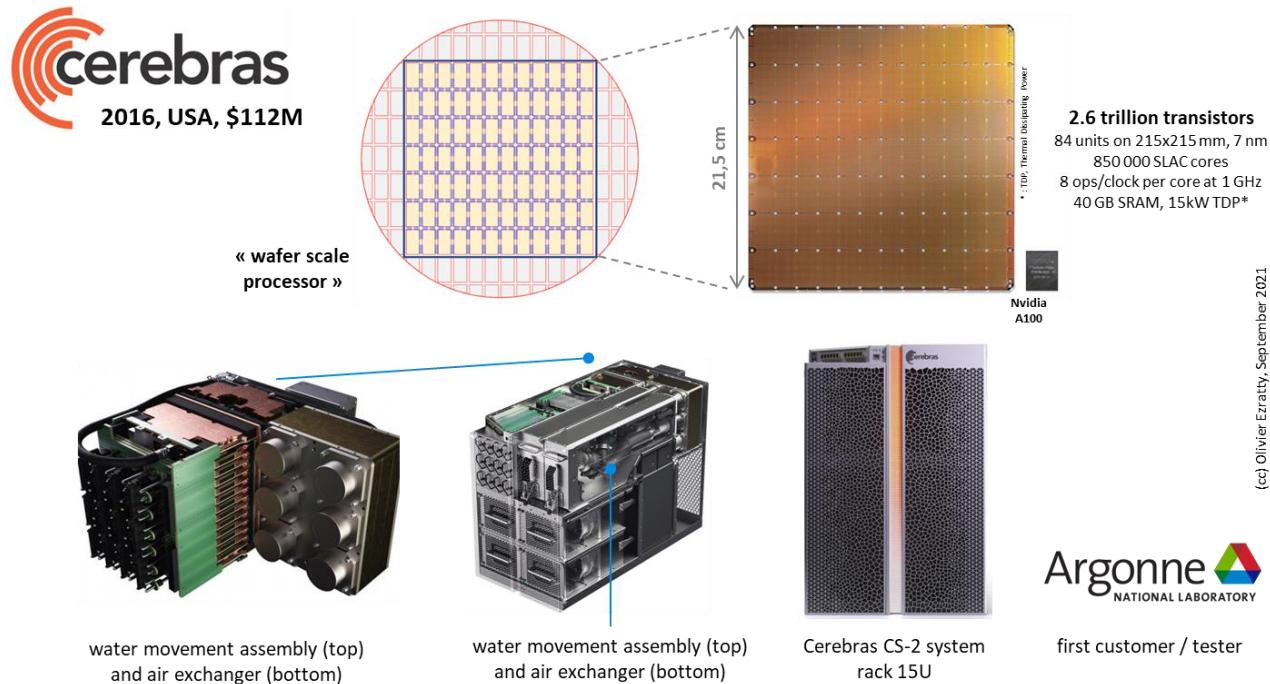
<sup>12</sup> See [Beyond CMOS, Superconductors, Spintronics, and More than Moore Enablers](#) by Jamil Kawa, Synopsys, March 2019 (43 slides), a good presentation describing the various ways to improve the power of components including cold CMOS, semiconductors operating at liquid nitrogen temperature levels (-70°C) and superconducting Josephson effect based transistors.

<sup>13</sup> See [IBM Introduces the World's First 2-nm Node Chip](#) by Dexter Johnson, IEEE Journal, May 2021.

<sup>14</sup> Source for Landauer's boundary diagram: [Reversible Circuits: Recent Accomplishments and Future Challenges for an Emerging Technology](#) by Rolf Drechsler and Robert Wille, 2012 (8 pages).

**Cerebras** (USA) nevertheless launched in 2019 an amazingly large 21.5 cm x 21.5 cm square processor, fitting in an entire 300 mm wafer, which circumvents the reticle size limit by being etched in several runs, for its 84 main processing units connected by metal layers. The second version of this chipset launched in 2021 contains 2,6 trillion transistors and 40 GB of cache SRAM memory and has a memory bandwidth of 20 PB/s, allowing it to significantly accelerate neural networks training. This massive chipset burns about 15 kW/h which are evacuated by a specific water-cooling system. Manufacturing techniques generate defects and more than a couple percents of the 850,000 processing units are defective and are short-circuited during software execution<sup>15</sup>.

Quantum computing will make it possible to overcome the various limitations of current CMOS processors for certain tasks. However, it will not replace them at all for tasks currently performed by today's computers and mobile devices.



Typically, video and audio compression and decompression are not relevant tasks for quantum computing. They are usually carried out in specialized CPU processing units, known as DSPs. Similarly, applications handling very large volumes of data are not suitable for quantum computing for a whole host of reasons that we will study, mainly because data loading speed into qubits is quite limited.

As its use cases will be different, it is hard to anticipate the IT landscape that will emerge with powerful quantum computers when they show up. Even with the advent of quantum computers, Ray Kurzweil's singularity predictions, which rely on the ad-vitam extension of Moore's law, will need to be adjusted!

### Unconventional computing

We will also quickly evaluate some [other avenues](#) considered to overcome the current limitations of classical computing, which can provide a power gain positioned between classical and quantum computing. These belong to the broad category of “unconventional computing”.

<sup>15</sup> With its D1 chipset presented in July 2021, Tesla chose another approach. Engraved in 7 nm, it has a computing capacity of 22.6 TFLOPS FP32, with 50 billion transistors and a 400W TDP. It contains 354 computing units with 1,25 MB SRAM per unit. They assemble these D1 in 25-chipsets tiles, consuming 15 kW, exactly like a Cerebras chipset.

This includes transistors operating at superconducting temperatures (around 4K, with new projects funded since 2014 by the US IARPA), digital annealing computing (proposed by **Fujitsu**), **reversible** and/or **adiabatic computing** that reduces energy consumption and circumvents Dennard's scale end, **probabilistic computing** as well as different forms of **optical computing**.

When working on this ebook, I also delved into the inner workings of supercomputers and specialized processors to better understand their strengths and weaknesses. When comparing quantum computers to classical computers, we are better off with knowing both sides of the equation!

These are sort of backup solutions, should science fail to create scalable quantum computers. It will also complement quantum computing used in the context of hybrid computing. Other solutions, such as with superconducting electronics, are potential enabling technologies for scaling certain types of quantum computers.

However, none of these solutions seem positioned to solve intractable problems although some of these are claiming they have this capacity.

The history of technology is about exploring multiple branches. Some do not succeed. Some help each other. Also, some can suddenly wake up after being frozen for decades.

### Why... key takeaways

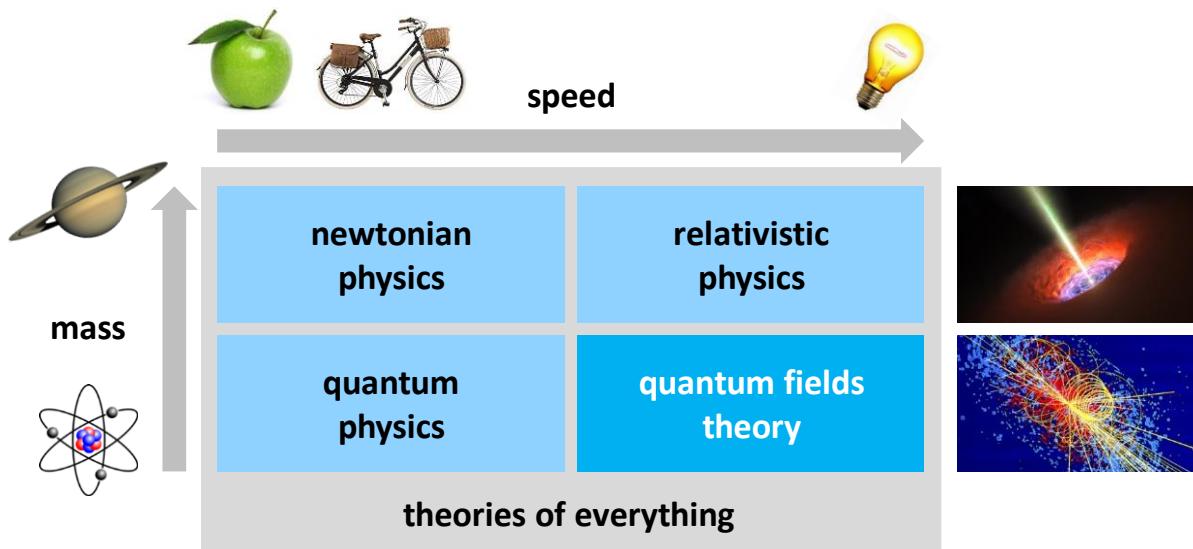
- All existing digital technologies are already quantum and belong to the first quantum revolution including transistors, lasers and the likes. The second quantum revolution is about using a variable mix of superposition, entanglement and individual quantum objects. It contains quantum computing, quantum telecommunications, quantum cryptography and quantum sensing.
- Quantum technologies are at the crossroads of many scientific domains encompassing physics, mathematics, computing, social sciences and the likes. It creates new educational and pedagogy challenges that must be addressed in innovative ways and customized according to various audiences. This ebook targets broad audiences with some technical background, including computer science engineers.
- Quantum computing makes sense to solve so-called intractable problems whose computing complexity grows exponentially with their size. These can't be solved with classical computing, whatever happens with Moore's law. But we're not there yet since there are many challenges to scale quantum computers beyond what can be done today.
- Other new technologies may compete with quantum computing, belonging to the broad "unconventional computing" category. Only a very few of these could also bring some exponential computing capacity. Most others bring other benefits compared with classical computing like in the energy consumption domain. Some of these technologies like superconducting electronics and adiabatic/reversible computing could also be helpful as enablers of quantum computing scalability.
- This ebook is unique in its shape and form. It covers quantum technologies with a 360° approach. It's more scientific than most publications, outside research review papers. It's a good appetizer for those who want to investigate the matter whatever the angle.

# History and scientists

After having set the stage, we'll make an history detour to discover the origins of quantum physics. As any scientific and technological endeavour, it's above all a great human story. I pay tribute here to the many scientists who, step by step, made all this possible and are still working on it for those who are still in this world.

**Nanoscopic physics.** Quantum physics deals with atomic and sub-atomic level particles and with the interactions between electromagnetic waves and matter. It differs from classical Newtonian physics, which predictably governs the dynamics of macrophysical objects, beyond a few microns and up to the size of planets and stars. Classical physics is governed by Newton's laws for matter, by Maxwell's laws for electromagnetic fields and associated forces and by statistical physics which describes continuous media such as gases and fluids and from which the principles of thermodynamics are derived.

When the speed of objects becomes close to the speed of light or when we reach large object's mass, the theory of relativity comes in, explaining the curvature of space-time and modelling the impact of gravity. It helps describing extreme phenomena such as black holes or neutron stars. It allows us to interpret the History of the Universe, but not entirely. But relativistic electrons are also hidden in our body's atoms and in many elements on earth as we'll quickly discover with the weird field of relativistic quantum chemistry.



The fourth domain of physics in this quadrant is the quantum fields theory. It describes the physics of high-speed elementary particles, such as those observed in particle accelerators like quarks and the famous Higgs boson. Richard Feynman is one of the founders of quantum electrodynamics, a subset of quantum field theory.

In a way, quantum physics was a mean to unify classical matter physics and electromagnetic waves physics. It helps describe how matter was organized at the atomic and electrons levels and how these interacted with quantized electromagnetic waves, aka photons, including visible light.

**Unification still in the making.** Physics is still not yet complete nor unified. Some observable physical phenomena still resist it. We do not know how to explain the origins of gravitation and we are still looking for the dark matter and energy that would explain the cohesion of galaxies and the Universe current expansion. Scientists would like to explain everything but some knowledge may never be accessible such as the shape and form of the Universe before the Big Bang.

The so-called theory of everything (ToE) or unification theory sought after by some physicists would be a formalism unifying all the theories of physics and in particular relativity, gravity and quantum physics. This very serious field of physics is still in the making<sup>16</sup>. Numerous proposals emerge and sorting it out is not easy<sup>17</sup>.

**Connecting the dots.** This part will help you memorize who's who in the History of quantum physics and quantum computing. It will also cover some important science basics such as the Maxwell and Schrödinger equations that I'll try to explain in layman's terms, at least for readers having basic sciences knowledge. Explaining quantum computing inevitably starts with some quantum physics 101 explanations. Some of its basics, although sometimes quite abstract, must be understood. I still always try to connect the dots between quantum physics and quantum computing from a practical basis. It's a vast puzzle. I'll add its pieces one by one and even though the puzzle may not be fully completed, you'll get a picture enabling you to become fairly well educated on quantum computing.

**Experiments and theories.** Quantum physics took shape in 1900. Like almost all sciences, it is the result of the incremental work of many scientists with interactions between experimentation, theories and mathematical models creation. Sometimes, quantum physics is better explained with its underlying mathematical models than with fairly incomplete physical interpretations. Representation models such as the broad field of linear algebra plays a key role to describe quantum states and their evolution in space and time. Linear algebra is an essential tool to understand how quantum computer qubits work.

Even if we can trace the beginning of quantum physics to Max Planck's 1900 quanta discovery, it was based on earlier work from many other scientists who devised about the particle or wave nature of light, on the discovery of electromagnetism and atoms. Quantum physics is a human adventure that brought together immense talents who confronted each other and evolved step by step their understanding of the nanoscopic world. New generations of scientists have always questioned the state of the art built by their predecessors<sup>18</sup>. Physicists conducted numerous experiments, build theories and then verified it experimentally, sometimes with several decades of latency. They also had to pour philosophy into their work to interpret the deep significance of their discoveries, and quantum physics was not an exception. Despite its constant enrichment, quantum physics has shown an astonishing robustness to stand the test of time.

**Misrepresentations.** Many quantum physics scientists are famous even for general audiences, even though their work has been overly simplified. Schrödinger's famous cat and Heisenberg's indeterminacy principle are commonplace... even when details are different from their related clichés.

---

<sup>16</sup> The American-Japanese physicist Michio Kaku estimates that some theory of everything will be finalized by 2100. See [Michio Kaku thinks we'll prove the theory of everything by 2100](#), April 2019. Michio Kaku is not an outsider. He is at the origin of string theory. He defines very well the connection between the different branches of physics and this theory of everything in [A theory of everything?](#).

<sup>17</sup> This is the case of the Wolfram Physics Project launched in April 2020 by Stephen Wolfram, a prolific Anglo-American physicist, mathematician and computer scientist. Building on his 2002 book "[A new kind of science](#)", the author's idea is to explain everything, the world, physics, the universe, whatever, with cellular automata, graphs and fractals. The world would be discrete on a small scale, including time. His Physics Project focuses on the unification of physics with the same set of tools. See the [hundred pages presentation of the project](#), the [white paper](#) which contains a section on quantum physics. Physicists' views on this theory is more than circumspect. The papers does not develop a theory that would be verifiable with an experimental approach as was the case for quantum physics (superposition, wave function, wave function collapse, atomic transition spectral lines, ...). Wolfram's theory was critically analyzed in 2002 by Scott Aaronson in a 14-page [review](#), particularly about his Bell's inequalities interpretation, and in [A New Kind of Science](#) by Cosma Rohilla Shalizi of Carnegie Mellon University, who does not mince his words. The same "hammer/nail explains everything" approach was created by a team of scientists who describe the Universe physics laws self-learning capabilities with a giant neural network approach, in [The Autodidactic Universe](#) by Stephon Alexander, Jaron Lanier, Lee Smolin et al, 2021 (79 pages).

<sup>18</sup> Max Planck's cynically explained in 1950 the evolution of science with the death of old generation of scientists: "A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die and a new generation grows up that is familiar with it".

Schrödinger's key work is still his non-relativistic particles wave equation, not the 10 lines he wrote in 1935 on his eponymous cat thought experiment that is usually grossly misinterpreted!

Like life in general, science is a great relay race, with many players. Hundreds of other less-known contributors have also contributed to the field and must be recognized. Sometimes, genius scientists were so prolific than we forget their contributions. This is the case for John Von Neumann who is better-known for his "Von Neumann model" that is the cornerstone of classical computing and for his contribution to the development of EDVAC in 1949, the first stored program based computer, than for his huge contribution to quantum physics mathematical formalism with density matrices and quantum measurement.

You won't find here inventors or entrepreneurs *a la* Steve Jobs or Elon Musk, even though the founders of startups like D-Wave, IonQ, Rigetti and PsiQuantum are among the entrepreneurial pioneers of this burgeoning industry, all being high-level scientists with a PhD!

**Hall of fame.** This History of 20<sup>th</sup> century quantum physics is embodied in the mythical Fifth Solvay Congress in 1927, held at the Institute of Physiology in Brussels. It brought together the greatest mathematicians and physicists of the time including almost all the historical founders of quantum physics with Max Planck, Albert Einstein, Niels Bohr, Louis de Broglie, Erwin Schrödinger, Max Born, Werner Heisenberg and Paul Dirac<sup>19</sup>. All this happened as the foundations of 20<sup>th</sup> quantum physics theories were fairly well laid out.



17 of its 29 participants have been awarded a Nobel Prize, 6 of which before the congress (names underlined in green) and the rest after (in blue). It was probably one of the largest concentration of scientific brains per square meter in the history of mankind!

Solvay conferences are held every 3 to 4 years since their creation in 1911 by the entrepreneur and chemist **Ernest Solvay**. The 1927 congress's topic was electrons and photons, which are at the heart of quantum physics. One half of these conferences are dedicated to quantum physics, the last one having taken place in 2011. The 27<sup>th</sup> and most recent edition was held in 2017.

<sup>19</sup> Only fathers and no mother! Marie Curie was present but was not specialized in quantum physics. She worked on radioactivity.

The major contributions of these protagonists are generally arranged in chronological order, with some indication of who influenced whom.

## Precursors

We begin with the classical physicists and mathematicians of the 18<sup>th</sup> and 19<sup>th</sup> centuries who laid the scientific groundwork that allowed their 20<sup>th</sup> century successors to formalize the foundations of quantum physics<sup>20</sup>.



It's roughly organized in scientific contributions chronological order.

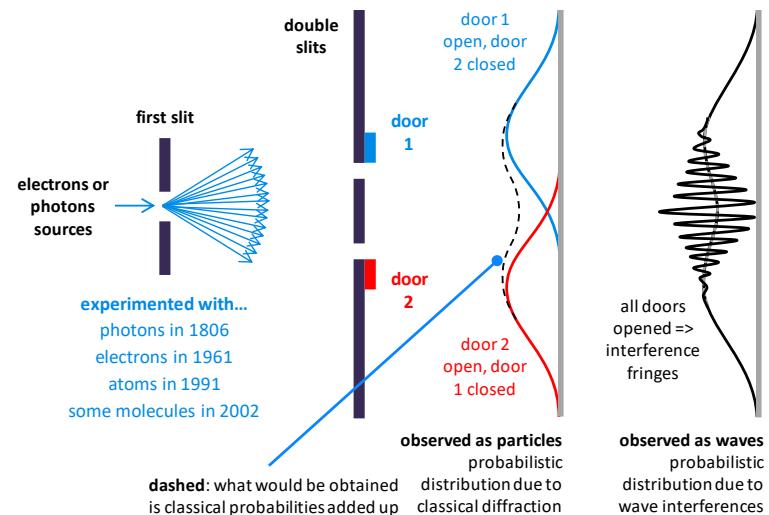


**Thomas Young** (1773-1829, English) was one of the great sciences and arts polymaths of his time, working in optics, medicine, linguistics, Egyptology and music. Above all, he determined that light behaved like a wave, which he proved with the double-slit experiment around 1806, illustrated *below*, that now bears his name. When reducing the size of both slits, it generates interference fringes creating alternating light and dark zones related to the wave nature of light. We had to wait till Albert Einstein's work in 1905 to determine that light was also made of particles.

His experiment used red filtered sunlight going through a first slit. Contemporary experiments use coherent laser light sources. This experiment is one of the cornerstones leading much later to the creation of the electromagnetism theory by James Maxwell.

The slit experiment was implemented with electrons in 1961, with a similar result, illustrating the electron wave-particle duality, devised first by Louis de Broglie in 1924. It was then also done with atoms in 1991 and with various molecules starting in 2002.

Thomas Young also worked on the principles of refraction and human trichromatic vision as well as in fluid mechanics, including on the notion of capillarity and surface tension.



As an Egyptologist, Thomas Young contributed to the study of the hieroglyphs of the famous Rosetta Stone, which was later used by **Jean-François Champollion** to decipher the whole stone texts. Champollion was then sponsored and helped by a certain **Joseph Fourier**. Yes, the mathematician!

<sup>20</sup> I do not always indicate the source of the diagrams used in this text. These are part of common scientific knowledge that are now in the public domain.



**William Rowan Hamilton** (1805-1865, Irish) was a mathematician and astronomer. He invented around 1827 a set of new mathematical formulations of the laws of physics incorporating electromagnetism. In quantum mechanics, we often speak of Hamiltonians or Hamiltonian functions. These are mathematical operators used to evaluate the total energy of a system of elementary particles including their kinetic and potential energies. This energy is evaluated over time.

Schrödinger's 1926 wave equation describes the evolution of a system's Hamiltonian over time. This concept is frequently used in analog quantum computers such as quantum simulators and quantum annealers, like with D-Wave's systems, and with universal adiabatic quantum computing. We'll have the opportunity to cover this in details in this ebook.



**Niels Henrik Abel** (1802-1829, Norwegian) is a prolific mathematician at the origin of the so-called Abelian groups. His work focused on the semi-convergence of numerical series, sequences and series of functions, the convergence criteria of generalized integrals, the notion of elliptic functions and integrals (used in cryptography) and the resolution of algebraic equations including his proof of the impossibility of solving general quintic equations.

He died way too early at the age of 26 from tuberculosis while visiting Paris and meeting his fiancée! Along with William Rowan Hamilton, Charles Hermite and Emmy Noether, he is one of the main 'suppliers' of the mathematical foundations used in quantum mechanics.

The adjectives "Abelian" and "non-Abelian" are associated with anyons, the quasiparticles that are the basis of topological quantum computing.

Why do these concepts of quantum mechanics invented long before his death refer to this mathematician? Mainly because the distinction between Abelian and non-Abelian is linked to their commutative mathematical representation. A system with A and B is Abelian when  $A^*B = B^*A$  or non commutative and non-Abelian when  $A^*B$  is not equal to  $B^*A$ . The most common non-commutative operations are non square matrices multiplications. The multiplication of a matrix  $(p \times q)^* (q \times p)$  will give a matrix  $(p \times p)$  whereas in the other direction,  $(q \times p)^* (p \times q)$  will generate a matrix  $(q \times q)$ , q and p being here numbers of rows and/or columns.

Non-commutativity is frequently found in quantum physics and particularly with quantum measurement. The order in which quantum objects properties are measured may influence the results because the used measurement operators are non-commutative. In some cases, though, operators are commutative, like with the Measurement-Based Quantum Computing (MBQC) technique that we will have the opportunity to describe later when dealing with photon-based quantum systems.



**Charles Hermite** (1822-1901, French) was another prolific mathematician of the 19<sup>th</sup> century. He worked on numbers theory, quadratic forms, the theory of invariants, orthogonal polynomials, elliptic functions and algebra. His main works were concentrated on the 1848-1860 period. We owe him the notion of Hermitian functions and matrices, which are widely used in quantum physics and quantum computing.

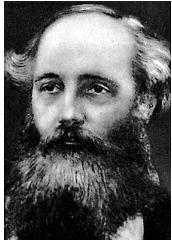
A Hermitian matrix is composed of real numbers in the diagonal and can be complex in the rest, and is equal to its transconjugate. Namely, their transpose matrix whose value of complex numbers has been inverted (i becomes -i and vice-versa).

Quantum measurement operations in quantum physics and computers are defined by Hermitian matrices.

$$A = \begin{bmatrix} 2 & i & -2i \\ -i & 1 & 3 \\ 2i & 3 & -1 \end{bmatrix}^\dagger \quad \bar{A} = \begin{bmatrix} 2 & -i & 2i \\ i & 1 & 3 \\ -2i & 3 & -1 \end{bmatrix}$$

transposed matrix

$A = \overline{(A)}^*$   
**Hermitian matrix**  
matrix equals its transconjugate



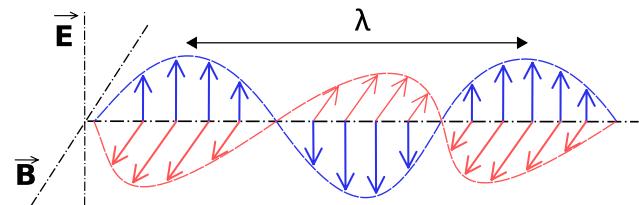
**James Clerk Maxwell** (1831-1879, Scottish) created in 1865 the theory of electromagnetic fields, combining an electric field and a magnetic field orthogonal to the direction of wave propagation as in the diagram *below*, and moving at the speed of light. This theory explains light-light interactions such as reflection, diffraction, refraction and interferences. Maxwell's work built on and improved the formalism from Faraday, Gauss and Ampère.

Maxwell's equations illustrate that when they are constant, electric and magnetic fields are independent, and in variable regime (with a wavelength  $\lambda$ ), it becomes interdependent ( $\vec{E}$  and  $\vec{B}$ ), one generating the other and vice-versa, hence the notion of electromagnetic waves and fields.

In Maxwell's equations, the electromagnetic field is represented by an electromagnetic tensor, a  $4 \times 4$  matrix whose diagonal is zero and whose half of the components describe the electric field and the other half the magnetic field. These four dimensions correspond to space (3) and time (1).

In fact, there are four main Maxwell equations<sup>21</sup>:

- The **Maxwell-Gauss** equation describes how an electric field is generated by electric charges. At each point in space, the electric field is directed from positive to negative charges in directions depending on the charges space position.



$$\text{div}(\vec{E}) = \frac{\rho}{\epsilon_0}$$

electric field  
divergent, measures field variation orientation  
charges distribution  
vacuum dielectric permittivity

Maxwell-Gauss equation describing the electric field created by electric charges

$$\text{div}(\vec{B}) = 0$$

$$\oint_{(\Sigma)} \vec{B} \cdot d\vec{S} = 0$$

magnetic field  
surface integral  
closed surface  
surface vector  $\Sigma$  derivative

- The **Maxwell-flux** equation states that a magnetic field is always generated by a dipole with positive and negative charges that are connected and inseparable. Mathematically, this translates into the fact that the divergence of the magnetic field is zero and that there is no magnetic monopole.

Namely, that there is no magnetic field line that escapes to infinity as we have with an electric field.

- The **Maxwell-Faraday** equation describes how the variation of a magnetic field creates an electric field. This is the principle used in electric alternators. The rotational operator using a nabla sign corresponds to a differential vector operation. It is equal to the first derivative of the magnetic field over time.

$$\vec{\nabla} \times \vec{E} = - \frac{\partial \vec{B}}{\partial t}$$

Maxwell-Faraday equation connecting magnetic and electric fields

<sup>21</sup> See these well done and visual explanations of Maxwell's equations: [A plain explanation of Maxwell's equations](#).

- The **Maxwell-Ampere** equation states that magnetic fields are generated by electric currents or by the variation of an electric field. This interdependence between magnetic fields and varying electric fields explains the circulation of self-sustaining electromagnetic waves. On the left of the equation is the rotational magnetic field.

As with Schrödinger's equation, Maxwell's equations have several variations, which may be confusing. Maxwell first published twenty equations with twenty unknown variables in 1865. In 1873, he reduced them to eight equations. In 1884, **Oliver Heaviside** (1850-1925, English) and **Willard Gibbs** (1839-1903, American) downsized the whole stuff to the four partial differential vector equations mentioned above. These four vector equations are reduced to two tensor equations for electromagnetic waves propagated in vacuum.

The non-interaction with other elements explains the independence in this equation between electric and magnetic fields.

Maxwell predicted that electromagnetic waves were travelling at the speed of light.

Electromagnetic waves were only experimentally discovered after Maxwell's death, by **Heinrich Hertz** (1857-1894) between 1886 and 1888. Hertz also discovered the photoelectric effect in 1887. Maxwell's description of electromagnetic waves had a phenomenal impact in electromagnetic telecommunications and optronics.

It also served as a foundation for the first quantum physics laws developed by Max Planck in 1900 which led progressively to the quantization of the electromagnetic waves.

Maxwell is also at the origin of the **Maxwell-Boltzmann** statistical law of gas distribution. It models the particle velocity distribution of a perfect gas. It does not take into account the interactions between particles and is not applicable to extreme conditions, such as very low temperatures. In particular, it is replaced by the **Bose-Einstein condensate** statistic for bosons (integer spin particles such as helium 4, which can be gathered in the same quantum state and energy level) and by the **Fermi-Dirac** statistic for fermions (particles with half-integer spins such as electrons or helium-3, which cannot cohabit in the same quantum and energy state).

Maxwell is the designer in 1867 of the so-called **Maxwell's demon** thought experiment which would make possible the reversibility of thermodynamic exchange processes and invalidate the second principle of thermodynamics.

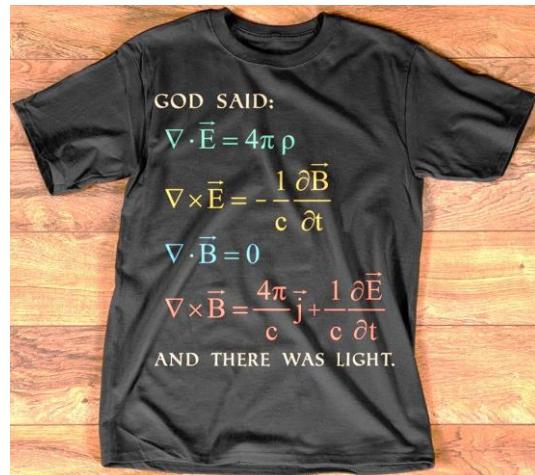
The diagram illustrates the derivation of Maxwell's equations from fundamental principles:

- Maxwell-Ampere equation connecting magnetic field to electric field:**

$$\vec{\nabla} \times \vec{B} = \mu_0 \vec{J} + \mu_0 \epsilon_0 \frac{\partial \vec{E}}{\partial t}$$
  - current density vector
  - vacuum magnetic permeability
  - vacuum dielectric permittivity
  - rotational
  - magnetic field
  - electric field
- Maxwell's equation in vacuum:**

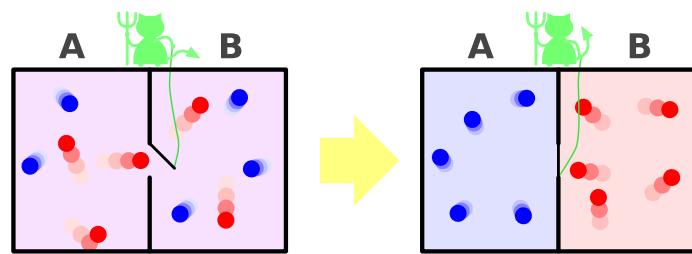
$$\frac{1}{c_0^2} \frac{\partial^2 E}{\partial t^2} - \nabla^2 \mathbf{E} = 0$$
  - second derivative over time of electric field
  - speed of light
  - electric field vector
  - second derivative over space of electric field
- Maxwell's equation in vacuum:**

$$\frac{1}{c_0^2} \frac{\partial^2 B}{\partial t^2} - \nabla^2 \mathbf{B} = 0$$
  - second derivative over time of magnetic field
  - magnetic field pseudo-vector
  - second derivative over space of magnetic field



It rests on two boxes containing two different gases where a gas at two different temperatures is separated by a hole and a closure controlled by a "demon". When the door is opened, the gases mix.

Once mixed (*on the left, Wikipedia sourced*), the demon would control which molecules could go from one box to another, taking advantage of the natural kinetic energy of the gases. This would allow in theory and after a certain time to return to the previous equilibrium in a non-equilibrium situation (*right*).



It took several decades to find the fault, notably via Léo Szilard in 1929 and Léon Brillouin in 1948. Initially, the explanation was that the demon needs to consume some energy to obtain information about the state of the gas molecules in order to sort them out. Therefore, energy is consumed to modify the stable equilibrium obtained to mix the gases.

The "up to date" explanation is somewhat different. The energy cost comes from resetting the demon's memory, which ultimately consists of a single bit of information<sup>22</sup>.

All this had repercussions on the notion of the energy value of information and led, much later, to the creation of the field of information thermodynamics, i.e. the study of the energetic and entropic footprints of information, particularly in quantum computing.

This field was then investigated by **Rolf Landauer**, known for his study of irreversible information management circuits heat generation, and by **Charles Bennett** and **Gilles Brassard**, the co-inventors of the QKD based BB84 protocol, which we will discuss later, and then by **Paul Benioff**, who was at the origin of the idea of gate-based quantum computing.

We finally owe Maxwell the creation of color photography in 1855, that was implemented in 1861, based on the three primary colors of human vision.

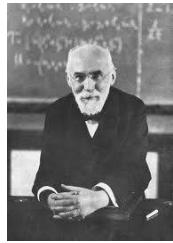
Maxwell's electromagnetic field equations has very well survived the test of time. It's still the basis of classical optics and quantum optics. Even when studying quantized light, researchers and students still rely on Maxwell's equations and their subsequent derivations created since then.



**Ludwig Boltzmann** (1844-1906, Austrian) was a physicist, the father of statistical physics, defender of the existence of atoms, facing a strong opposition from scientists until the beginning of the 20th century, and creator of equations describing fluid and gas dynamics in 1872. He is also at the origin of the probabilistic interpretation of the second principle of thermodynamics, which establishes the irreversibility of physical phenomena, particularly during thermal exchanges.

Irreversibility is associated with the creation of entropy. Boltzmann tried his hand at philosophy while defending the existence of atoms. Depressed, he died by committing suicide.

<sup>22</sup> Here is the detailed explanation by Alexia Auffèves (CNRS-Institut Néel): we can understand the operation of resetting a bit of memory by considering an ultimate Carnot engine, consisting of a single particle that can be located to the left or right of a certain thermostated volume. Left = 0, Right = 1 There are two possible operations. The first one is compression. The particle is initially to the left or to the right of the volume that contains it (we don't know) and we compress the said volume so that at the end it is necessarily on the left. It is an initialization operation where the bit is reset to state 0. As with any compression, you have to pay, here in this ultimate case, the work to be expended is  $kT \log 2$ . This is Landauer's famous work, which sets an energy bound to all logically irreversible operations. The second operation is relaxation. In the beginning, we know whether the particle is on the left or on the right. We position a wall, a pulley with a mass at the end and let the trigger operate while extracting an elementary work equivalent to  $kT \log 2$ . This is a Szilard machine. These two manipulations were performed experimentally in 2011 at ENS Lyon. It shows the energy footprint of information and are the ultimate solution to Maxwell's demon paradox. See [Information and thermodynamics: Experimental verification of Landauer's erasure principle](#) by Antoine Bérut, Artyom Petrosyan and Sergio Ciliberto, Université de Lyon, ENS Lyon, 2015 (26 pages).



**Henri Poincaré** (1854-1912, French) was a mathematician and physicist, precursor of the theory of relativity and gravitational waves. We owe him a probabilistic function that bears his name and which is the optical equivalent of the Bloch representation that we will see later, which mathematically describes the state of qubits. He is also the author of the mathematical conjecture that bears his name and that was demonstrated in 2003 by the Russian mathematician Grigori Perelman. It is relative to the existence of spheres in four-dimensional spaces.

He was a first cousin of Raymond Poincaré (1860-1934), president of France during the First World War, a lesser-known figure than Georges Clémenceau who was then Prime Minister and drove the war efforts against Germany and with allies from the UK and the USA.



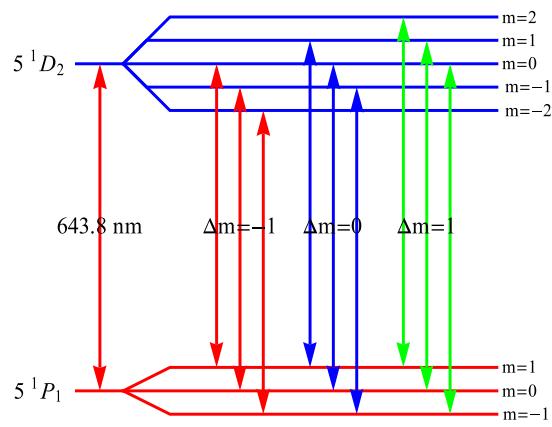
**David Hilbert** (1862-1943, German) is yet another prolific mathematician who, at the end of the 19<sup>th</sup> century, was the creator of the mathematical foundations widely used in quantum physics, in particular his so-called Hilbert spaces using vectors to measure lengths, angles and define orthogonalities. They are used to represent the state of qubits with vectors and complex numbers and more generally of all quantum systems. Still, his work had nothing to do with quantum mechanics, which was not yet formulated at the time.

His work was used by Paul Dirac in 1930 and John Von Neumann in 1932 to lay the groundworks of quantum physics mathematical foundations like the Dirac Bra-Ket notation and the Von Neumann quantum measurement formalism.



**Pieter Zeeman** (1865-1943, Dutch) was a physicist, Nobel Prize in Physics in 1902 with Hendrik Lorentz, for the discovery of the effect that bears his name between 1896 and 1897. The Zeeman effect occurs when excited atoms are exposed to a magnetic field. This affects their emission or absorption spectrum, that displays many discrete spectral lines. The effect is observed with spectroscopy, which breaks down light rays of different wavelengths with a prism.

In his experiment, spectral lines are broken down into an even number of lines (normal Zeeman effect) or an odd number of lines (abnormal Zeeman effect). The decomposition depends on the intensity of the magnetic field passing through the analyzed atoms.



It is matched by a polarization of the generated light whose nature and intensity depends on the orientation of the magnetic field relative to the light beam as shown here. The Zeeman effect can be explained by Pauli's exclusion principle, elaborated in 1925, and by the transitions in the energy level of the electrons in the same atom layer and having different magnetic moments. In astronomy, the Zeeman effect measurement is used to evaluate the intense magnetic fields in stars as well as within the Milky Way. It is also implemented in magnetic resonance spectroscopy (nuclear and electronic) in MRI scanners.



**Hendrik Antoon Lorentz** (1853-1928, Dutch) was a physicist who worked on the nature of light and the constitution of matter. He made the link between light and Maxwell's equations of electromagnetism. We owe him the Lorentz transformations that explain the results of Michelson-Morley's experiments between 1881 and 1887 which showed that the speed of light is stable, whatever the frame of reference. With Henri Poincaré and George Francis Fitzgerald (1851-1901, Irish), he is one of the key contributors to the theory of relativity formalized later by Albert Einstein between 1905 and 1915.

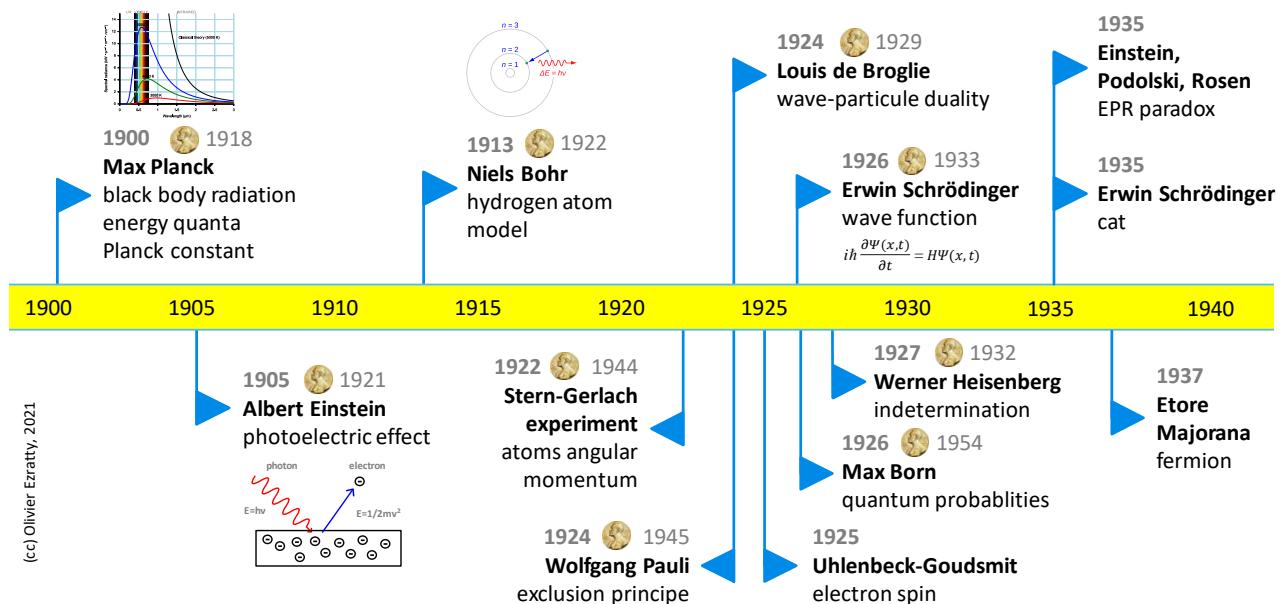
Let's also add **Joseph Larmor** (1857-1942, Irish/British) who, among other various contributions, was one of the first to associate electric charges with electron particles in 1894. We also owe him the notion of Larmor precession, the rotation of the magnetic moment of an object when it is exposed to an external magnetic field, discovered with protons in 1919 and later extended to electrons.

## Founders

The foundations of quantum physics started with Max Planck's black-body explanation with energy quanta and, then took shape over three and a half decades, roughly until 1935.

It involved the successive contributions from Einstein, Bohr, De Broglie, Schrödinger, Born, Heisenberg and Dirac to mention only the best-known contributors who were all theoreticians and not experimentalists. In the timeline below, the gold coins represent a Nobel prize.

Things were relatively quiet during World War II as lots of scientists were focused on creating the atomic bomb in the USA under the umbrella of the then very secret Manhattan project while Europe was not the best place in the world for travel and international scientific collaborations. German scientists who initially led quantum physics became isolated or emigrated to the USA or the UK because they were Jews, like Albert Einstein or Max Born.

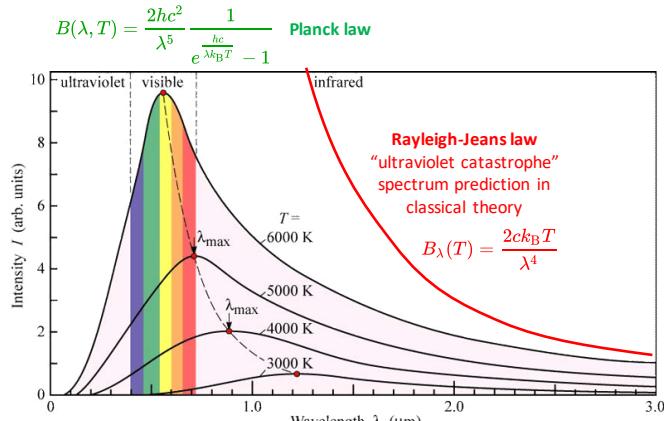


Here is a broader tour of the great physicists and mathematicians who laid the foundations of quantum physics. They are all Europeans who, some of whom emigrated from Europe to the United States before World War II.



**Max Planck** (1858-1947, German) was a physicist, initially specialized in thermodynamics. In 1900, he developed the first basis of quantum physics, hypothesizing that energy exchanges between light and matter are made by discrete quanta. This radiation is not continuous but varies by thresholds, in steps of a certain amount of energy, hence the term "quantum" and "quantum physics" or "quantum mechanics". His theory allowed him to roughly explain for the first time the enigmatic radiation of black bodies, that absorbs all incident magnetic radiation.

Examples of black bodies are a closed cavity like an oven, a heated metal that becomes red, orange, then white depending on the temperature, or a star like our own Sun. The spectrum of electromagnetic waves emitted by a black body depends only on its temperature and not at all on its material. The higher the temperature is, the more the electromagnetic spectrum emitted by the black body slides towards higher frequencies on the left, therefore towards purple and ultraviolet. The theory solved the ultraviolet catastrophe.

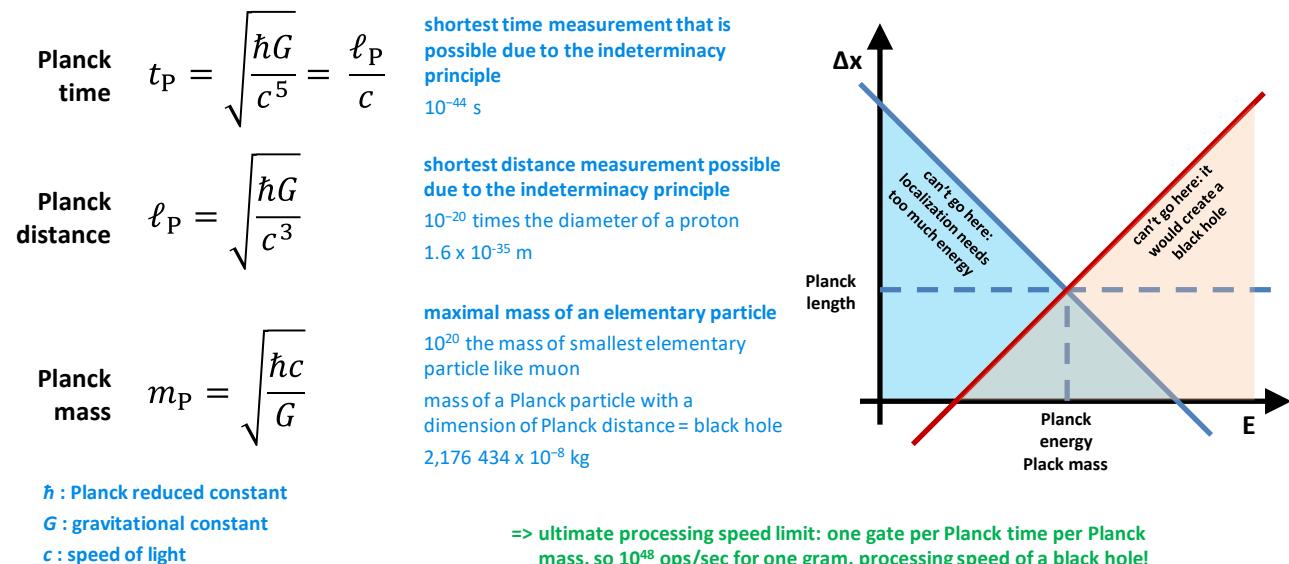


This so-called ultraviolet catastrophe, an expression **Paul Ehrenfest** created later in 1911, happened with the Rayleigh-Jeans law also proposed in 1900, which was trying to predict the shape of the light spectrum with the black body temperature. It was diverging to infinite values as the temperature was growing. Planck's law solved the problem and avoided the ultraviolet catastrophe. He found his spectrum equation empirically and only then, a related explanation based on harmonic oscillators and energy quanta exchanged between the radiation and the black-body "wall". For this work, Max Planck was awarded the Nobel Prize in Physics in 1918.

We also owe him the constant which bears his name ( $\hbar$ ) and which is used in his blackbody radiation equation. The Planck constant ( $6.626 \times 10^{-34}$  Js) was then used in the equation according to which atomic state energy shifts equals to the radiation frequency multiplied by Planck's constant. The constant appears in most quantum physics equations (De Broglie, Schrödinger, Dirac, etc).

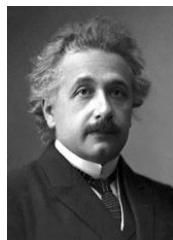
When an electron changes its orbit in a hydrogen atom, it emits or absorbs an electromagnetic wave whose energy is equal to Planck's constant multiplied by the emitted light frequency. Despite the numerous experimental validations carried out a few years later, Max Planck expressed until his death a lot of doubts about the very principles of quantum physics!

Planck is also at the origin of several infinitesimal constants: Planck time, which is  $t_P = 10^{-44}$  s and Planck distance which is  $l_P = 1.616255 \times 10^{-35}$  m. Planck's time is the time it would take for a photon to travel the Planck distance.



These are the dimensions of the infinitely small below which any observation would be impossible. The length of Planck  $l_P$  is so small that a photon used to observe it would have such a high frequency and energy that it would generate a black hole around it and would therefore become unobservable!

At last, Planck mass is the maximum mass of an elementary particle. A particle with this mass and the size of Planck's distance would be a black hole. These are quite extreme physics. In today's classical cosmology, Planck's wall corresponds in the history of the expansion of the Universe to the moment when  $10^{-43}$  s after the big bang, its size would have been  $10^{-35}$  m, which is respectively the Planck time and Planck distance.



**Albert Einstein** (1879-1955, German then American) got his Nobel Prize in 1921 for his interpretation of the photoelectric effect in 1905, which became one of the foundations of quantum mechanics after Planck and before De Broglie, Heisenberg and Schrödinger. Einstein determined that Planck's quanta are elementary grains of energy  $E = h\nu$  (Planck constant times frequency) with a momentum of  $p = Hv/c$ <sup>23</sup>. These were named “photons” in 1926 by **Gilbert Lewis** (1875-1946, American). Symbolically, 1905 is also the year of Jules Verne’s death.

Symmetrically to what Louis De Broglie would later do with electrons, he hypothesized that a photon behaves both as a wave and as a particle.

<sup>23</sup> In [On a Heuristic Viewpoint Concerning the Production and Transformation of Light](#), 1905.

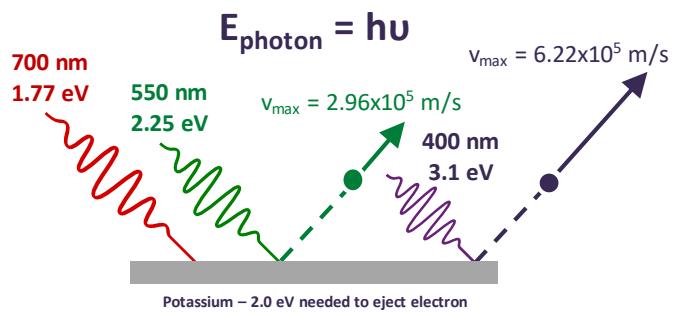
This was coming out of just one out of his four 1905 “annus mirabilis” papers sent between March and June to *Annalen der Physik*, the others being on special relativity, Brownian motion and mass-energy equivalence, published when he was just 26. On top of his own 24 pages PhD thesis on a theoretical method to calculate molecular sizes using fluid mechanics and hydrodynamics.

With the photoelectric paper, he reconciled the corpuscular theories of **René Descartes** (1596-1650, French, in 1633) and **Issac Newton** (1642-1726, English, in 1704) with the wave-based theories of **Christiaan Huygens** (1629-1695, Dutch, in 1678) to describe light.

This was followed by the works from **Augustin-Jean Fresnel** (1788-1827, French), **Léon Foucault** (1819-1868, French, who measured first the speed of light), **Hippolyte Fizeau** (1819-1896, French, who co-discovered the Doppler effect) and of course **James Clerk Maxwell**.

The photoelectric effect corresponds to the capacity of a photon to dislodge an electron from a generally inner orbit of an atom and to create some electric current<sup>24</sup>.

It is exploited in the cells of silicon-based photovoltaic solar panels. It also explains photosynthesis in plants, which is the metabolic starting point of glucose production.



In addition to Max Planck's work on black body radiation, Einstein's interpretation was based on the earlier work of **Heinrich Hertz** (1857-1894, German) who discovered in 1887 that light can extract an electron out of metal, and **Philipp Lenard** (1862-1947, German) who, in 1902, studied the photoelectric effect and determined that it is only triggered at a certain frequency for the projected light. The latter was awarded the Nobel Prize in Physics in 1905. Becoming a fervent Nazi and opposed to Einstein by scientific rivalry and then by explicit anti-Semitism, he mostly disappeared from quantum physics hall of fame.

Einstein's photoelectric effect equations were then verified by the experiments of **Robert Andrews Millikan** (1868-1953, American) between 1909 and 1914. It enabled him to measure the electric charge of a single electron, which earned him the Nobel Prize in Physics in 1923.

Of course, Einstein is also at the origin of the special and general theories of relativity. He didn't obtain a Nobel Prize for his work on relativity despite its considerable impact on science.

This is due, among other things, to his theories being based on earlier work from **Heindrick Lorentz** and **Henri Poincaré** as well as the contribution of his former professor **Hermann Minkosvki** (1864-1909, German) who created the four-dimensional space-time notion in 1908.

On top of many other contributions in quantum physics, Einstein predicted the photons stimulated emission effect in 1917, that would later lead to the creation of lasers. He also predicted in 1925 a particular behavior of matter, the Bose-Einstein condensate, which occurs when gases are cooled to very low temperatures. Atoms are then in a minimum energy quantum state showing particular physical properties.

<sup>24</sup> The electron layers of the atoms are numbered from 1 to N, their quantum number. One also starts the numbering by K (first layer close to the nucleus with a maximum of 2 electrons) then L (8 electrons maximum), M (with a maximum of 18 electrons but in practice 8), etc.. The photoelectric effect mainly concerns the layers K and L. The ejected electron is then replaced by an electron of external orbit, which generates a new photon, in X-rays or in fluorescence, according to the energy of the incident photon. This then emits an X-ray photon due to the energy differential between electronic layers or an electron called "Auger" from the name of Pierre Auger. This phenomenon was discovered around 1923 by the latter and by Lise Meitner. Another variant of the photoelectric effect is the Compton effect, when the high energy of an incident photon in gamma rays will release an electron from the valence layer and generate another photon. Finally, when the energy of the incident photon is even higher, the interaction takes place at the nucleus of the target atom and generates an electron and a positron.

This is the case of superfluid helium, discovered in 1938, which is superfluid at very low temperatures, i.e. it can move without dissipating energy. Bose is the name of **Satyendra Nath Bose** (1894-1974, India) with whom Einstein had worked during the 1920s and to whom we owe the "bosons", which verify the characteristics of Bose-Einstein's condensates.

Bosons include elementary particles without mass such as photons and gluons but also certain atoms such as deuterium or Helium 4 as well as certain quasi-particles such as the superconducting electron pairs that are Cooper's pairs. We will see a little later that it is a question of the spin sum of these particles that determines the fact that they are bosons as opposed to fermions.

Albert Einstein also contributed to the philosophical-scientific debates on quantum physics realism, confronting Niels Bohr. He focused on the fact that quantum physics did not seem to completely describe the physical world with its probabilistic bias.

Einstein wanted to find a realistic interpretation of physics. He could not be satisfied with a probabilistic description of the state of electrons and other quantum objects. He could not find sufficient the interpretation of quantum physics according to which the observer and the measurement "make" the real world. He thought that the real world exists independently of measurements and observers.

The debate between Albert Einstein and Niels Bohr revolved around various thought experiments on determinism discussed during the 1927 Solvay Congress.

MAY 15, 1935

PHYSICAL REVIEW

VOLUME 47

## Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in

quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

It culminated later, in 1935, with the famous **EPR paradox** paper, named after its authors Albert Einstein, Boris Podolsky and Nathan Rosen. The paper raised the question of the incompleteness of quantum mechanics at the time<sup>25</sup>.

It sought to explain the non-locality of quanta allowing an instantaneous action at distance between two quanta via entanglement. This non-locality was the consequence of Schrödinger's wave function<sup>26</sup>. It was not yet physically observed in 1935. For the authors, the quantum theory based on Schrödinger's wave function was either incomplete or two quanta could not be instantaneously synchronized at a distance. For them, a physical theory is complete if each component of reality has a counterpart in the theory that allows us to predict its behavior, such as a tuning at the source (entangled quanta) modeling itself with hidden variables. This underlies the notion of determinism, a principle absent from Schrödinger's wave function.

<sup>25</sup> See [Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?](#), by Albert, Einstein, Boris Podolsky and Nathan Rosen 1935 (4 pages).

<sup>26</sup> Einstein's landmark was classical and relativistic physics that acted locally. Gravity is local and is transmitted at the speed of light. All physical theories before quantum physics were local or EPR-local. Remote actions all involve a delay, usually coupled with attenuation with distance as it's the case for gravity.

The EPR paper ends with indicating that it should be possible to build a complete theory of quantum mechanics<sup>27</sup>. Einstein was then often credited with the idea that there were hidden variables. It seems, however, that he never mentioned them in his writings despite what John Bell said. The explanation of entanglement by "hidden variables" comes rather from Louis de Broglie with his pilot wave hypothesis elaborated in 1927, an idea later pursued by David Bohm in the 1950s<sup>28</sup>.

With his "inequalities", John Stewart Bell demonstrated in 1964 that the existence of such hidden variables was incompatible with the principles of quantum mechanics. Alain Aspect's 1982 experiment on photon entanglement confirmed this hypothesis.

In the end, Einstein could not finish his work on his theory of general relativity which was, for him, as incomplete as quantum mechanics. In particular, he wanted to reconcile quantum mechanics and gravity.

Be careful with the simplistic views that Einstein was against quantum mechanics or did not believe in it<sup>29</sup>. He first questioned the principle of indeterminacy in 1927 and 1930, then estimated that the theory was incomplete to explain entanglement, with the EPR paradox paper published in 1935, and finally, he opposed the lack of realism of quantum theory. This incompleteness is still being discussed more than 80 years later. The origins of entanglement are still not physically explained under certain conditions, particularly with long distance. It is simply observed physically and described mathematically<sup>30</sup>. This remains an open debate as scientists continue to ponder the different possible interpretations of quantum physics. This is part of the field of [quantum foundations and quantum physics philosophy](#) that we cover later in this ebook (page 744).



**Niels Bohr** (1885-1962, Danish) was a physicist, Nobel Prize in Physics in 1922, who created in 1913, aged 28, a descriptive model of the hydrogen atom with its nucleus made of a proton and an electron rotating around the nucleus on precise orbits corresponding to levels of kinetic energy, multiple of  $h/2\pi$ ,  $h$  being Planck's constant and  $n = 1, 2, 3$  and so on. This model explained hydrogen spectral lines observed in the experiments of **Johann Balmer** (1825-1898) in 1885, **Theodore Lyman** (1874-1954) in 1906 and **Friedrich Paschen** (1865-1947) in 1908.

It also explained why electrons didn't crash on atom nucleus! Niels Bohr followed the work of **Ernest Rutherford** (1871-1937) who discovered in 1911 the structure of atoms with their positively charged nucleus, thanks to its protons, and their electrons revolving around the nucleus. The latter, with whom Niels Bohr was doing his post-doc in 1911, relied himself on **Hantaro Nagaoka** (1865-1950, Japan) who predicted in 1903 the structure of atoms with a positively charged nucleus and negatively charged electrons revolving around it, called the "Saturnian model".

<sup>27</sup> The 1935 New York Times article was published thanks to a "leak" provoked by Boris Podolsky, the youngest of the EPR 3 gang.

<sup>28</sup> See [Albert Einstein, David Bohm and Louis de Broglie on the hidden variables of quantum mechanics](#) by Michel Paty, 2007 (29 pages) which sets the record straight on Albert Einstein's position on the subject of hidden variables. The author, born in 1938, is a physicist and a philosopher of science.

<sup>29</sup> This story is well told in [Einstein and the Quantum - The Quest of the Valiant Swabian](#) by A. Douglas Stone, 2013 (349 pages).

<sup>30</sup> See the abundant [Einstein Bohr debates](#) and [Interpretations of quantum mechanics](#) pages on Wikipedia, from which the table on the next page is taken.

**The New York Times.**

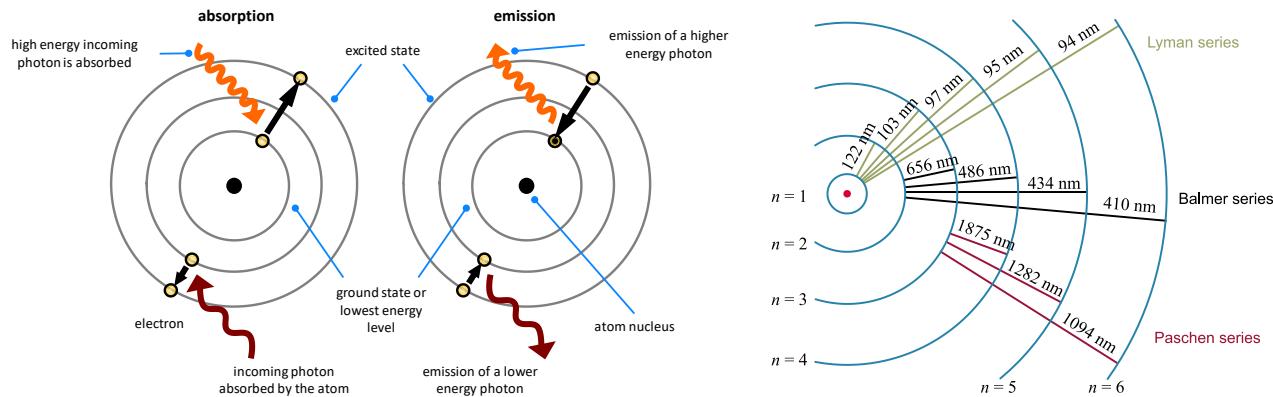
Copyright, 1935, by The New York Times Company.  
NEW YORK, SATURDAY, MAY 4, 1935. • P TWO CENTS

---

**EINSTEIN ATTACKS  
QUANTUM THEORY**

Scientist and Two Colleagues  
Find It Is Not 'Complete'  
'Even Though 'Correct.'

Electrons had been discovered by **Joseph John Thomson** (1856-1940, English) in 1897 by analyzing the rays emitted by a cathode in a cathode ray tube (CRT), deflected by an electric field as well as by a magnetic field, and detected by a layer of phosphorus. He was awarded the Nobel Prize in Physics in 1906.



Ernest Rutherford had also imagined the existence of neutrons, which was not verified experimentally until 1932 by **James Chadwick** (1891-1974, English). **Marie Curie** (1867-1934, Polish and French) had discovered polonium and radium in 1898 and some effects of radioactivity but not the existence of neutrons.

According to Niels Bohr, electrons emit or absorb a photon when they change orbit. Subsequently, Louis de Broglie's work on wave-particle duality interpreted that the orbits of the electrons were an integer multiple of their associated wavelength.

Together with Werner Heisenberg, Pascual Jordan and Max Born, Niels Bohr is at the origin of the so-called **Copenhagen** interpretation of quantum physics which is based on three key principles<sup>31</sup> :

- The description of a wave-particle is realized by its wave function, and no other "hidden" information or variable can be used to describe its state. We must accept the wave function probabilistic used to describe a quantum state.
- When a quantum state measurement is performed, its composite wave function of several states is reduced to the wave function of one of the possible states of the quantum. This is the collapse of the wave function.
- When two properties are linked by an uncertainty relationship, the two properties cannot be measured with a greater precision than that allowed by the uncertainty relationship (Heisenberg principle of indeterminacy). Moreover, when we measure the position of a particle, we affect its motion, and vice versa.

This is the main interpretation of quantum mechanics. There are many other interpretations available, listed below in a table coming from Wikipedia. We will have the opportunity to detail the interpretation of Copenhagen towards the end of the ebook in the part dedicated to the [philosophy of quantum physics](#), page 744.

<sup>31</sup> See also Richard Webb's [Seven ways to skin Schrödinger's cat](#), 2016 which describes the different schools of thought in quantum physics. See also other interpretations of quantum physics in Ethan Siegel's [The Biggest Myth In Quantum Physics Starts With A Bang](#) in Forbes, 2018.

Interpretation	• Year published •	Author(s)	• Deterministic? •	Ontologically real wavefunction?	Unique history?	Hidden variables?	Collapsing wavefunctions?	Observer role?	Local dynamics?	Counterfactually definite?	Extant universal wavefunction?
Ensemble interpretation	1926	Max Born	Agnostic	No	Yes	Agnostic	No	No	No	No	No
Copenhagen interpretation	1927	Niels Bohr, Werner Heisenberg	No	No <sup>1</sup>	Yes	No	Yes <sup>2</sup>	Causal	Yes	No	No
de Broglie–Bohm theory	1927-1952	Louis de Broglie, David Bohm	Yes	Yes <sup>3</sup>	Yes <sup>4</sup>	Yes	Phenomenological	No	No	Yes	Yes
Quantum logic	1936	Garrett Birkhoff	Agnostic	Agnostic	Yes <sup>5</sup>	No	No	Interpretational <sup>6</sup>	Agnostic	No	No
Time-symmetric theories	1955	Satoshi Watanabe	Yes	No	Yes	Yes	No	No	No <sup>56</sup>	No	Yes
Many-worlds interpretation	1957	Hugh Everett	Yes	Yes	No	No	No	No	Yes	Ill-posed	Yes
Consciousness causes collapse	1961-1993	John von Neumann, Eugene Wigner, Henry Stapp	No	Yes	Yes	No	Yes	Causal	No	No	Yes
Stochastic interpretation	1966	Edward Nelson	No	No	Yes	Yes <sup>14</sup>	No	No	No	Yes <sup>14</sup>	No
Many-minds interpretation	1970	H. Dieter Zeh	Yes	Yes	No	No	No	Interpretational <sup>7</sup>	Yes	Ill-posed	Yes
Consistent histories	1984	Robert B. Griffiths	No	No	No	No	No	No	Yes	No	Yes
Transactional interpretation	1986	John G. Cramer	No	Yes	Yes	No	Yes <sup>9</sup>	No	No <sup>12</sup>	Yes	No
Objective collapse theories	1986-1989	Ghirardi–Rimini–Weber, Penrose Interpretation	No	Yes	Yes	No	Yes	No	No	No	No
Relational interpretation	1994	Carlo Rovelli	No <sup>56</sup>	No	Agnostic <sup>9</sup>	No	Yes <sup>10</sup>	Intrinsic <sup>11</sup>	Yes <sup>57</sup>	No	No
QBism	2010	Christopher Fuchs, Ruediger Schack	No	No <sup>16</sup>	Agnostic <sup>17</sup>	No	Yes <sup>18</sup>	Intrinsic <sup>19</sup>	Yes	No	No

Note that Niels Bohr's son, **Aage Niels Bohr** (1922-2009, Danish), was awarded the Nobel Prize in Physics in 1975 for his work on the structure of atom nucleus<sup>32</sup>!



**Emmy Noether** (1882-1935, German) is the creator of the theorem that bears her name in 1915 at the University of Göttingen in Germany<sup>33</sup>. At the origin of the field of abstract algebra, it is a foundation to Lagrangian mechanics, precursor of Hamilton's theory. At that time, she could not teach at the University because this role was forbidden to women. Her theorem was only published in 1918 and she could not officially teach until 1919.

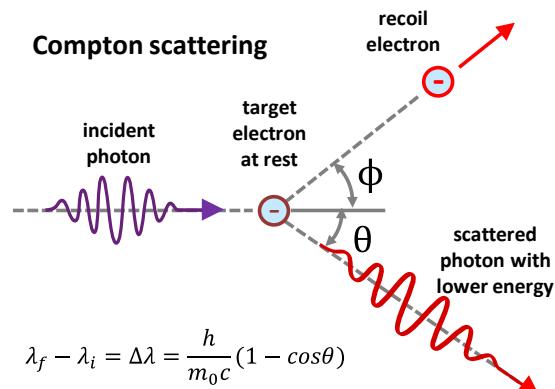
She did not receive a salary from the University until 1923. Her theorem links conservation principles and symmetries. It is one of the foundations of particle physics. Her work helped Albert Einstein to refine the foundations of the theory of general relativity he developed in 1915<sup>34</sup>. She died relatively young, at 53.

$$\frac{d}{dt} \left( \sum_a \frac{\delta L}{\delta \frac{dq_a}{dt}} \delta q_a \right) = 0$$



**Arthur Holly Compton** (1892-1962, American) was a physicist who got the 1927 Nobel Prize in physics for the discovery in 1922/1923 of the effect which demonstrates that photons can have momentum and behave as particles. His experiment makes a photon interact with a free electron around an atom, validating the photoelectric effect theories of Planck and Einstein. The Compton effect is a variant of this effect, applied to X and gamma rays which are high energy photons.

Compton scattering deals with the reception of an X or gamma photon which has an energy higher than that of the ejected electron. The X ray photon is slowed down and deflected with a lower energy and becomes a scattered photon. This is also called an elastic shock. The effect is used in X-ray radios. X-rays are emitted during electronic transitions between the atomic layers K, L and M (the first around the nucleus of the atom). The emission angles of the ejected electron and the re-emitted photon depend on the energy level of the incident photon.



$$\lambda_f - \lambda_i = \Delta\lambda = \frac{h}{m_0 c} (1 - \cos\theta)$$

<sup>32</sup> See [Quantum Model of the Atom](#) by Helen Klus, 2017.

<sup>33</sup> See [In her short life, mathematician Emmy Noether changed the face of physics](#) Noether linked two important concepts in physics: conservation laws and symmetries by Emily Conover, 2018.

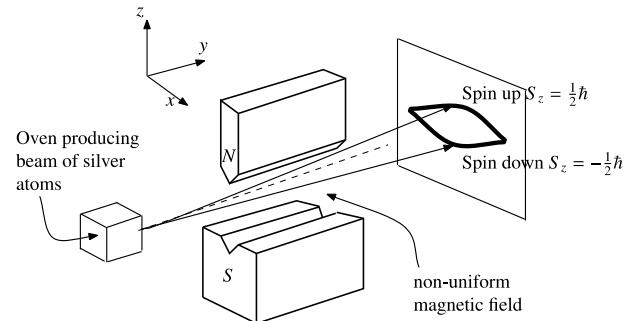
<sup>34</sup> See [Women in Science: How Emmy Noether rescued relativity](#), by Robert Lea, February 2019.



**Otto Stern** (1888-1969, German-American) and **Walther Gerlach** (1889-1979, German) respectively conceived in 1921 and together realized in 1922 in Frankfurt the famous Stern-Gerlach experiment which discovered the angular momentum quantization in a magnetic field using a beam of electrically neutral silver atoms<sup>35</sup>. In the experiment, this momentum came from the 47<sup>th</sup> electron spin from heated silver atoms.



It did show that these atoms have a quantized angular dipole that deflects the beam in a given direction upward or downward. It later became known as particle spins. It did show that spin measurement along a given direction was incompatible with being done in another direction.



**Jacques Salomon Hadamard** (1865-1963, French) was a mathematician who gave his name to the Hadamard gate used in quantum computers and quantum algorithms. He had worked on complex numbers, differential geometry and partial differential equations, particularly during the 1920s. He also became interested in the creative process of mathematicians with studying the creative process of hundreds of colleagues.

We owe him in particular the Hadamard transforms, square matrix operations with  $2^n$  complex or integer values on each side. The quantum gate named after Hadamard is used in quantum computation to create a superposition of the states  $|0\rangle$  and  $|1\rangle$  with a transform of Hadamard type H1.

This superposition enables computing parallelism in quantum computing, in addition to the principle of entanglement which links the qubits together conditionally and is the real source of quantum exponential acceleration. Superposition is only responsible for a potential polynomial acceleration.

$H_0=1$

$$H_1=\frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$H_2=\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$H_3=\frac{1}{2^{3/2}}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$



**Louis de Broglie** (1892-1987, French) was a mathematician and physicist who, in 1923 and 1924, extended the particle-waves duality, then only applied to photons, to massive particles, mainly electrons, and also atoms, protons and neutrons<sup>36</sup>. According to this principle, elementary particles behave like particles (with a position, a trajectory and possibly a mass) and like waves (potentially delocalized and scattering in all directions and generating interference) depending on the circumstances.

<sup>35</sup> Illustration coming from: [Chapter 6, Particle Spin and the Stern-Gerlach Experiment](#). See [Stern and Gerlach, how a bad cigar helped reorient atomic physics](#) by Bretislav Friedrich and Dudley Herschbach, Physics Today, December 2003 (7 pages). The X, Y and Z components of the electron spin measured in the Stern-Gerlach experiment are complementary variables. Measuring one of the three variables prevents from doing so with the two others.

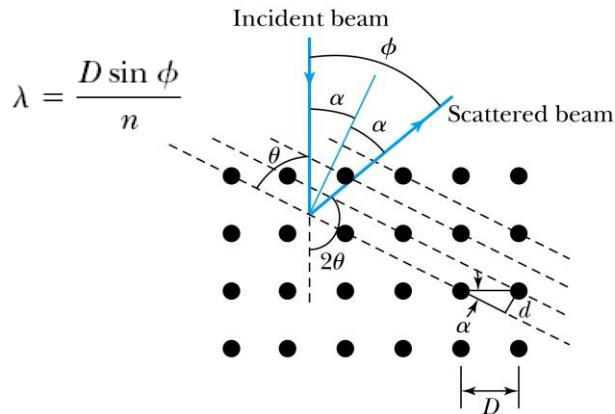
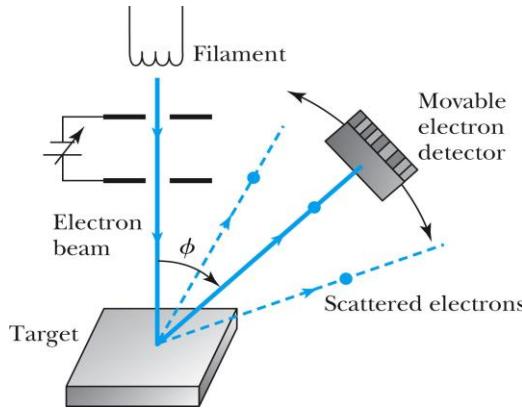
<sup>36</sup> Louis de Broglie's brother, Maurice de Broglie (1875-1960), was also a physicist. He had studied X-rays and spectrography. Both brothers were members of the Academy of Sciences in France.

This is the case of electrons which have a mass and can interfere with each other. Louis de Broglie turned this duality into an equation:  $\lambda p = h$ , where  $\lambda$  is a wavelength,  $p$  is a quantity of motion and  $h$  is Planck's constant.

This earned him the Nobel Prize in Physics in 1929. He is the main French contributor to quantum physics during the inter-war period. The wave-particle duality of electrons was confirmed in 1927.

particle energy	$E = hv$	wave frequency
particle momentum	$p = \frac{h}{\lambda}$	Planck constant wave length

De Broglie wave-particle equation for electrons, 1924



It was done with a nickel crystal based diffraction experiment by **Clinton Davisson** (1881-1958) and **Lester Germer** (1896-1971) from the Bell Labs in the USA, who shared a Nobel Prize in Physics in 1937 ([illustration source](#)).

**George Paget Thomson** (1892-1975) from the University of Aberdeen in Scotland did a similar experiment also in 1927. However, the Young double-slit experiment done with electrons was realized much later, in 1961, by **Claus Jönsson** (1939, German).

The confirmation of the wave-particle duality was then verified for neutrons much later in 1988 by **Roland Gähler** and **Anton Zeilinger** ([source](#)) and for atoms in 1991 by **Olivier Carnal** and **Jürgen Mlynek** ([source of](#) the diagram *on the right below*). It is even verifiable with molecules of several atoms.



**Wolfgang Pauli** (1900-1958, Austrian/American) is at the origin of the principle of exclusion which bears his name elaborated in 1925 and according to which two electrons cannot have the same quantum state in an atom. He took part in the discovery of electron spin between 1925 and 1927, as well as the neutrino in 1930, the existence of which was only experimentally proven in 1956, and on works on quantum electrodynamics. He was awarded the Nobel Prize in Physics in 1945. The history of his discoveries is more complex than it seems.

He first discovered in 1924 the atom nucleus spin, used to explain the hyperfine structure of atomic spectra, i.e. the existence of very close spectral lines observed during their excitation. It cannot be explained by the quanta and energy levels of the electron layers in the atoms. He then introduced in 1925 a new degree of freedom for electrons that he did not qualify at first.

It adds to the first three parameters describing the state of an electron in an atom, aka quantum numbers.

The first is the energy level of the electron in the atom (the layer where it is located), the second is the azimuthal quantum number (which defines the electron sub-layer) and the third is the magnetic quantum number (which makes it possible to distinguish the orbitals of the electron in the atom)<sup>37</sup>. This fourth degree of freedom was identified by **George Uhlenbeck** (1900-1988, Netherlands/USA) and **Samuel Goudsmit** (1902-1978, Netherlands/USA) as an electron spin<sup>38</sup>.

In 1925, Wolfgang Pauli also formulated the exclusion principle according to which electrons in the same system (an atom) cannot be simultaneously in the same quantum state, a principle that was later extended to all fermions, i.e. half-integer spin particles (electrons have a spin  $\frac{1}{2}$  but fermion atoms can have  $3/2$ ,  $5/2$ ,  $7/2$  and even  $9/2$  spins, like  $^{40}\text{K}$ ).

The quantum state of an electron is defined with the four quantum numbers, or degrees of freedom, that we have just mentioned.

An electron spin is described as a direction of magnetic polarization or as an angular rotation of the electron in one direction or the other, but it is only an image and not a physical representation<sup>39</sup>. Electron spins are used in silicon qubits that we cover later, starting page 281.

137 is a number that played a weird role in Pauli's life. It turns out that  $1/137$  is a value that roughly corresponds to the fine-structure constant, a ratio that is found in many places in quantum physics and compares data of the same dimension<sup>40</sup>. It is for example the ratio between the velocity of an electron in the lower layer of a hydrogen atom and the speed of light or the probability of emission of the absorption of a photon for an electron. 137 is a bit like 42 in quantum physics ([complete list](#)). And Pauli died after some pancreatic cancer surgery, while his hospital room number was 137!



**Erwin Schrödinger** (1887-1961, German) is a physicist who was awarded the Nobel Prize in 1933 for the creation of his famous wave function in 1926, aka Schrödinger equation, which describes the evolution in time and space of the wave state of a massive quantum particle, i.e. the probabilities of finding the quantum at a given place and time. Schrödinger's equation is a variant of the Newtonian mechanics equations that define the total energy of an object as the sum of its kinetic energy and its potential energy.

Erwin Schrödinger is also credited with his famous and somewhat convoluted thought experiment to explain the notion of superposition with his alive and dead cat in a box<sup>41</sup>. The box contains a vial of poison, the opening of which is caused by the disintegration of a radioactive radium atom via a Geiger counter detecting some ionizing radiation.

<sup>37</sup> The second and third electron quantum numbers were introduced by Arnold Sommerfeld (1868-1951, German). Among others, Wolfgang Pauli and Werner Heisenberg were his PhD students. The alpha constant or fine structure constant is also called the Sommerfeld constant per his work from 1916! See [Electron spin and its history](#) by Eugene D. Commins, May 2012 (28 pages).

<sup>38</sup> Georges Uhlenbeck and Samuel Goudsmit were students of Paul Ehrenfest (1880-1933, Austria/Netherlands). His laboratory had welcomed some illustrious future physicists such as Enrico Fermi, Robert Oppenheimer, Werner Heisenberg and Paul Dirac. Ehrenfest was a specialist in statistical physics. In particular, he contributed to the understanding of phase changes in matter.

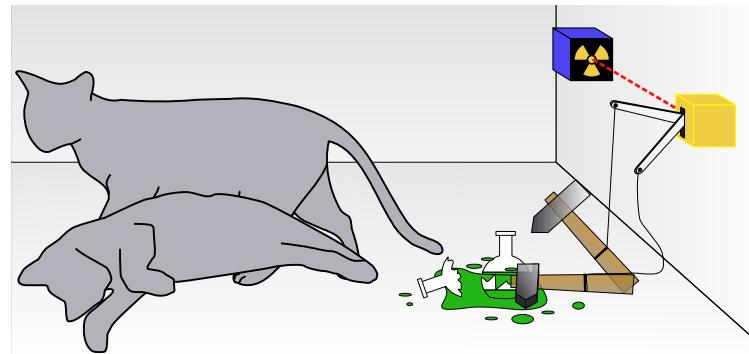
<sup>39</sup> See [How Electrons Spin](#) by Charles T. Sebens, California Institute of Technology, July 2019 (27 pages) which provides a good background on electron spin's physical interpretations, particularly with regards to electron's size.

<sup>40</sup> The fine-structure constant was measured with a precision of  $2.0 \times 10^{-10}$  in 2020 using cold atoms interferometry. See [Determination of the fine-structure constant with an accuracy of 81 parts per trillion](#) by Léo Morel, 2020 (36 pages).

<sup>41</sup> The Cat Thought Experiment was published in a series of three papers in 1935, shortly after the publication of the EPR paradox by Einstein, Podolsky and Rosen. See [The Present Status of Quantum Mechanics](#) by Erwin Schrödinger, 1935 (26 pages). The history of the cat occupies only nine lines in this long document which deals with the question of superposition, measurement and entanglement. That's even where Schrödinger coined the term entanglement in the first chapter "*The Lifting of Entanglement. The Result Depends on the Will of the Experimenter*". Schrödinger translated himself the German word Verschränkung into entanglement. The cat that appears only three times in all and for all is therefore anecdotal but that is what everyone has retained. Which is quite normal: the rest is much less easy to apprehend!

The radiation is made of alpha particles, comprising two protons and two neutrons. It is the equivalent of a helium 4 atom without its electrons. Since radium has a 50/50 chance of disintegrating after its half-life, the cat has a 50/50 chance of being alive and dead, at this half-life period, as long as the box is not opened. When opened, it is either alive or dead. As long as the door is not opened, it is supposed to be superposed in the alive and dead states.

The problem is a cat can't be superposed in two states because it's a macro-object. It's either alive or dead, not both. On top of that, the radium atom disintegration as well as the cat's death are both irreversible processes. They can't be implemented as linear superpositions of waves. When the cat is dead, he's dead, not in a superposition.



The uncertainty about the cat state is a classical one, not a purely indeterministic quantum state. If you were to use a webcam inside the box and making sure it didn't influence the radium half-life period, you could trace the cat state all along, from alive to dead or alive to alive, which are the only two available paths<sup>42</sup>. The cat is beyond the quantum-classical frontier, in the classical realm.

Let's make a parallel with lotteries. When the numbers are drawn and you don't know yet the result because you are not connected online, your lack of knowledge about it is classical and not quantum. Even if the lottery numbers were generated by some quantum random number generator (QRNGs)! We could make a parallel with quantum states: when results are drawn and you don't know them yet, these are in a mixed state without any coherence and superposition (we'll define these notions later). So, not in a pure and superposed state and with no superposition between "winner and loser", on top of the usual low chance to win in this game. For the Schrödinger's cat experiment to be truly quantum, it would eventually have to be based on a radium atom passing through a semi-reflecting mirror with a 50/50 chance of passing through it in a quantum frame, in which case we would get closer to a quantum interpretation<sup>43</sup>.

Let's not forget that this thought experiment was intended to highlight the fact that superposition only applied to the infinitely small and not to macroscopic objects. History has retained the principle of superposition and not this difference between microscopic and macroscopic worlds.

Let's forget about the cat anyway and retain Schrödinger's wave function and the notion of states superposition which only makes sense on a microscopic scale. In his private life, Schrödinger was a great womanizer. He was even capable of having several liaisons at the same time, applying the principle of quantum superposition to his private life.



**Max Born** (1892-1970, German) is a physicist and mathematician who developed the mathematical representation of quantum in a matrix form. We owe him in 1926 the statistical explanation of the probability of finding an electron in a given energy state from its wave function, elaborated by Schrödinger the same year. This principle is applied to qubits, where the sum of the square of the probabilities of the two states of the qubit is equal to 1, given the probabilities are complex numbers.

<sup>42</sup> You can apply this thought experiment to the baking of the half-cooked chocolate. As long as you don't take it out of the oven after the mandatory baking of 9 minutes, but with an oven with an unknown power, you don't know if it is well done or not, and run it through the middle before you take it out. It is in a state of superposition between undercooked, well done and overcooked. On the other hand, if it is overcooked, it will be difficult to go back, like Schrödinger's half-dead cat in case he died. Overcooking as well as the death of the cat are irreversible. It is therefore not a true superposition of quantum states. Cheers!

<sup>43</sup> The interpretation on disintegration can be found in [Schrödinger's cat Wikipedia entry](#).

In 1925, he created the non-commutativity relation of two conjugate quantities, one being the Fourier transform of the other (the commutator  $[X,P]=XP-PX=i\hbar I$ , where  $X$  is a position and  $P$  a momentum and  $I$ , the identity). It led to the indeterminacy principle creation. He also created the first version of the adiabatic theorem with Vladimir Fock in 1928. He got the Nobel prize in physics in 1954. Fun fact, the British singer Olivia Newton-John is his grand-daughter<sup>44</sup>.



**Werner Heisenberg** (1901-1976, German) is a physicist, Nobel Prize in Physics in 1932, to whom we owe in 1927 the creation of the famous principle of uncertainty, or rather indeterminacy, according to which one cannot accurately measure both the position and the velocity of an elementary particle, or, more generally, two arbitrary unrelated quantities. Above all, he is at the origin, with Max Born and Pascual Jordan in 1925, of the quantum matrix formalism describing physical quantities.

The indeterminacy principle is a consequence of this formalism. It was described mathematically in a simplified manner in 1928 by **Earle Hesse Kennard** (1885-1968, American) in the famous equation, where the product of the standard deviation of position and velocity is greater than half the Dirac constant.

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

This principle can be used to improve the accuracy of a measurement of any quantity by lowering the accuracy of another quantity characterizing a quantum<sup>45</sup>. These quantities can be for example an energy level, a position, a wavelength or a speed.

One consequence of Heisenberg's principle is that all particles in the Universe are in constant motion. If they were stable, we would know their position (fixed) and their velocity (zero), violating the indeterminacy principle.

Another consequence is that a perfect vacuum could not exist because the value and evolution of the magnetic and gravitational fields that pass through it would be stable, violating once again Heisenberg's indeterminacy. This explains the astonishing vacuum quantum fluctuations we discover a [little further](#). The non-cloning theorem of a qubit state also derives from the principle of indeterminacy.

For some, this indeterminacy principle is a simplified interpretation of the corpuscular nature of matter. It leads to the question of the position and velocity of an electron, when it has no precise position. According to the Copenhagen interpretation of quantum mechanics, we shouldn't try to determine where the electron is located. Try to apply the concepts of classical mechanics to electrons is vain.

In practice, quantum particles are not classical physical particles and therefore their velocity and position cannot be measured. They can only be described by their (Schrödinger) wave function. More generally, in the infinitely small, the measurement device influences the quantity to be measured. The example on the right illustrates this phenomenon at the macroscopic level: if you illuminate an insect with sunlight and a magnifying glass to better observe it, you may burn it<sup>46</sup>! The same happens with a photon used to detect an electron, in the Heisenberg microscope thought experiment.



<sup>44</sup> See [Olivia Newton-John's grandfather Max Born was friend of Albert Einstein](#) by Matthew Alice, 1995.

<sup>45</sup> This measurement technique is used in "quantum squeezing" which is integrated in the latest version of LIGO for the measurement of gravitational waves: [NIST Team Supersizes 'Quantum Squeezing' to Measure Ultra Small Motion](#), 2019.

<sup>46</sup> Image source: [It's only when you look at an ant through a magnifying glass on a sunny day that you realise how often they burst into flames](#).

Finally, like many of the colleagues of his time, Werner Heisenberg was interested in the links between science, quantum mechanics and philosophy, and as early as 1919. He was assistant to Niels Bohr between 1924 and 1927, before leaving for the University of Leipzig. He also had Max Born as a professor!

During World War II, he was asked with other German scientists to work on the Reich's atomic bomb project. Later revelations did show that he was not very active on this project and did not believe it was an achievable goal.



**Paul Dirac** (1902-1984, English) is a mathematician and physicist among the founders of 20th century quantum physics. He is credited with the 1928 electron spin equation, which is one of the foundations of relativistic quantum physics (*below*). His equation is a kind of variant of Schrödinger's equation for free relativistic particles, fermions (electrons, protons, neutrons, quarks, neutrinos) which are half-integer spin particles. Relativistic particles are those moving at a speed close to the speed of light.

In Dirac's equation, the wave function of the electron  $\psi$  includes four components of complex numbers that integrate time and space.

Dirac's equation enabled him to predict the existence of a particle that was later be called the positron, an opposite of the electron with a positive charge<sup>47</sup>.

$$\left( \beta mc^2 + c \sum_{n=1}^3 \alpha_n p_n \right) \Psi(x, t) = i\hbar \frac{\partial \Psi(x, t)}{\partial x}$$

Dirac formalized the quantization of the free electromagnetic field in 1927. He also introduced in 1939 the bra-ket notation, known as Dirac's notation, which simplified the notation and manipulation of quantum states and operators in linear algebra (example:  $\langle \phi | \psi \rangle$ ).

The Dirac constant also named reduced Planck constant is otherwise the Planck constant  $h$  divided by  $2\pi$ , also called "h-bar" for its italicized strikethrough h symbol:  $\hbar$ . This Dirac constant is used in the Schrödinger wave function that we have already detailed.

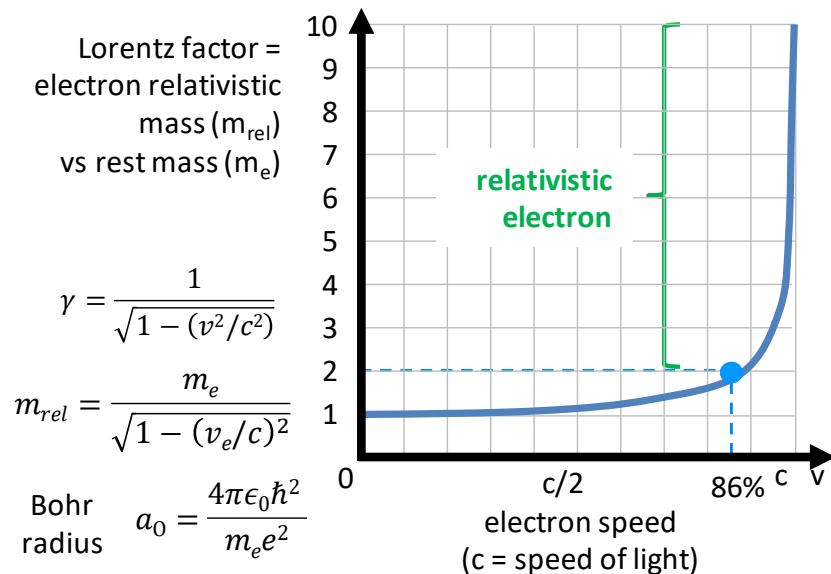
Paul Dirac was awarded the Nobel Prize in Physics in 1933, at the age of 31. The Nobel Prizes of the early 20th century were frequently awarded to young scientists, which seems to be out of fashion since then! The youngest Nobel Prize in Physics was awarded to Lawrence Bragg, who won it at the age of 25 in 1915 for his discovery of X-ray refraction at the age of 22<sup>48</sup>.

In which case do we have to deal with relativistic particles, in particular with electrons? It is generally considered that an electron becomes relativistic when the total of its mass and kinetic energy is at least twice the rest mass. This ratio corresponds to the [Lorentz factor](#). It represents a speed of at least 86% of the speed of light. But relativistic phenomena may occur before that speed is reached. In Newtonian equivalent, the speed of an electron around the nucleus of a hydrogen atom is about c/137. With electrons from heavy atoms inner shells, this velocity can exceed c/2.

This is the case for electrons of the first layer of the gold atom, which move at 58% of the speed of light. This affects the position of relativistic electrons in the low orbits of heavy atoms such as lanthanides, which belong to the rare earths.

<sup>47</sup> Positrons were discovered experimentally by Carl Anderson in 1932. He was awarded the Nobel Prize in Physics in 1936.

<sup>48</sup> Paul Dirac was distinguished by his shyness and parsimonious oral expression in meetings or during meals. So much so that his Cambridge colleagues had defined the "dirac" unit as the most concise way to express himself in a meeting, namely, at the rate of a single word per hour. His behavior was equivalent at the Solvay Congresses he attended, notably that of 1927. However, he must have broken a record in his [speech](#) accepting his Nobel Prize at the end of 1933. It is still six pages long! Half, however, of the 12 pages of the speech of Erwin Schrödinger, also winner of the Nobel Prize in Physics that year.



The Bohr radius that defines the average orbital of an electron decreases inversely proportional to the apparent mass of the electron. Because the electron's apparent mass increases, this Bohr radius is smaller for relativistic electrons. This modifies the structure of the electron orbitals of heavy atoms and the transition energy levels between orbitals that absorb or emit photons.

This explains the color of gold and silver, due to relativistic modification of orbits of electron layers between which transitions occur due to the absorption of photons. Blue is absorbed in the case of gold, explaining its yellow color. Without the relativistic effect, gold would be white.

This has a lot of implications in the chemistry of these materials and with their crystal organization<sup>49</sup>. This quantum relativistic effect also explains why mercury is liquid at room temperature<sup>50</sup>. All this gives rise to a field of chemistry called [relativistic quantum chemistry](#)<sup>51</sup>. It also explains why the size of atoms is not proportional to their number of protons and electrons<sup>52</sup>.

Particles also become relativistic in **particle accelerators** such as the CERN LHC near Geneva (the largest in the world), the ESRF in Grenoble (European Synchrotron Radiation Facility, specialized in the generation of "hard", very high-frequency X-rays) or the SOLEIL light synchrotron located in Saint-Aubin near Saclay just next to the CEA, also in France.

The SOLEIL synchrotron uses electrons accelerated to a relativistic speed and inverters that generate beams of light 10,000 times denser than sunlight<sup>53</sup>. Equivalent instruments exist such as the Advanced Photon Source at the Argonne National Laboratory from the US Department of Energy near Chicago.

<sup>49</sup> See more examples in [Relativistic Effects in Chemistry More Common Than You Thought](#) by Pekka Pyykko, 2012 (24 pages).

<sup>50</sup> Voir [Why is mercury liquid? Or, why do relativistic effects not get into chemistry textbooks?](#) by Lars J. Norrby, 2018 (4 pages).

<sup>51</sup> See [Relativistic quantum chemistry](#) by Trond Saue, 2019 (110 slides) and [An introduction to Relativistic Quantum Chemistry](#) by Lucas Visscher (107 slides). The mathematical formalism of relativistic quantum chemistry is well documented in the voluminous [Introduction to Relativistic Quantum Chemistry](#) by Kenneth Dyall and Knut Faegri, 2007 (545 pages).

<sup>52</sup> See this [periodic table of elements](#) with an indication of the sizes of the atoms.

<sup>53</sup> See the conference [Electrons relativists as light sources](#) by Marie-Emmanuelle Couprie, Synchrotron Soleil, 2011 (1h25). Electrons circulate in the synchrotron at a speed close to that of light. SOLEIL powers more than 25 analytical instruments covering the spectrum from infrared to X-rays, with numerous applications in precision microscopy, including a microscopy using very well collimated and polarized white light. These instruments can be used to analyze the three-dimensional structure of organic molecules such as complex proteins, such as the glycoproteins that surround viruses. This even allows one to study how these proteins combine with those of the attacked cells, or ribosomes, which are used to produce the proteins in the cells, are also analyzed.

**Free Electron Lasers (FEL)** exploit relativistic electron sources. These are lasers generating coherent light (spatially and temporally, the emitted photons have the same frequency, phase and in that case, also polarization) and exploit relativistic electron sources from synchrotrons.

The interaction between these electrons and a strong alternating magnetic field makes it possible to generate coherent light in electromagnetic frequency ranges from infrared to X-rays, through visible light and ultraviolet<sup>54</sup>. The FEL are used to explore all sorts of matter, particularly in biomedical research like with X-rays crystallography.

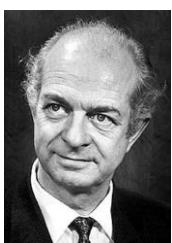
Finally, relativistic particles can be found in **astrophysics** and, for example, in cosmic ray sources as well as in relativistic plasma jets produced at the center of galaxies and quasars<sup>55</sup>.



**Vladimir Fock** (1898-1974, Russian) was a theoretician physicist who worked on quantum physics, the theory of gravitation and theoretical optics. We owe him the Fock space, representation and state, used in quantum photonics to represent the state of bosons many-body systems having the same quantum state. He co-created the Klein-Gordon equation in 1926, the relativist version of Schrödinger's equation for zero spin massive particles, the adiabatic theorem with Max Born in 1928 and the Hartree-Fock quantum simulation method in 1930. He also worked on quantum electrodynamics and quantum foundations.

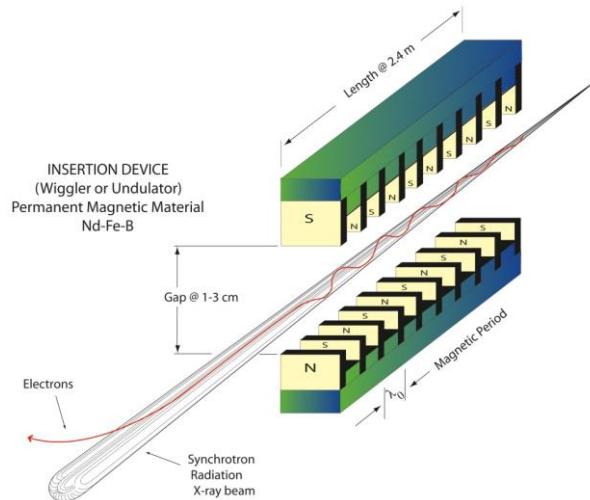


**Pascual Jordan** (1902-1980, German) was a physicist who collaborated with Max Born and Werner Heisenberg and contributed to laying the mathematical foundations of quantum mechanics, especially in matrix computation. Like Philipp Lenard, he was somewhat forgotten because of his membership in the Nazi Party during the 1930s, although he was rehabilitated after the Second World War thanks to the help of Wolfgang Pauli. He became interested in the philosophical notion of free will.



**Linus Pauling** (1901-1994, American) was a biochemist known to have co-founded the scientific fields of quantum chemistry and molecular biology. He had the opportunity to meet in Europe the founders of quantum physics like Erwin Schrödinger and Niels Bohr in 1926-1927. He described chemical bonds over a period between 1928 and 1932 and in particular the hybridization of orbitals which explains the geometry of molecules. He published "The Nature of the Chemical Bond" in 1939.

He was awarded the Nobel Prize in Chemistry in 1954 and the Nobel Peace Prize in 1962 for his political activism in favor of nuclear disarmament. He is considered to be at the origin of computational chemistry, which makes it possible to numerically simulate the structure of molecules and which we discuss in the section on quantum applications in health on page 543.



<sup>54</sup> Source of illustration : [X-ray diffraction: the basics](#) by Alan Goldman (31 slides).

<sup>55</sup> Dirac's equation is linked to the **Klein-Gordon equation** (1926) which applies to bosons such as elementary gluon particles and pions, particles having integer or zero spin. Relativistic quantum mechanics is a broad field of physics, used in particular in elementary particles physics. I have not yet found any use cases of this branch of physics in current quantum technologies. See the main foundations of relativistic quantum mechanics in [Relativistic Quantum Mechanics](#) by David J. Miller, University of Glasgow, 2008 (116 slides).



**James Chadwick** (1891-1974) is an English physicist who was responsible for the discovery of neutrons in 1932, which earned him the Nobel Prize in Physics in 1935. This discovery was late compared to quantum physics and the discovery of electrons. Nuclear physics has indeed progressed in parallel with quantum physics, which was mainly concerned with the interactions between electrons and photons. Before the discovery of neutrons, scientists thought that the nucleus of atoms contained protons and electrons.



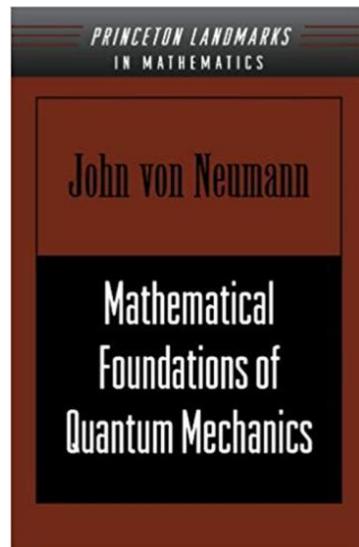
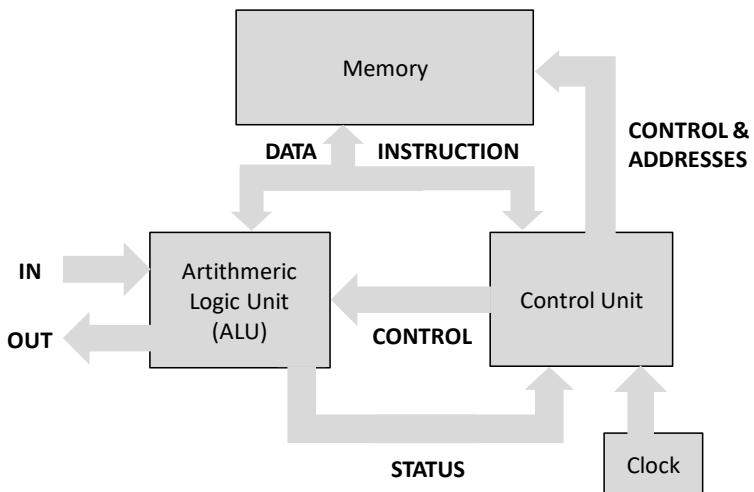
**John Von Neumann** (1903-1957, Hungarian, then American) was a polymath and an extremely prolific mathematician. He participated in the creation of the mathematical foundations of quantum mechanics, notably in the "Mathematical Foundations of Quantum Mechanics" published in 1932. He transposed the main principles of quantum mechanics into models and equations of linear algebra. He devised the key mathematical principles behind quantum measurement models.

This deals, for example, with the representation of quantum states as a position in a Hilbert space, the observables which are projections into Hilbert spaces and the indeterminacy principle which can be explained by the non-commutativity of measurement operators. These principles are also named Birkhoff-von Neumann *quantum logic*, in connection with their seminal paper published in 1936<sup>56</sup>.

Von Neumann also affirmed that the introduction of hidden variables to incorporate determinism was a lost cause because it would contradict other (verified) predictions of quantum physics. Three years before Einstein/Podolsky/Rosen's EPR paper!

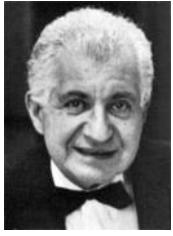
We owe him the creation of the notion of entropy (by Von Neumann), in 1932, which is associated with the notions of operators and density matrices that he created in 1927 and which describe the state of a multi-partite quantum system. He participated in the Manhattan Project in the USA.

### PRINCETON (VON NEUMAN) ARCHITECTURE



He modelled explosions and lenses for compressing plutonium in A-bombs. He is also responsible for the basic concepts in game theory and classical computers that are still in use. Thus, almost all computers use a Von Neumann architecture with memory, registers, control unit, computing unit, inputs and outputs. What a contribution!

<sup>56</sup> See [The Logic of Quantum Mechanics](#) by Garrett Birkhoff and John Von Neumann, 1936 (22 pages).



**Boris Podolsky** (1896-1966, Russian then American) wrote the EPR paradox paper with Albert Einstein and Nathan Rosen in 1935 on quantum entanglement and questions of non-locality of the properties of entangled quanta. He was a specialist in electrodynamics which deals with the analysis of electric and electromagnetic fields. He emigrated to the USA and, according to Russian archives, was a post-war KGB spy and informer of the USSR on the American atomic program between 1942-1943. His code name was... "Quantum".



**Nathan Rosen** (1909-1995, American then Israeli) is the third EPR paradox author when working as an assistant to Albert Einstein in Princeton. After moving to Israel in 1953, he created the Institute of Physics at Technion University in Haifa. He was mainly working on astrophysics and relativity theory. He devised the concept of wormholes, a theoretical link between different points in space and time. He also thought neutrons were built out of a proton coupled to an electron.



**Ettore Majorana** (1906-circa 1938, Italian) imagined the existence of a fermion in 1937 based on Dirac's equations, a particle that would be its own antiparticle. Its existence would have been discovered in 2012 and would have been verified in 2016 and then 2018, even if it is still disputed by many physicists. These fermions of Majorana should make it possible to design universal quantum computers called topological computers that can handle very efficient error correction codes requiring a small number of physical qubits.

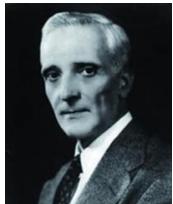
This is the exploration path chosen by Microsoft after the work of Michael Freedman and Alexei Kitaev in the late 1990s. Ettore Majorana is said to have committed suicide after a depression, because he could hardly stand the pressure of his genius! But his disappearance remains enigmatic because his body has never been found!



**Alonzo Church** (1903-1995, American) was a mathematician who was a key contributor to the foundations of theoretical computer science and on the notion of computability. Among other things, he created the lambda calculus in 1936, a universal abstract programming language which inspired the creation of LISP. He also created the so-called Church-Turing thesis. For this last one, any automatic calculation can be carried out with a Turing machine. Church and Turing also proved an equivalence between being  $\lambda$ -computable and Turing computable.

Many variations of the Church-Turing thesis were elaborated after them to extend the broad field of complexity theories. For example, the extended Church-Turing thesis states that the computation time of a problem is equivalent at worst to a polynomial depending on the size of the problem. It is not demonstrable.

What about the others, known, unknown or less famous from the 1927 Solvay Congress? Two participants deserve to be mentioned who had some connections with quantum physics.

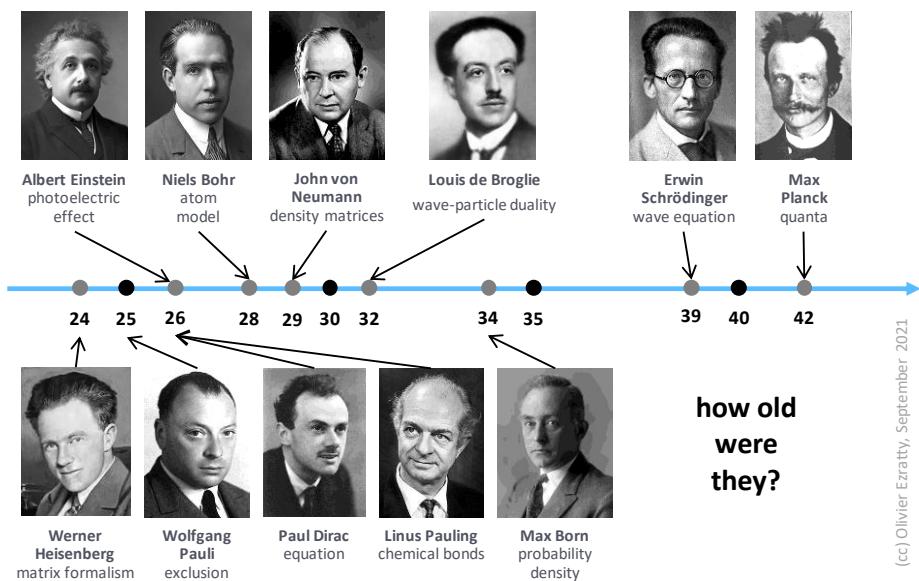


**Léon Brillouin** (1889-1969, Franco-American) who is less-known in France because of his expatriation to the USA during World War II contributed to advances in quantum physics between the two World Wars. In particular, he brought quantum mechanics closer to crystallography. He especially discovered the phenomena of diffraction of waves traversing crystals, called Brillouin scattering.

And then, finally, **Hendrik Anthony Kramers** (1894-1952, Dutch) who assisted Niels Bohr in the creation of quantum theory.

Many of the participants were not quantum physics scientists. They were invited because the Belgium organizers tried to have a stable proportion of Belgians, French, Germans and English participants. Were there, for example, **Émile Henriot** and **Marie Curie** who were focused on radioactivity, **Paul Langevin** (with whom Marie Curie had had an affair in 1910, after the accidental death of her husband Pierre Curie in 1906), as well as a good number of chemists.

At last, here's a simple chart reminding us how young the founders of quantum physics were when they published their seminal work in the key years from 1900 to 1935. Back then, scientific research didn't work the same way. They also were frequently awarded Nobel prizes at less than 40! Nowadays, most of the times, you have to wait until you are at least 50 if not 70.



(cc) Olivier Ezratty, September 2021

## Post-war

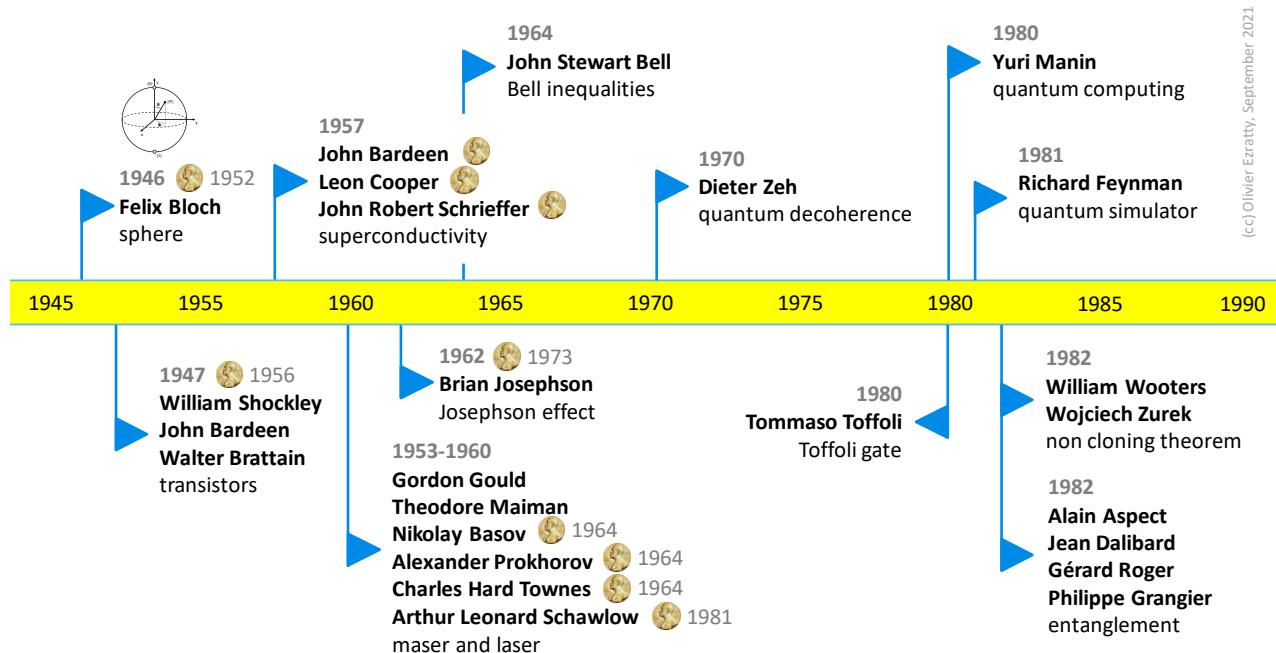
As mentioned before, quantum physics developments seemed to slow down between 1935 and 1960. Physicists were then busy with nuclear physics. The Manhattan project mobilized an amazingly large number of physicists like John Von Neumann and Enrico Fermi.

Quantum physics still led, after World War II, to an incredible wealth of technologies that revolutionized the world. We can mention three important branches resulting from the applications of the first quantum revolution: **transistors**, invented in 1947 by William Shockley, John Bardeen and Walter Brattain from the Bell Labs<sup>57</sup>, **masers** and **lasers** invented between 1953 and 1960 by Gordon Gould, Theodore Maiman, Nikolay Basov, Alexander Prokhorov, Charles Hard Townes and Arthur Leonard Schawlow, only a few of whom received the Nobel Prize associated with these discoveries, **photovoltaic cells** that convert light into electricity, and the **GPS**. Transistors and lasers are the basis of much of today's digital technology. All our digital devices are already quantum! The field of quantum optics started in the early 1960s with the laser invention and Roy J. Glauber's work, with his seminal work in 1963 on light classification where he formalized the coherent states generated by lasers, *aka* Glauber states.

The post-war period was also dominated in quantum physics by advances made on superconductivity with the BCS theory in 1957 and the Josephson junction in 1962, and by the theoretical work of John Stewart Bell in 1964.

<sup>57</sup> Transistors are based on many quantum phenomena, particularly the electronic structure of atoms in semiconductors crystals that was discovered during the 1930s and creates forbidden energy levels named band gaps (found by Sir Alan Herries Wilson, UK, in 1931), the impact of defects in crystals leading to doping and the tunneling effect due to the wave-particle duality of electrons. The first transistor was made of germanium, not silicon. See [The Transistor, an Emerging Invention: Bell Labs as a Systems Integrator Rather Than a 'House of Magic'](#) by Florian Metzler, October 2020 (57 pages) which shows the flow of discoveries that led to the creation of the first transistor by the Bell labs in 1947.

We then have the verification of entanglement by Alain Aspect's experiment in 1982. 1980 and 1981 are other key dates which mark the symbolic beginnings of quantum computing, imagined by Yuri Manin (gate-based quantum computing) and Richard Feynman (quantum simulation).



The term **second quantum revolution** covers advances from the 1990s and later, when the quantum properties of individual particles could be controlled at the level of photons (polarization, ...), electrons (spin) and atoms or ions, as well as superposition and entanglement. This led to the emergence of quantum cryptography and quantum telecommunications, in addition to the premises of quantum computing. The original definition of this second quantum revolution is however not as precise as that<sup>58</sup>.



**Felix Bloch** (1905-1983, Swiss then American) is a physicist who created the geometrical representation of a qubit state in a sphere, Bloch's sphere was elaborated in 1946 in a paper on nuclear magnetism, his main specialty. Like other physicists of his time, he contributed to the Manhattan Project, although quite shortly. He was awarded the Nobel Prize in Physics in 1952 for his work on nuclear magnetic resonance and magnons conceptualization. He was also the first director of the international particle physics laboratory CERN in 1954.



**Chien-Shiung Wu** (1912-1997, Chinese then American) was a scientist who contributed to the development of nuclear physics and to the Manhattan Project, with her gaseous diffusion process used for separating uranium 238 from uranium 235. She also contributed to the development of quantum physics by conducting the first experiment related to the synchronization of photon pairs and entanglement in 1949, before Alain Aspect's experiment in 1982<sup>59</sup>.

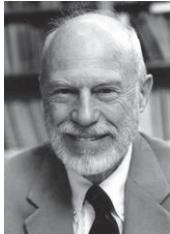
This experiment was different and was based on the measurement of the angular correlation of gamma ray photons (with very high-frequency and high-energy) generated by the encounter of electrons and positrons.

<sup>58</sup> The second quantum revolution expression was created simultaneously and independently in 2003 by Alain Aspect and by Jonathan Dowling and Gerard Milburn. The latter is also known to be one of the three protagonists of the KLM model of photon-based quantum computing, created in 2001 jointly with Emanuel Knill and Raymond Laflamme.

<sup>59</sup> See [The Angular Correlation of Scattered Annihilation Radiation](#), Wu and Shaknov, 1949.



**Hugh Everett** (1930-1982, American) is a physicist who created the formulation of relative states and a global wave function of the Universe integrating observations, observers and tools for observing quantum phenomena. He met Niels Bohr with other physicists in Copenhagen in 1959 to present his theory. He was politely listened to, but his interlocutors said that he understood nothing about quantum physics.



Everett was also a contributor to the connections between the theory of relativity and quantum physics, especially around quantum gravitation. He is credited with the hypothesis of multiple or multiverse worlds, or many-worlds interpretation, explaining quantum entanglement and non-locality. It is in fact coming from **Bryce DeWitt** (1922-2004, American) who interpreted his work in 1970. DeWitt also worked on the formulation of quantum gravity theories.



**John Wheeler** (1911-2008, American) supervised Hugh Everett's thesis. He was a specialist in quantum gravitation. He worked in the field of nuclear physics, notably in the Manhattan project, on the first American H-bombs and on very high-density nuclear matter found in neutron stars. He popularized the term black hole in 1967. He imagined a delayed-choice experiment to decide when a quantum object decides to travel as a wave or as a particle.

He collaborated with Niels Bohr and among his PhD students were Richard Feynman and Wojciech Zurek!



**John Stewart Bell** (1928-1990, Irish) relaunched research in quantum mechanics in the 1960s on the notion of entanglement. We owe him the [Bell inequalities](#) that highlight the paradoxes raised by quantum entanglement. Bell's 1964 theorem indicates that no theory of local hidden variables - imagined by Einstein in 1935 - can reproduce the phenomena of quantum mechanics<sup>60</sup>. He was rather pro-Einsteinian in his approach and favorable to a realistic interpretation of quantum physics<sup>61</sup>.

His Bell inequalities define the means to verify or invalidate the hypothesis of the existence of hidden variables explaining quantum entanglement. Bell's inequalities were violated by the experiments of **Alain Aspect** in 1982, demonstrating the inexistence of these local hidden variables.

Prior to this experiment, Bell's inequalities had been formulated for pairs of entangled photons by **John Clauser, Michael Horne, Abner Shimony** and **Richard Holt** in 1969 with their so-called CHSH inequalities with some experimental settings proposals<sup>62</sup>. John Bell's work was completed in 2003 by **Anthony Leggett** (1938, Anglo-American, Nobel Prize in Physics in 2003) with his inequalities applicable to hypothetical non-local hidden variables<sup>63</sup>. Leggett was also an initial contributor to the creation of superconducting qubits.

**Anton Zeilinger** (1945, Austrian) managed to experimentally violate these inequalities in 2007. According to Alain Aspect, however, this did not call into question the non-local hidden variable model proposed by David Bohm.

---

<sup>60</sup> See this explanation of Bell's theorem in a paper by Tim Maudlin on the occasion of the 50th anniversary of the theorem: [What Bell Did](#), 2014 (28 pages). And Bell's original document: [On the Einstein-Podolsky-Rosen paradox](#), John S. Bell, 1964 (6 pages).

<sup>61</sup> See [What Bell Did](#) by Tim Maudlin, 2014 (28 pages) which describes the EPR paradox and Bell's contribution.

<sup>62</sup> See [Proposed experiment to test local hidden-variable theories](#), 1969 (5 pages).

<sup>63</sup> See [Nonlocal Hidden-Variable Theories and Quantum Mechanics: An Incompatibility Theorem](#) by Anthony Leggett, 2003 (25 pages).



**Claude Cohen-Tannoudji** (1933, French) is a former student of Normale Sup where he followed the teachings of mathematicians Henri Cartan and Laurent Schwartz and physicist Alfred Kastler. He was awarded the Nobel Prize in Physics in 1997 at the same time as Steven Chu, who was later Secretary of Energy during Barack Obama's first presidency. This Department (DoE, Department of Energy) is one of the federal agencies most invested in quantum technologies, notably because they operate the largest supercomputers in the country.

Claude Cohen-Tannoudji owes his Nobel Prize to his work on atoms laser cooling which made it possible to reach extremely low temperatures, below the milli-Kelvin (see his [reading](#)). Alain Aspect once worked in his team. Alain Aspect says that he discovered quantum physics with reading the reference book on quantum physics by Claude Cohen-Tannoudji, Bernard Diu and Franck Laloë published in 1973<sup>64</sup>.



**Serge Haroche** (1944, French), Nobel Prize in Physics in 2012, is a founder of Cavity Electrodynamics (CQED) which describes the interaction between photons and atoms in cavities. He used it to create cold atom based qubits. **Jean-Michel Raymond**<sup>65</sup> and **Michel Brune** were among his collaborators. Serge Haroche was the first to measure the phenomenon of quantum decoherence (loss of superposition) in an experiment in 1996. This experiment was conducted at the ENS with rubidium atoms. Serge Haroche is also a member of Atos Scientific Council. CQED was later applied in the field of superconducting qubits with Circuit Electrodynamics (cQED), where atoms are replaced by an artificial atom made with a Josephson junction and the cavity by a planar microwave resonator.

Serge Haroche is one of the most circumspect scientists on the future of quantum computing, at least for universal gate computing. He believes more in the advent of quantum simulation<sup>66</sup>.



**Alain Aspect** (1947, French) invalidated Bell's inequalities with a series of experiments conducted between 1980 and 1982 at the Institut d'Optique of the Orsay University in the southern suburb of Paris with Jean Dalibard, Philippe Grangier and Gérard Roger. It validated the entanglement of distant photons and the principle of non-locality of quantum properties<sup>67</sup>. The experiment avoided any potential synchronization between the polarizers, using a 50 MHz random optical switch on both sides, feeding two orthogonal polarizers and photon detectors.

From 1988 to 2015, other experiments were conducted elsewhere and implemented loophole-free Bell tests, first closing individual loopholes and then, in 2015, closing them altogether. It confirmed then that there were no local variables explaining entanglement and validated the non-locality condition: long distance between analyzers to avoid any interactions made possible by special relativity.

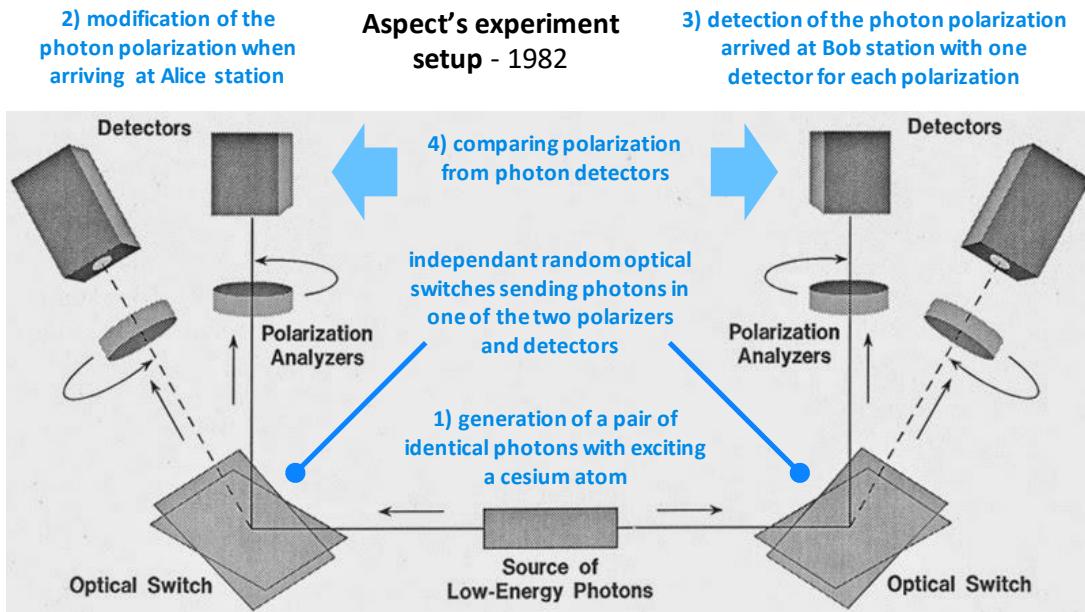
---

<sup>64</sup> This book is published in three tomes that were last revised in 2019. The first one is [Quantum Mechanics, Volume 1: Basic Concepts, Tools, and Applications](#). The second deals with [Angular Momentum, Spin, and Approximation Methods](#) and the third one with [Fermions, Bosons, Photons, Correlations, and Entanglement](#). These are classical quantum physics students textbooks.

<sup>65</sup> See his interesting conference [Quantum Computing or how to use the strangeness of the microscopic world](#), Jean-Michel Raymond, 2015 (1h36mn). See also his [presentation material](#) (56 slides).

<sup>66</sup> See [Quantum Computing: Dream or Nightmare?](#) by Serge Haroche and Jean Michel Raimond, Physics Today, 1995 (2 pages) who expressed their skepticism about quantum computing. Serge Haroche continues to convey this skepticism.

<sup>67</sup> Alain Aspect's experiments were using calcium atoms as source of photons, using some laser excitation and an atomic cascade generating pairs of entangled photons at 551 nm and 423 nm. There were actually several experiments: in 1981 with Philippe Grangier and Gérard Roger with one way polarizers, 1982 also with Grangier and Roger with two-channels polarizers and also 1982, with Jean Dalibard and Gérard Roger, using variable polarizers based on acousto-optical 10 ns switches. These could act faster than light propagation between the polarizers (40 ns) and even than the photons time of flight between the source and each switch (20 ns). See [Experimental Test of Bell's Inequalities Using Time-Varying Analyzers](#) by Alain Aspect, Gérard Roger and Jean Dalibart, Physical Review Letters, December 1982 (4 pages).



It avoided detection loopholes with high-efficiency photon detectors on top of escaping ‘memory loopholes’, which was already obtained by Alain Aspect et al in their seminal 1982 experiment<sup>68</sup>.

After his work on photon entanglement, Alain Aspect shifted gear on cold atoms control with lasers, starting with helium. This led to the creation of a promising field of quantum computing in France, using cold atoms, embodied by the startup **Pasqal**, whose scientific director is Antoine Browaeys, a former PhD student of Philippe Grangier, himself the first PhD student of Alain Aspect.

Along with other scientists, Alain Aspect is also a member of Atos Scientific Council and in the scientific board of **Quandela**. He teaches quantum physics, notably in MOOCs created for Ecole Polytechnique and distributed by Coursera.



**Philippe Grangier** (1957, French) was a PhD student of Alain Aspect with whom he worked on the 1982 experiment with Gérard Roger and Jean Dalibard. He is one of the world's leading specialists in quantum cryptography, especially on CV-QKD. He was involved in the creation of the associated startup, Sequrnet, in 2008 and closed in 2017, probably created a little too early in relation to the needs of the market.

He is also invested in cold atoms control with lasers at IOGS (Institut d'Optique). At last, he cocreated the CSM ontology of quantum foundations with Alexia Auffèves and Nayla Farouki, starting in 2013 and with a series of 7 foundational papers published between 2015 and 2019. CSM ontology is quickly covered in the [Quantum Foundations section](#).



**Jean Dalibard** (1958, French) is a research physicist at the ENS and teaches at the Polytechnique and the Collège de France. He is a specialist in quantum optics and interactions between photons and matter<sup>69</sup>. He participated with Philippe Grangier in the set-up of Alain Aspect's experiment in 1982 when he was a contingent scientist at the Institut d'Optique. He has been a member of the French Academy of Sciences since 2020 and was awarded the CNRS gold medal in 2021.

<sup>68</sup> See [Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km](#) by B. Hensen et al, ICFO and ICREA in Spain and Oxford, UK, August 2015 (8 pages) and also [A strong loophole-free test of local realism](#) by Lynden K. Shalm et al, September 2016 (9 pages).

<sup>69</sup> See in particular his lesson on [cold atoms at the Collège de France](#) which describes well how atoms are cooled at very low temperatures with lasers.



**Dieter Zeh** (1932-2018, German) is the discoverer of the quantum decoherence phenomenon in 1970. It marks the progressive end of the phenomenon of superposition of quantum states, when particles are disturbed by their environment and their amplitude and phase is modified. The notion of decoherence is key in the design of quantum computers. The objective is to delay it as much as possible resulting from the interaction between quanta and their environment<sup>70</sup>.



**Wojciech Zurek** (1951, Polish) is a quantum decoherence physicist who contributed to the foundations of quantum physics applied to quantum computers. We owe him the Non-Cloning Theorem, which states that it is impossible to clone a qubit identically without the resulting qubits then being entangled. He is also at the origin of the concept of quantum Darwinism which would explain the link between the quantum world and the macrophysical world.

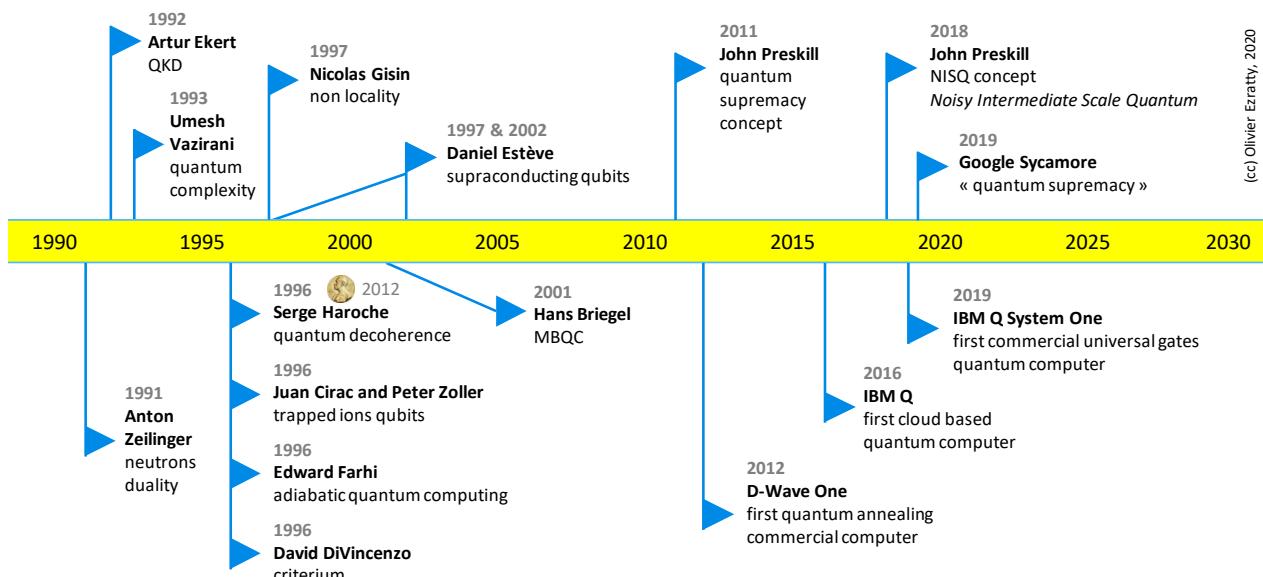


**Anton Zeilinger** (1945, Austrian) is physicist who advanced the field of quantum teleportation in the 2000s. He also proved in 1991 the wave-particle duality of neutrons. He was also the first to realize a qubit teleportation. He is a specialist in quantum entanglement, having proved that it is possible to entangle more than two quantum objects or qubits. He created theoretical and experimental foundations for quantum cryptography.

With two colleagues, he also developed the GHZ (Greenberger-Horne-Zeilinger) entangled state, which enables yet another demonstration of the inexistence of hidden variables which would explain quantum entanglement of at least three particles and with a finite number of measurements. The concept was created in 1989 and was validated experimentally in 1999. Anton Zeilinger also supervised the thesis of **Jian-Wei Pan**, who became later the quantum research czar in China.

## Quantum computing physicists

This story now provides an overview of key contributors to the physics of quantum computing. They are often specialized in condensed matter, such as for superconducting qubits, and in photonics.



<sup>70</sup> Dieter Zeh is notably the author of [On the Interpretation of Measurement in Quantum Theory](#) in 1970 (8 pages).

I highlight many European and French physicists, particularly those I have had the opportunity to meet for the last three years in my journey in the quantum ecosystem. This inventory is both objective and subjective. Objective because it includes a broad hall of fame in the field. Subjective because I have added a good dose of physicists I know, which creates a measurement bias. Which is easy to understand in both social science and quantum physics.



**Richard Feynman** (1918-1988, American) is one of the fathers of quantum electrodynamics, which earned him the Nobel Prize in Physics in 1965. He theorized in 1981 the possibility of creating quantum simulators, capable of simulating quantum phenomena, which would be useful to design new materials and molecules in various fields like chemistry and biotechs<sup>71</sup>. He is also at the origin of the quantum explanation of helium superfluidity at very low temperature in a series of papers published between 1953 and 1958. He was also known for his great presentation skills.



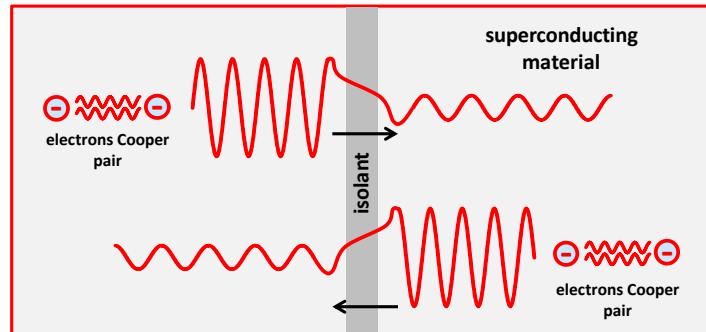
**Wolfgang Paul** (1913-1993, Germany), not to be confused with Wolfgang Pauli, is a physicist who conceptualized trapped ions in the 1950s. He got the Nobel Prize in Physics in 1989. We owe him the traps that bear his name and are used to control trapped ions. He shared his Nobel prize with **Hans Georg Dehmelt** (1922-2017, Germany) who codeveloped these traps with him. The physicists **Juan Cirac** (1965, Spanish) and **Peter Zoller** (1952, Austria) theorized, designed and tested the first trapped ion qubits in 1996, based on the work of Wolfgang Paul.



**Brian Josephson** (1940, English) is a physicist from the University of Cambridge. He was awarded the Nobel Prize in Physics in 1973 at the age of 33<sup>72</sup>, for his prediction in 1962 of the effect that bears his name when he was only 22 years old and a PhD student at the University of Cambridge. The Josephson effect describes the passage of current in a superconducting circuit through a thin insulating barrier a few nanometers thick, using tunneling effect, and the associated threshold effects.

Below a certain voltage, the current starts to oscillate. It is generated by electrons organized in Cooper pairs named after Leon Cooper who discovered it in 1952. These electrons pairs have opposite spins (magnetic polarity).

The system behaves as a resistance associated with a loop inductance, the oscillation being controllable by a magnetic field and having two distinct energy states. Superconductivity was discovered in 1911 by **Heike Kamerlingh Onnes** (1853-1926, Netherlands). This is the basis of superconducting qubits and their quantum gates!



<sup>71</sup> See [Simulating Physics with Computers](#) published in 1981 and [Quantum Mechanical Computers](#) also by Richard Feynman, published in 1985 (10 pages). He describes how a quantum computer could perform mathematical operations similar to those of traditional computers. He concludes by saying that it should be possible to create computers where a bit would fit into a single atom!

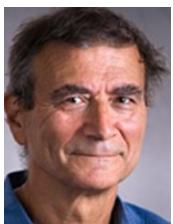
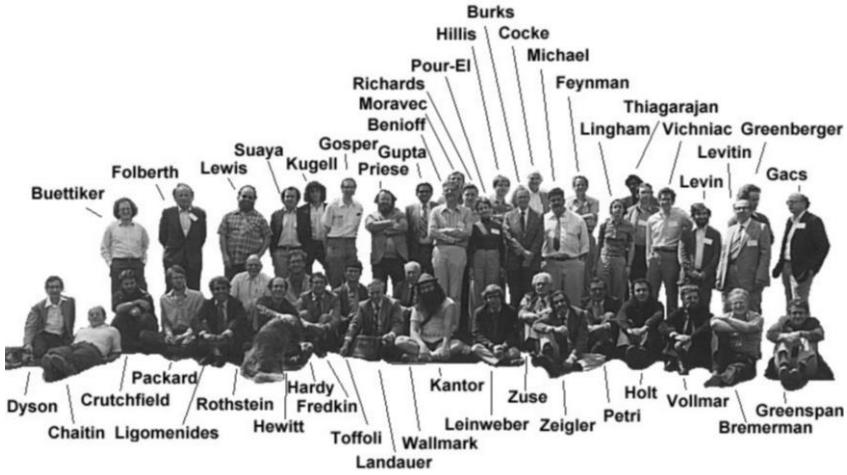
<sup>72</sup> Brian Josephson shared the 1973 Nobel Prize in Physics with two scientists who had worked before him in the same field: Leo Esaki (1925, Japan, still alive in early 2020) for his discovery of the tunnel effect in semiconductors in 1958 and Ivar Giaever (1929, Norway, also still alive) who found that this effect could occur in superconducting materials in 1960.



**Yuri Manin** (1937, Russian and German) is a mathematician who, along with Paul Benioff and Richard Feynman, was among the first scientists to propose the idea of creating gate-based quantum computers, in his 1980 book "Computable and Uncomputable". This was just before Richard Feynman who, in 1981, devised the quantum simulator idea. They both participated in the "Physics & Computation" conference at MIT in 1981.

It brought together a number of well-known scientists in quantum information technology such as Tommaso Toffoli and Edward Fredkin (*opposite, source*).

Rolf Landauer was also among them. It was for this conference that Richard Feynman published Simulating Physics with Computers<sup>73</sup>.



**Tommaso Toffoli** (1943, Italian then American) is an engineer known for the creation, at the beginning of the 1980s, of the quantum gate bearing his name, a conditional gate with three inputs that is widely used in quantum programming. After working at MIT, he became a Boston University professor, where he has served since 1995. Like Stephen Wolfram, his interests include cellular automata and artificial life.



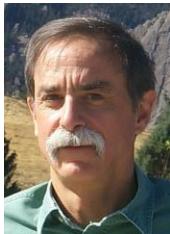
**Edward Fredkin** (1934, American) is a professor at Carnegie Mellon University. He is the author of the two-way conditional swap quantum gate (SWAP). He is also the designer of the concept of reversible classical computer with Tommaso Toffoli at MIT. He is also a prolific inventor far beyond quantum computing and is the originator of vehicle identification transponders and automotive geonavigation.

Finally, he is a promoter of the notion of "digital philosophy" which reduces the world and its functioning to a giant quantum program, a theory he shares with Seth Lloyd, an idea that has been revived by Elon Musk who believes that the Universe is a gigantic program and that we live in a simulation. Is the "automatic" respect of elementary physical laws a "program"? A thorny philosophical and semantic question!



**Rainer Blatt** (1952, Austrian and German) from the University of Innsbruck is an experimental physicist specialized, among other things, in trapped ions qubits. He was the first to entangle the quantum states of two trapped ions in 2004 and then with eight ions in 2006. He co-founded Alpine Quantum Technologies (AQT), whose ambition is to create and commercialize a trapped ions based quantum computer.

<sup>73</sup> See [Simulating Physics with Computers](#) by Richard Feynman, 1981 (103 pages).



**David Wineland** (1944, American) is a Boulder-based NIST physicist known for his advances in trapped ions and their laser-based cooling in 1978. He also created in 1995 the first single quantum gate operating on a single atom. He was awarded the Nobel Prize in Physics in 2012 jointly with Serge Haroche for his advances in atoms and ions laser cooling, a technique he first experimented in 1978, followed by the first quantum gate applied to a trapped ion in 1995 and the entanglement between four trapped ions in 2000.



**Christopher Monroe** (1965, American) is an American physicist known for his work on trapped ions and for co-founding IonQ in 2015, one of the two best funded quantum startups worldwide with PsiQuantum. He worked on trapped ions with David Wineland at the NIST Maryland laboratory. He demonstrated the ability to entrap ions, create ions-based quantum memory and create analog quantum simulators. He also ran a laboratory at the University of Michigan in the early 2000s.



**Edward Farhi** (1952, American) is a theoretical physicist who has worked in many fields, including high-energy particle physics, particularly at the CERN LHC in Geneva and then at MIT. He worked with Leonard Susskind on unified theories with electro-weak dynamical symmetry breaking. He and Larry Abbott proposed a model in which quarks, leptons, and massive gauge bosons are composite. He is above all the creator of adiabatic quantum algorithms and quantum walks. He also introduced with Peter Shor the concept of quantum money in 2010.



**Daniel Esteve** (1954, French) is a physicist in charge of the CEA's Quantronique laboratory in Saclay, France, launched in 1984 with Michel Devoret and Cristian Urbina, and part of the IRAMIS laboratory. He contributed to the development of transmon superconducting qubits. He created a first operational qubit in 1997, the quantronium, followed by another controllable prototype in 2002, with Vincent Bouchiat. He continues to work on improving the quality of superconducting qubits.



**Michel Devoret** (1953, French) is a telecom engineer turned physicist, co-founder of the Quantronique laboratory with Daniel Esteve at the CEA in Saclay between 1985 and 1995, which is one of the world pioneers of superconducting qubits. He is a professor at Yale University since 2002.

He was a co-founder of the American startup QCI with his Yale colleague Rob Schoelkopf, which he left in 2019/2020. He preferred to be entirely dedicated to research.

He worked several times with John Martinis, when John was a PhD student in UCSB, then when he was a post-doc at CEA in Saclay in the early 2000s, and at last at the University of Santa Barbara, where they wrote together a review paper in 2004 on superconducting qubits<sup>74</sup>.



**Irfan Siddiqi** (1976, American-Pakistani) is one key contributor to advancements in superconducting qubits. He did his PhD and post-doc at Yale, working initially in aluminum hot-electron bolometers for microwave astronomy and then, high frequency measurement techniques for superconducting qubits. He developed the Josephson Bifurcation Amplifier that uses the non-dissipative and non-linear nature of the Josephson junction to create high gain and minimal back action readout of qubits.

<sup>74</sup> In [Implementing Qubits with Superconducting Integrated Circuits](#) by Michel Devoret and John Martinis, 2004 (41 pages).

This led to the creation of superconducting parametric amplifiers and Josephson traveling wave parametric amplifiers. He then moved at Berkeley University and the DoE Lawrence Berkeley National Laboratory. He works on quantum electrodynamics, quantum error correction, multi-partite entanglement generation and single photon detection. He runs there the Advanced Quantum Testbed, an integrated research platform on superconducting qubits and enabling technologies.



**Artur Ekert** (1961, Polish and English) is a quantum physicist known to be one of the founders of quantum cryptography. He had met Alain Aspect in 1992 to talk to him about this inspiration after discovering the latter's experiments. This is a fine example of step-by-step inventions, one researcher inspiring another! He was the director of the Singapore Center for Quantum Technology from 2007 to 2020. He is also a teacher at Oxford University and a member of Atos's Scientific Council.



**Nicolas Gisin** (1952, Switzerland) is a physicist specialized in quantum communication. He demonstrated quantum non-locality with an experiment in 1997 over a 10 km distance, extending the performance achieved in the laboratory by Alain Aspect in 1982. He co-founded IDQ in 2001, a Swiss startup initially specialized in quantum random number generators using photons passing through a dichroic mirror. It was acquired by SK Telecom in 2018.



**David DiVincenzo** (1959, American) was a researcher at IBM and the creator of the criteria that define the minimum requirements for a quantum computer with universal gates. He is now a researcher and professor at the University of Aachen in Germany. He is a member of the Atos Scientific Council, along with Alain Aspect, Serge Haroche, Artur Ekert and Daniel Esteve, among others.



**John Preskill** (1953, American) is a professor at Caltech. Among many other contributions, he is the creator of quantum supremacy notion in 2011 and of NISQ in 2018, the Noisy Intermediate-Scale Quantum, qualifying current and future noisy quantum computers. He is a regular speaker at conferences where he reviews the state of the art of quantum computing<sup>75</sup>. He's now involved with Amazon and their cat-qubits superconducting project revealed in December 2020.



**Lieven Vandersypen** (1972, Belgian) started as a mechanical engineer and a PhD at Stanford, then went to IBM in San Jose where he became interested in MEMS. He demonstrated the use of Shor's algorithm for factoring the number 15 with NMR qubits, and then became a researcher at TU Delft University in the Netherlands and in its QuTech spin-off. He is a pioneer of electron spin qubits. In this capacity, he works notably with Intel, which is testing its silicon qubit chipsets at QuTech and in which Intel invested \$50M in 2015.



**Christophe Salomon** (1953, French) is a physicist specialized in photonics and cold atoms, research director at the LKB (Normale Sup in Paris). He is particularly interested in quantum gases superfluidity (Bose-Einstein condensates) and in time measurement with cesium atomic clocks. He did a thesis in laser spectroscopy and then did a post-doc at the joint JILA laboratory between NIST and the University of Colorado. He is also a member of the Academy of Sciences since 2017.

---

<sup>75</sup> See his presentation that provides an overview of the state of the art of quantum computing [Quantum Computing for Business](#), John Preskill, December 2017 (41 slides).

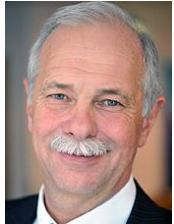


**John Martinis** (1958, American), is a physicist from UCSB who famously worked at Google between 2014 and 2020 where he led the hardware team in charge of superconducting qubits up to creating the Sycamore processor and its related “quantum supremacy experiment”, published in Nature in October 2019. After his thesis at Berkeley on superconducting qubits, he did a post-doc in Daniel Esteve's Quantronics laboratory at the CEA in Saclay.

In September 2020, he started to work with Michelle Simmons at SQC in Australia. He also created Quantala in 2020, a quantum computing company selling IP and protecting his own patents.



**Andreas Wallraff** (German) is a Professor for Solid State Physics at ETH Zurich after having obtained degrees in physics from the London Imperial College and RWTH Aachen in Germany and worked at the Jülich Research Center also in Germany, Yale in the USA and the LKB in France. He is specialized in the coherent interaction of single photons with quantum electronic circuits and quantum effects as well as on hybrid quantum systems combining microwave control, superconducting circuits and semiconductor quantum dots.



**Jürgen Mlynek** (1951, German) is a physicist specialized in optronics and interferometry. He was the coordinator of the strategic advisory board behind the launch of the European Flagship project on quantum in 2018. We owe him, as mentioned in connection with Louis De Broglie, the experiment validating the wave-particle duality of atoms carried out using helium in 1990 with Olivier Carnal at the University of Konstanz.



**Marie-Anne Bouchiat** (1934, French) is a specialist in rubidium atoms physics and their control by optical pumping. This is the basis for the creation of quantum computers based on cold atoms. Her daughter **Hélène Bouchiat** (1958, French) is also a physicist, specialized in condensed matter at the LPS laboratory of the University Paris-Saclay and member of the Académie des Sciences since 2010, like her mother who has been there since 1988.



**Elisabeth Giacobino** (1946, French) is a specialist in laser physics, nonlinear optics, quantum optics and superfluidity, particularly in relation to the control of cold atoms. She worked at the CNRS in the ENS LKB (Laboratoire Kastler-Brossel). She is a member of the scientific selection committee of the European Quantum Flagship and also for the ANR (Agence Nationale de la Recherche).



**Jacqueline Bloch** (1967, French) is a research director at CNRS (PI) in the Centre de Nanosciences et de Nanotechnologies (C2N) lab from CNRS and Université Paris-Saclay, working on polaritons, quasi-particles coupling light and semiconductor matter, mainly built in gallium arsenide (AsGa). These have potential applications in the creation of quantum simulators based on polariton arrays as well as for quantum metrology ([source](#)).



**Jean-Michel Gérard** (1962, French) is a physicist from the CEA IRIG laboratory in Grenoble and director of the joint PHELIQS laboratory (PHotonics, ELectronics and Quantum Engineering) from UGA (University of Grenoble) and CEA. He works in particular on the creation of single photon sources based on quantum dots as well as single photon detectors based on superconducting nanowires and OPO laser diodes.



**Antoine Browaeys** (c. 1970, French) is a CNRS research director leading the quantum optics-atom team in the Charles Fabry Laboratory at Institut d'Optique specialized in the control of cold atoms. He is also a cofounder and the scientific director of Pasqal, a startup designing a cold atoms computer that will be first used as a quantum simulator, and then, as a universal gates quantum computer. He was awarded the CNRS silver medal in 2021.



**Pascale Senellart** (1972, French) is a physicist, CNRS research director at the C2N laboratory. She designed and invented a process for manufacturing sources of unique and indistinguishable photons used in quantum telecommunications and computing. These are semiconductor quantum dot trapped in a multi-layered 3D structure, powered by a laser and directly feeding an optical fiber. She co-founded the startup Quandela which is selling these photon sources, also is creating photon qubit based quantum computers, and is their scientific advisor.

Pascale also launched the Quantum hub of the University Paris-Saclay in November 2019, which brings together public and private research laboratories as well as higher education institutions. She was awarded the CNRS Silver Medal in 2014.



**Maud Vinet** (1975, French) is an engineer and researcher. She leads the silicon qubit project at CEA-Leti in Grenoble. She had previously contributed to the industrialization of the FD-SOI technology from CEA and STMicroelectronics<sup>76</sup>, which reduces power consumption and improve the performance of CMOS chipsets, particularly in mobility and radiofrequency processing (in the RF-SOI variation). CEA-Leti is focused on creating electron spin qubits leveraging the strong experience of CEA and the Grenoble ecosystem with semiconductor manufacturing.

We will describe this work in more detail later in this ebook. The silicon qubit industry involves several laboratories in addition to CEA-Leti: IRIG (also from CEA), CNRS's Institut Néel, LPMMC, and various entities of UGA (Université Grenoble Alpes). Maud is also driving QLSI, the European Quantum Flagship research project on electron spins qubits, awarded in March 2020, after obtaining with Tristan Meunier (CNRS Institut Néel) and Silvano de Franceschi (CEA IRIG) an ERC funding of €14M in 2018 for the QuQube silicon qubit project.



**Alexia Auffèves** (1976, French) is a CNRS research director from Néel Institute in Grenoble, specialized in quantum thermodynamics. She collaborates with various teams in France (C2N, ENS Lyon) and around the world (Center for Quantum Technologies in Singapore, Chapman University and Saint-Louis University in the USA, Oxford and Exeter Universities in the UK, Madrid University in Spain and Luxembourg University). Her recent work focuses on the energetic aspects of quantum technologies, both from a full-stack and fundamental perspective.

Alexia Auffèves also developed the CSM ontology of quantum mechanics (Contexts, Systems and Modalities) with Philippe Grangier and the philosopher Nayla Farouki that we cover later in this ebook, when discussing the topic of quantum foundations, page 744<sup>77</sup>. She launched and actively coordinates QuEnG (Quantum Engineering Grenoble), the Grenoble quantum ecosystem which is set to become the QuantAlps federation in late 2021.

---

<sup>76</sup> FD-SOI = Fully-Depleted Silicon on Insulator. The technology uses on the one hand a layer of silicon oxide insulator and on the other hand, channels of undoped silicon between the drain and the source, limiting leakage between the latter two.

<sup>77</sup> See [Contexts, Systems and Modalities: a new ontology for quantum mechanics](#) by Alexia Auffèves and Philippe Grangier, 2015 (9 pages). See also the [associated Wikipedia](#) page. This work has been articulated on a total of seven papers released between 2015 and 2019.



**Hélène Perrin** (c. 1975, French) is CNRS research director working at the Laboratoire de Physique des Lasers (LPL) from Université Sorbonne Paris Nord, working on Bose-Einstein condensates and cold atoms control. Together with Pascal Simon, she drives the Quantum Simulation SIM project, a cold atom-based quantum simulator. She also gives lessons on quantum computing. She did her PhD thesis with Christophe Salomon at the ENS LKB in Claude Cohen-Tannoudji's group. At CEA-Saclay, she also worked on fractional quantum Hall effect.



**Eleni Diamanti** (1977, Franco-Greek) is a leading specialist and experimenter in the development of photonic resources for quantum cryptography, also working on quantum communication complexity. She's a CNRS research Director and faculty at LIP6 laboratory from Paris-Sorbonne University. She is the vice-director of the Paris Centre for Quantum Computing since April 2020. She is also involved in many European projects around quantum key distribution, like the Quantum Internet Alliance and OpenQKD. She is a recipient of a European Research Council Starting Grant.



**Jason Alicea** (American) is a Professor of Theoretical Physics at Caltech University's IQIM (Institute for Quantum Information and Matter). He is specialized in condensed matter physics and topological phase of matter which could lead on creating non-Abelian anyons and Majorana fermions, a qubit type mainly explored by Microsoft.



**Michelle Simmons** (1967, British-Australian) is a physicist from the University of New Wales in Australia (UNSW), working on electron spin qubits. She is the director of CQC2T (Centre of Excellence for Quantum Computation and Communication Technology) from UNSW. She is also the co-founder of SQC (Silicon Quantum Computing), the leading quantum computing Australian startup (\$66M), a spin-off from her university and from QQC2T.

In 2019, her team built the first two-qubit gate between phosphorous atom qubits in silicon, operating in only 0.8 ns.



**Andrew S. Dzurak** (Australian) is the Director of the Nanotechnology Fabrication Unit at UNSW's Australian National Fabrication Facility from the CQC2T research center. This facility's white room is used to manufacture silicon qubits chipsets. Andrew Dzurak is a pioneer of silicon qubits since 1998. He is leading research at CQC2T on silicon qubit control and reading. He created the first phosphorus-based silicon double qubits in 2015. He was a lead scientist for SQC, founded by Michelle Simmons, but seemingly left the company in 2021.



**Andrea Morello** (1972, Italian) is one of the star researchers at UNSW in Australia. He is Program Manager of the ARC Centre of Excellence at CQC2T and leads the Fundamental Quantum Technologies Laboratory at UNSW. During his studies, he attended the Laboratoire National des Champs Magnétiques Intenses of the CNRS in Grenoble. Today he is one of the specialists in silicon-based qubits. He is also a quantum engineering teacher at UNSW. He also participated to the creation of SQC and left it like Andrew Dzurak in 2021.

His team was the first to demonstrate coherent control and readout of an individual phosphorus atom electron and nuclear spin in silicon and held for many years the record for the longest quantum memory time of 35.6 s in a single solid-state qubit.



**Christine Silberhorn** (1974, German) is a researcher and professor working on photon-based quantum computing at the University of Paderborn located between Dortmund and Hanover. She leads there the Integrated Quantum Optics group. Her laboratory designs and manufactures integrated optronics components, entangled photon sources and quantum array systems. Her team designed a system to convert photon qubits between infrared and visible wavelengths. She also works on optical quantum memories. She was awarded the Leibnitz prize in 2011.



**Stephanie Wehner** (1977, German) is a physicist working on quantum communication protocols, based at the University of Delft in the Netherlands. She coordinates the "Quantum Internet Alliance", one of the projects of the European Quantum Flagship, which plans to deploy a quantum key distribution (QKD) Internet network running in mesh mode. She started her professional life in cybersecurity, detecting system flaws. She is also producing many quantum tech MOOCs.



**Perola Milman** (c. 1975, French) is a specialist in the theory of quantum computing and in particular with trapped photons and ions. In particular, she has demonstrated the entanglement capacity of molecules. She is a lecturer-researcher at the Laboratory of Quantum Materials and Phenomena of the University Paris Diderot. She is a professor of quantum theory of light and on quantum entanglement.



**Sara Ducci** (1971, French) is another teacher-researcher at the same Laboratoire Matériaux et Phénomènes Quantiques (MPQ) where she co-founded in 2002 a team in charge of non-linear optical devices. She is working on producing pairs of entangled photons sources based on III-V semiconductors. She is also interested in the characterization (state measurement...) and manipulation of photons. At last, she teaches quantum physics at Ecole Polytechnique.



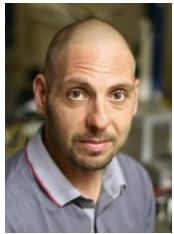
**Jacqueline Romero** (c. 1985, Philippines) is a quantum optics physicist doing research in Australia at the University of Queensland, after completing her PhD in Glasgow, UK. She is working on optical neuromorphic architectures and on dense encoding of information in photons using several of their characteristics in addition to the usual polarization.



**Patrice Bertet** (c. 1976, France) is part of Daniel Esteve's team at CEA-SPEC. He did his thesis at Serge Haroche on Rydberg atoms and then went to Delft University. He participated in the early days of superconducting qubits (quantronium at CEA and TU Delft). He then worked on QED (quantum electrodynamics) circuits based on cavities and then on transmon qubits. He is working on the association of superconducting qubits and the measurement of their state with electron spins, notably based on NV centers, which can also be used for quantum memories.



**Audrey Bienfait** (c. 1990, France) is a former PhD student of Patrice Bertet at CEA-SPEC who is now doing her research at ENS Lyon in Benjamin Huard's team. She was awarded the Bruker Prize 2018 for her thesis on electron paramagnetic resonance or "ESR - Electron Spin Resonance" in quantum regime and the Michelson Postdoctoral Prize 2019 in March 2020 for her work on the entanglement of superconducting qubits via phonons.



**Sébastien Tanzilli** (France) is the director of the InPhyNi physics laboratory in Nice and also the CNRS national quantum program director. He works on quantum cryptography with continuous or discrete keys (CV-QKD and DV-QKD), in fundamental quantum optics as well as in hybrid quantum systems for the study and realization of quantum communication networks. He is also the president of the GDR-IQFA, a community of quantum physics researchers in France (IQFA = Information Quantique, Fondements & Applications). It was created in 2011.



**Virginia D'Auria** (Italy) is a researcher working on quantum optics transmission systems using continuous and discrete variables and DV/QV hybridization. Having worked at the ENS LKB in Paris, she also worked on photon detectors. Since 2010, she is part of the photonics group of InPhyNi and works on discrete and continuous variable quantum communications compatible with optical fibers of telecom operators.



**Fabio Sciarrino** (1978, French-Italian) is the director of the Quantum Information Lab at the Sapienza University of Rome and specialized in photonics. His team is at the origin of many advances in the field, notably in boson sampling, a key experiment in the path of photon-based quantum computers. He collaborates with Qandela's team and the C2N of Palaiseau (Pascale Senellart).



**Jelena Vucokic** (c. 1975, Serbian) is a research professor at Stanford, working in quantum photonics. She directs the Nanoscale and Quantum Photonics Lab and the Q-FARM (Quantum Fundamentals, ARchitecture and Machines initiative), an interdisciplinary quantum laboratory. She contributes to developments in photonics for the development of optical quantum computers. She did her PhD at Caltech in 2002.



**Francesca Ferlaino** (1977, Italian) is a typically European researcher, having worked in many laboratories from different countries. She is research director at the IQOQI in Innsbruck, Austria, where she leads the Dipolar Quantum Gases laboratory. She is a specialist in cold atoms and erbium-based Bose-Einstein condensates.



**Marcus Huber** (Austria) is a research group leader at the IQOQI in Vienna, working on quantum entanglement, qubit state measurement and quantum thermodynamics in general. In addition to the IQOQI, he has also worked at the Universities of Bristol, Geneva and Barcelona. He is a great advocate of the open publication of research work, being at the origin of the Quantum-Journal.org website, a kind of Arxiv for quantum science.



**Tracy Northup** (c. 1975, Austria) is a researcher working on trapped ions and optical cavities, one of the major branches of quantum computing. She leads the Quantum Interfaces Group laboratory at the University of Innsbruck, which is one of the most active in the field of trapped ions, a major Austrian specialty.



**Anne Matsuura** (c. 1970, Japanese-American) is a physicist who is leading the Quantum & Molecular Technologies team from the Intel Quantum Research Laboratory since 2014. She leads the American's efforts in the creation of superconducting and silicon qubits quantum computers, with an overall vision of the hardware architecture. Her impressive career starts with a thesis at Stanford in synchrotrons, then in US Air Force labs and In-Q-Tel (the CIA investment fund). She also directed the European Theoretical Spectroscopy Facility in Belgium.



**Sarah Sheldon** (c. 1986, American) has been a member of IBM's quantum computing teams based at the Thomas J. Watson Research Center in Yorktown, New York, since 2013. She is particularly active in improving the quality of superconducting qubits, their quantum gates and error correction codes. She obtained her PhD at MIT in 2013 before doing a post-doc with IBM.



**Stefanie Barz** (c. 1980, German) is a quantum optics professor and researcher at the University of Stuttgart. Her interests include quantum cryptography and quantum telecommunications. She worked in particular on blind computing with Elham Kashefi and Anne Broadbent. She leads the SiSiQ project funded by the German Ministry of Research with €3.6M of European funding, which aims to create quantum communication infrastructure with silicon photonics.



**Alexei Grinbaum** (1978, Franco-Russian) is a researcher at CEA-Saclay in Etienne Klein's LARSIM laboratory. He works on the quantum foundations and quantum physics philosophy<sup>78</sup>. He is notably the author of the book "Les robots et le mal" (Robots and evil) published in 2018. He is particularly interested in the ethics of science, its acceptance by society and responsible innovation.



**Frédéric Grosshans** (1976, French) is a CNRS researcher at LIP6 from Université Paris-Sorbonne, specialized in QKD, repeaters and quantum networks. He was the creator with Philippe Grangier of the continuous variable QKD. He is also the co-director with Nicolas Treps (from LKB) of the Quantum Information Center Sorbonne of the Alliance Paris-Sorbonne launched in September 2020, which federates quantum research and training of several Parisian quantum groups.



**Jean-François Roch** (1964, French) is a quantum physics professor at ENS Paris Saclay. He is a pioneer of the usage of NV centers in many applications, particularly in quantum sensing, including for studying matter and magnetism at very high-pressure, which could be helpful for the discovery of high-temperature superconducting materials. He conducts these researches in partnership with Thales and with the CEA. He also led the founding Wheeler delayed choice experiment in 2006.

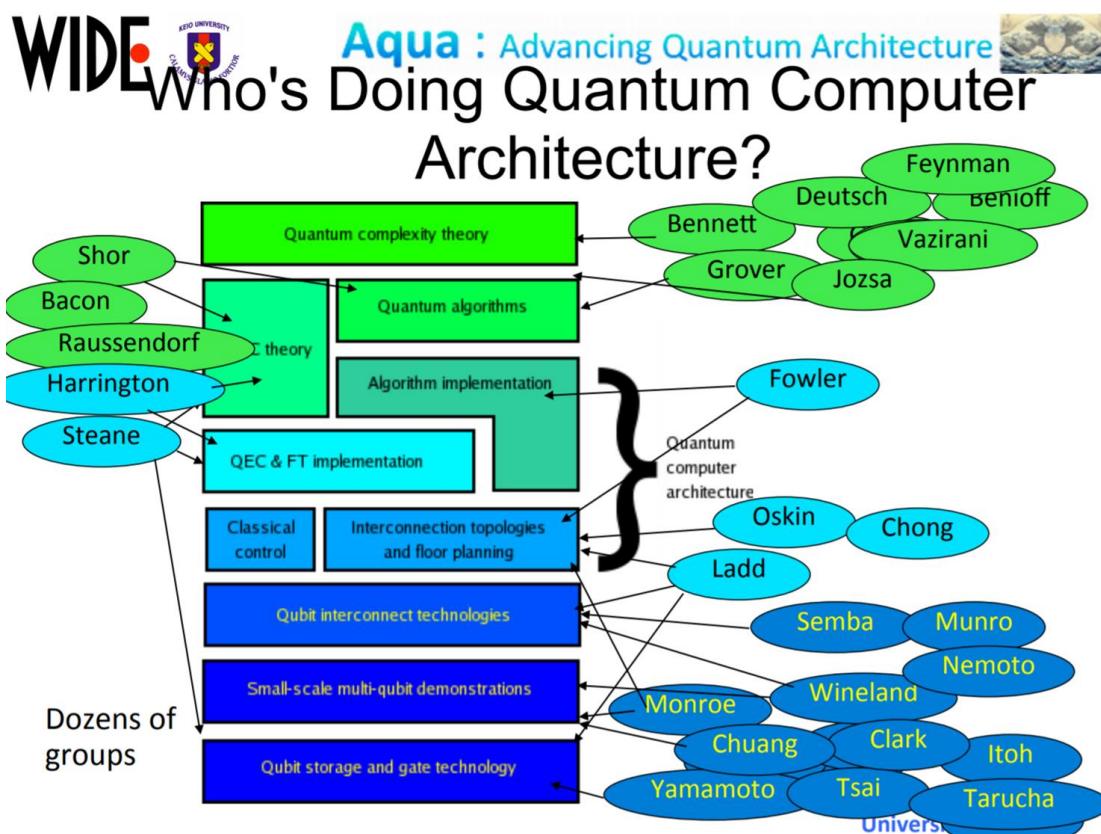
## Quantum information science and algorithms creators

Let's end this long "hall of fame" with some of the main contributors to the creation of quantum information science and algorithms.

<sup>78</sup> See [Narratives of Quantum Theory in the Age of Quantum Technologies](#) by Alexei Grinbaum, 2019 (20 pages).

It is a relatively new discipline that emerged in the early 1990s. One good way of looking at this discipline is the schema *below*<sup>79</sup>. The quantum algorithms specialists are in green, error correction codes specialists are in light blue, and qubits physical layers specialists are in dark blue.

Unfortunately, all of them are not mentioned in this book and this list will certainly continue to grow from year to year as the field is constantly making progress.



**Paul Benioff** (1930, American) is a pioneering physicist of theoretical quantum computing, whose theoretical bases he defined in the 1980s, alongside Richard Feynman, whose ideas dealt with the other field of quantum simulation. Benioff's model foresaw the possibility of performing reversible quantum computing with quantum gates. He spent some time at the CNRS in France between 1979 and 1982, at the University of Marseille-Luminy.



**Alexander Holevo** (1943, Russian) is a mathematician working in quantum information science and who devised the 1973 Holevo theorem according to which we cannot retrieve more than N bits of useful information from a register of N qubits<sup>80</sup>. This is the consequence of the wave packet reduction that reduces the qubit state to its basis states  $|0\rangle$  and  $|1\rangle$  after measurement. He also developed the mathematical basis of quantum communications.

<sup>79</sup> The schema comes from the presentation [Quantum Computer Architecture](#) by Rod Van Meter, 2011 (89 slides).

<sup>80</sup> This theorem indirectly validates the fact that it is difficult to do "big data" with a quantum computer in the sense of storing and analyzing large volumes of information. On the other hand, Grover's algorithm makes it possible to quickly find a needle in a haystack, as we will see later.



**Umesh Vazirani** (1945, Indian-American) is a professor at the University of Berkeley. He is one of the founders of quantum computing, with his paper co-authored in 1993 with his student Ethan Bernstein, [Quantum Complexity Theory](#). He is also the creator of the Quantum Fourier Transform (QFT) algorithm, which was used less than a year later by Peter Shor to create his famous integer factoring algorithm that served as a spur to funding research in quantum computing in the USA. The QFT is a founding algorithm used in many other quantum algorithms.



**Peter Shor** (1959, American) is a mathematician who became the father of the algorithm of the same name in 1994 which allows the factorization of integers into prime numbers, based on quantum Fourier transforms (QFT). He also created the first quantum discrete-log algorithm and the famous nine-qubit amplitude (flip error) and phase error correction algorithm for quantum computers called "Shor code". We indirectly owe to him the whole movement of post-quantum cryptography (PQC).

PQC is about creating cryptography codes resisting to public keys breaking using the Shor algorithm and other quantum algorithms... with quantum computers that do not yet exist. Peter Shor created his famous factorization algorithm while working at Bell Labs. He has been teaching applied mathematics at MIT since 2003.



**David Deutsch** (1953, Israeli and English) is a physicist from the Quantum Computing Laboratory at Oxford University in the UK. He is the author of a search algorithm, with two variants, a first one from 1985 and a second one in 1992 co-created with Richard Jozsa. He devised in 1985 the idea of creating a quantum Turing machine which led him to create in 1989 the gate-based circuits programming model, completing Yuri Manin's 1980 idea.



**Lov Grover** (1961, Indian-American) is a computer scientist who created the seminal quantum algorithm in 1996 that is said to be a search algorithm in a database but has many more use cases as we'll see in the quantum algorithms part of this book (page 442). He currently works in the Department of Mathematics of the Guru Nanak Dev University, in Punjab, India. His full name is Lovleen Kumar Grover.



**David Simon** (American) is the creator of another search algorithm in 1994, bearing his name. Precisely, his quantum algorithm solves the hidden subgroup problem (HSP), providing an exponential acceleration comparer to classical computing. David Simon worked at Microsoft Research when he created his famous algorithm. I've had a hard time finding where and what he was working on now. His name makes it difficult to search information on him :)



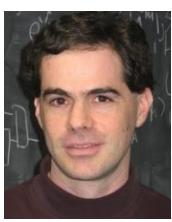
**Michael Freedman** (1951, American) is a mathematician who founded and runs the Microsoft Station Q laboratory in Santa Barbara, California. He is one of the fathers of topological quantum computing along with Alexei Kitaev. He was also awarded the Fields Medal in 1986 for his work on the Poincaré conjecture, later demonstrated in 2006 by Grigori Perelman.



**Alexei Kitaev** (1963, Russian and American) is with Michael Freedman one of the fathers of the topological quantum computer concept in 1997, investigated by Microsoft. He was a researcher at Microsoft Research in the early 2000s and is now working at Caltech University. He has also done a lot of work on error correction codes, including the creation of *surface codes* and *magic states distillation* (with **Sergey Bravyi**) and the Quantum Phase Estimate algorithm, used in Shor's integer factorization algorithm.



**Aram Harrow** (American) is a prolific specialist in quantum algorithms. He teaches both quantum physics and quantum computing at MIT. At MIT, he is surrounded by Peter Shor and Charles Bennett. He is the co-author of the HHL quantum algorithm used to solve linear equations which he created jointly with Avinatan Hassidim and Seth Lloyd<sup>81</sup>. He is also interested in the creation of hybrid classical/quantum algorithms.



**Daniel Gottesman** (1970, American) is a physicist from the Perimeter Institute in Waterloo, Canada. He did his PhD thesis at Caltech under the supervision of John Preskill. He is known for his work on quantum error correction codes (QEC) and is co-author of the famous Gottesman-Knill's theorem according to which a quantum algorithm using only Clifford gates can be efficiently simulated (meaning, polynomially) on a classical computer.

Clifford group quantum gates are based on half and quarter-turn rotations (of the qubit in the Bloch sphere), Hadamard gate and the C-NOT conditional gate. This theorem thus indirectly proves that a basic gate set is insufficient to generate an exponential quantum advantage.

We need to add a T gate to make it possible to approximate any arbitrary unitary transformation, meaning, any move within the Bloch sphere for single qubit operations. This is particularly important for the Shor algorithm.



**Gil Kalai** (1955, Israeli) is a professor of mathematics at the Hebrew University of Jerusalem and at Yale. His main ambition is to demonstrate mathematically that it will be impossible to create real universal quantum computers, due to their error rate, even with error correction codes and the notion of logical qubits that assemble physical qubits. He also questioned the reality of the October 2019 Google supremacy performance.



**Andrew Steane** (1965, English) is a Professor of Physics at Oxford University. He created the so-called Steane quantum error correction code in 1996. This code corrects flip and phase errors on a single qubit. Looking at how it works provides good insights on the inner workings of quantum error correction codes, although this particular code will probably not be used when we'll have scalable quantum computers. Other more sophisticated QEC codes are planned like color codes and surface codes.

---

<sup>81</sup> See [Quantum algorithm for linear systems of equations](#), 2009 (24 pages).



**Scott Aaronson** (1981, American) teaches information science at the University of Austin in Texas. He is a leading expert in quantum algorithms and complexity theories. He is notably at the origin of a quantum algorithm used for boson sampling, a way to demonstrate some quantum advantage for photonic based experiments. Bosons are integer spin particles such as photons, while particles such as electrons, neutrons and protons are fermions, with a spin 1/2.



**Dorit Aharonov** (1970, Israel) is a quantum algorithms researcher. She received her PhD in Computer Science in 1999 at the Hebrew University of Jerusalem on "Noisy Quantum Computation" and then did a post-doc at Princeton and Berkeley. She is credited with the "quantum threshold theorem" co-demonstrated with Michael Ben-Or which states that below a certain error rate threshold, error correction codes can be recursively applied to obtain an arbitrarily low error rate of logical qubits.

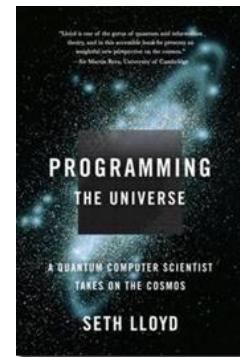
This is a very theoretical mathematical approach that doesn't take into account the way noise is also scaling as we increase the number of qubits. Dorit Aharonov's uncle is **Yakir Aharonov** (1932, Israeli), a physicist who had worked with David Bohm, among others.



**Seth Lloyd** (1960, American) is a professor at MIT who is a prolific contributor to quantum information and quantum algorithms. He is the initiator of Quantum Machine Learning, of the concept of qRAM (quantum random access memory), of continuous variables gates-based quantum computing (1999), of quantum radars (2008). He's also the L in the famous HHL quantum linear equation solving algorithm and worked on quantum error correction codes and quantum biology.

In his 2006 book, Programming the Universe, Lloyd contends that the universe itself is one big quantum computer producing what we see around us, and ourselves, as it runs a cosmic program. According to Lloyd, once we understand the laws of physics completely, we will be able to use small-scale quantum computing to understand the universe completely as well. In about 600 years.

Seth Lloyd was laid off from MIT in 2019 then put on leave, then on disciplinary actions for a period of five years starting in 2020 because he had not informed his management of some Jeffrey Epstein originated funding.



**Alan Aspuru-Guzik** (circa-1978, American) is a research director at the University of Toronto, formerly at Harvard, who, among other things, created various quantum chemistry algorithms, a topic we will cover in the section dedicated on quantum algorithms. He is also the co-founder of the Zapata Computing, a startup developing quantum computing software frameworks, particularly in chemical simulation.



**Elham Kashefi** (1973, British-Iranian) is a research director at CNRS in France, in the LIP6 laboratory from Sorbonne University. She is the co-founder with Marc Kaplan of VeriQloud, a secure quantum telecommunications startup. She is also teaching quantum information science at the University of Edinburgh. Originally a mathematician and computer scientist, she became a specialist in quantum communication protocols and quantum algorithms, around topics like code verification and blind quantum computing.

She did her PhD thesis "Complexity Analysis and Semantics for Quantum Computation" at the Imperial College of London in 2003 under the co-supervision of Peter Knight. She created the BFK blind computing protocol in 2009 with Anne Broadbent and Joe Fitzsimons.

With her team at LIP6, she is at the origin of the creation of a site on the zoo of quantum communication protocols<sup>82</sup>. And as this was not enough, she is also versed in Quantum Physical Unclonable Functions (QPUF), physical identifiers of quantum and tiltable objects that we will explore in an upcoming edition of this ebook.



**Anne Broadbent** (Canadian) is a mathematician from the University of Ottawa specialized in quantum computing, quantum cryptography and quantum information. She was a student of Alain Tapp and Gilles Brassard at the Université de Montréal. She created the BFK blind computing protocol in 2009 along with Elham Kashefi and Joe Fitzsimons.

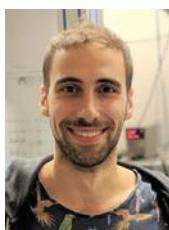


**Maria Schuld** (c. 1989, German) is a researcher at Xanadu, based in South Africa at the University of KwaZulu-Natal in Durban. She is a key contributor to the development of quantum machine learning algorithms, particularly in the field of pattern recognition.



**Mazyar Mirrahimi** (circa 1980, Iranian) is a mathematician who moved to quantum physics. He is currently the director of Inria's Quantic laboratory, which specializes in error correction codes and quantum algorithms, among other topics. He did his post-doc with Michel Devoret at Yale. Back in 2013, he published a seminal paper on cat-qubits.

These are physical qubits using a cavity and a superconducting qubit that self-corrects some errors, starting with flip errors. These cat-qubits are used by the startup Alice&Bob as well as by Amazon, as announced in December 2020.



**Zaki Leghtas** (Morocco/France) is a researcher based in France in Mazyar Mirrahimi's team and is also specialized in error correction codes and systems. He is notably one of the creators of cat-qubits mentioned above. These are supposed to enable the creation of logical qubits with fewer than 100 physical qubits. He worked in Michel Devoret's laboratory at Yale before joining Inria's Quantic team in 2015.



**Shi Yaoyun** (1976, Chinese) is a professor at the University of Michigan and also leading the Alibaba Quantum Laboratory. He created various records of quantum simulation on server clusters that we will describe in this ebook. He earned a computer science PhD from Stanford. He also worked on quantum cryptography and certifiable randomness.



**Kristel Michelsen** (circa-1969, Belgian) is a physicist working at the University of Aachen in Germany and at the Jülich Supercomputing Centre (JSC). She has contributed to numerous works in quantum computing both in physics and algorithms. She created the [QTRL scale](#), for Quantum Technology Readiness Level, that is used to evaluate the level of maturity of quantum technologies and which we will discuss in the section dedicated to [practices in research](#).

---

<sup>82</sup> See [https://wiki.VeriQloud.fr/index.php?title=Protocol\\_Library](https://wiki.VeriQloud.fr/index.php?title=Protocol_Library).



**John Watrous** (Canadian) is a researcher working at the University of Waterloo, Canada, specialized in quantum algorithms and complexity theory. He demonstrated some complexity classes equivalencies like QIP is in EXP and QIP=PSPACE. He also worked on cellular automata. He had previously collaborated with Scott Aaronson. He is the author of the voluminous [The Theory of Quantum Information](#), 2018 (598 pages).



**Ryan Babbush** (circa-1989, American) is a Google researcher working on quantum simulation algorithms. His goal is to create commercial quantum chemistry solutions. In a February 2020 [presentation](#), he did show that chemical simulation with Google's Sycamore 53 qubits processor could not use more than 12 qubits because of its high error rate.



**Matthias Troyer** (1968, Austrian) is Professor of Computational Physics at ETH Zurich. He joined Microsoft Research in Redmond at the beginning of 2017. He is one of the creators of the Q# language for quantum programming and of the open-source framework ProjectQ launched in 2016 by ETH Zurich. He is particularly interested in chemical simulation with quantum computers. He received his PhD from ETH Zurich in 1994.



**Krysta Svore** (c.1978, American) is currently the general manager of quantum software at Microsoft. She has a Ph.D. in Computer Science from Columbia University. Her contribution in quantum information science covers a broad range of topics: MBQC, quantum machine learning, contributing to the creation of the LIQUiD quantum programming language, surface codes, fault-tolerance quantum computing.



**Iordanis Kerenidis** (c. 1980, Greek) is a director of research from CNRS at IRIF (Institut de Recherche en Informatique Fondamentale), working on cryptography, quantum communication, quantum complexity theories and quantum machine learning, his latest specialty. He did his thesis at MIT under the supervision of Peter Shor and worked in the same office as Scott Aaronson and also worked at Berkeley with Umesh Vazirani. He is part of the founding team of QC Ware.

There he leads the R&D in quantum algorithms. He also co-leads the Paris Quantum Ecosystem (PCQC) with Eleni Diamanti. He was one of the members of the parliamentary mission on quantum technologies led by MP Paula Forteza between April 2019 and January 2020.



**Frédéric Magniez** (French) is the Director of the CNRS IRIF laboratory mentioned above. He also runs a Chair at Collège de France in Spring 2021. His research focuses on the design and analysis of randomized algorithms for processing large datasets, as well as the development of quantum computing, particularly algorithms, cryptography and its interactions with physics. In 2006, he founded and led the national working group for quantum computing, bringing together 20 research groups.



**Benoît Valiron** (1980, France) is a researcher at the CNRS LIR laboratory from Université Paris-Saclay and teaching quantum programming and algorithms, including at CentraleSupélec. This quantum programming specialist is the co-author of the open-source quantum programming language Quipper, which he contributed to create while being at the University of Pennsylvania.



**Bettina Heim** (c. 1980) is a Microsoft developer specializing in quantum software. She is responsible for the development of the quantum programming language Q# compiler, promoted by Microsoft since 2017 and which is part of their Quantum Development Kit, currently running on quantum emulators on traditional processors and now supported on third party hardware proposed on the cloud, including IonQ and Honeywell trapped ion based quantum processors.



**Cristian Calude** (1952, Romanian/New Zealander) and **Elena Calude** (Romanian/New Zealander) are researchers from the Institute of Information Sciences, University of Albany in Auckland, New Zealand. They work on quantum algorithms, hybrid quantum algorithms and complexity theories.



**Sophia Economou** (c. 1980, Greek-American) is an Associate Professor in the Department of Physics at Virginia Tech College of Science. She previously worked at the US Naval Research Laboratory. She is a physicist specialized in the control of quantum dot semiconductor spins and their spin-photon interfaces. She is also a creator of advanced molecular simulation algorithms on quantum computers.



**Ewin Tang** (2000, American) published in July 2018 a paper demonstrating a classical recommendation algorithm as efficient as an algorithm designed for D-Wave quantum computers by Iordanis Kerenidis and Anupam Prakash in 2016<sup>83</sup>. They responded by finding a flaw in the reasoning. On close inspection, the quantum algorithm would scale better in some extreme conditions. She was 18 years old at the time. Ewin Tang is now a computer scientist at the University of Washington.



**Cyril Allouche** (French) has been leading Atos R&D efforts in Quantum Computing since its beginning in 2015. Cyril Allouche are the "implementers" of the quantum vision of Thierry Breton, CEO of Atos until 2019. His work encompasses developing the aQASM (Atos Quantum Assembly Language) quantum programming language and the myQLM quantum programming emulator running on regular personal computers and servers.

Here we are. We've covered a whole lot of people and probably missed many who should be in this hall of fame list! I'll update it whenever required. We will encounter many of these scientists in this ebook.

## Research for dummies

As I investigated the broad quantum science and technology landscape, I learned more on how fundamental and applied research was operating.

I did not know much about it before this adventure. Working in the ‘digital world’, as a developer, marketer and in the entrepreneurial ecosystem doesn’t necessarily make you look deeply into the inner workings of research. I discovered many aspects that I am detailing here, particularly with regards to practices, lingua-franca, careers and evaluations.

---

<sup>83</sup> See [A quantum-inspired classical algorithm for recommendation systems](#), Ewin Tang, July 2018 (32 pages) and [Major Quantum Computing Advance Made Obsolete by Teenager](#) by Kevin Harnett, July 2018.

If you're a researcher, this is very basic stuff that you already know fairly well. For others, it will clarify some of vague understanding you might have on how research works.

## Long-term

The first key point is the long-term approach in quantum technologies. It can also be found in other branches of physics and so-called deep-tech related sciences. Time scales are measured in decades. It starts with intuitions, creativity, passion, rigor and hard work. These ideas are not always broadly adopted right away. There's always some resistance with the current scientific establishment.

This long-term history can be observed in condensed matter physics. Brian Josephson devised the Josephson junction in 1962. IBM tried to use it unsuccessfully to build superconducting computers. Anthony Leggett made significant discoveries in the early 1980s which led to the creation of the first superconducting qubits in the early 2000s and to Google and IBM's superconducting machines between 2016 and 2020. And we're not done there since this technology's scalability has not yet been proven.

Alain Aspect's work, which started in the late 1970s and culminated with his 1982 experiment had no immediate industrial application. Fortunately, he was well supported by many laboratories, particularly to build the necessary instrumentation. His work led to the creation of many of the branches of quantum technology. For example, Artur Ekert was inspired by Alain Aspect's work to advance the field of quantum cryptography in the early 1990s.

All of this cannot be meticulously planned in advance. Research serendipity must prevail. Commercialization comes later, through meetings between specialists from different and complementary disciplines. Innovators are either the researchers themselves, or more generally others, engineers and entrepreneurs, who know how to detect research work having some business potential. Hence the importance of bringing them together in innovation ecosystems. However, in its current shape, the quantum startup ecosystem is mostly made of researchers turned into entrepreneurs.

This generates its share of misunderstandings with public authorities. They are tempted to over-evaluate and measure the performance of basic research, if not to fund it, using only criteria from the business world. On the other hand, and this is particularly true for quantum technologies, research work requires peer reviews. This may give the impression that researchers are both judge and jury. To prevent this from driving decision-makers and people suspicious, research work must honestly be translated in layman's terms. This should encourage researchers to communicate with broader audiences than their peers. It requires leadership. Scientists must be more involved there, particularly in those times where people are more and more skeptic on science and innovation.

## Publications

This document contains many references to scientific publications. I do this almost systematically and always look for the original scientific publication whatever the news.

Research is now frequently published first in open access in the famous **Arxiv** site from Cornell University. These are articles "prepublications" that have not yet gone through peer reviews and be published in peer-reviewed journals. These articles must sometimes be taken with a grain of salt. However, they allow authors to collect comments from informed readers. Their quantity and quality depend on the author's fame, the topic and the number of researchers who master it<sup>84</sup>.

---

<sup>84</sup> See [Comment bien lire et comprendre une étude scientifique](#) par Gary Dagorn, Mathilde Damgé et Bessma Sikouk, May 2021. It provides a lot of insights on how to read a scientific paper. You can translate this article in French in your browser. Also look at [Ten simple rules for reading a scientific paper](#) by Maureen A. Carey, Kevin L. Steiner and William A. Petri Jr, July 2020.

Between 9 and 18 months later, a paper publication in a peer-reviewed journal may follow. If the delay is too short, it may mean the journal is a predatory one. It is usually published mostly as is, includes some revisions suggested by the "referees" of the review committees, or even with a change of title. In these cases, the version published on Arxiv is not necessarily the most recent. It is sometimes updated. The benefits are openness and free access.

As a general rule, when I discover the existence of an article, I search for it on Google Search with the name followed by "filetype:PDF" and I find it free of charge in more than 90% of the cases on Arxiv or on the ResearchGate site, the researchers' reference social network.

Quantum technologies peer-reviewed<sup>85</sup> journals include **Nature** and its various thematic variations like **Nature Communications**, **Science**, **Physical Review X**, **Physical Review Research**, **Physical Review Letters**, **Quantum Science and Technology**, **Journal of Applied & Computational Mathematics**, **International Journal of Quantum Information**, **Quantum Engineering**, **Advanced Quantum Technologies**, **Quantum Journal**, **Quantum Information Processing**, **IEEE Journal of Quantum Electronics**, and **IEEE Transactions on Quantum Engineering**. Fortunately, in this field, there are only a few predatory journals that do not have peer-review process and charge researchers for their work publication.



PhD theses are easier to retrieve and are generally published freely. These are usually good sources of bibliographical information. Beyond the main thesis goal that is to advance science in a usually narrow domain, it generally starts with making an inventory of the state of the art, like in review papers. Review papers present a state of the art of a field. Their bibliography is generally impressive, sometimes as long as the paper itself. They are a good starting point to study a subject, especially if the paper is not too old. I provide links to many such review papers, particularly on specific qubit types. If the author's pedagogy is good, it can be very useful for learning on your own. A bibliography generally allows you to go deeper into the subject by discovering the need-to-know fundamental texts.

Several authors are usually mentioned in scientific papers. It can be a very large number. In general, beyond three authors, the first is the one who was the owner and done the bulk of the work. It's usually a PhD student or a post-doc. He/she has processed the experience and written a large part of the document, but this may depend on countries, laboratories and thesis supervisors.

---

<sup>85</sup> In peer-reviewed journals, the reviewers are unknown to the paper authors. They provide some feedback on the paper and expect a paper update. The authors provide an updated version and comments that are either accepted or rejected by the reviewer. It can lead authors to modify their claims and even their paper title. When everything's finalized, the paper can be published. Nowadays, the initial paper published on Arxiv is also updated to reflect these changes. There is also a special double-blind review process where the authors are unknown from the reviewers to avoid any reviewer bias. I have bumped only once on such a case in quantum technologies, on a QML algorithm: [On the universal approximability and complexity bounds of deep learning in hybrid quantum-classical computing](#), 2021 (15 pages).

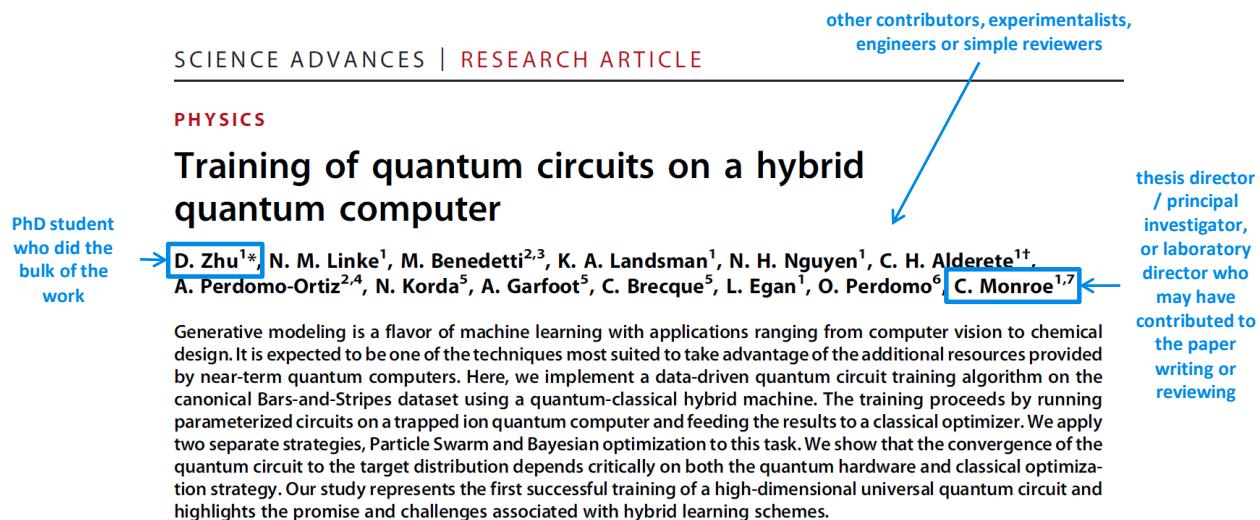
The last one is the thesis or research laboratory supervisor<sup>86</sup>. In the latter case, the penultimate author is the thesis director who supervised the work. In between are the other contributors, experimenters or simple reviewers. When quoting an article without mentioning all contributors, I use the expression "et al" which is an abbreviation of the Latin "*et alia*", meaning "*and the others*".

In many countries, such as the USA, it is common practice to mention authors with the initials of their first and *middle names*. It does not make it easy to search them online, especially for Chinese authors. This is particularly the case when there are many contributors. I try to quote authors with their first and middle name when they are easy to be found.

Some papers are provided with some *supplemental materials* with technical details. It can be very interesting, like for example, to describe the experimental setup and hardware engineering.

These scientific publications can be discovered by following the RSS feeds of Arxiv, reference specialized papers, in addition, from scientific news feeds of online media or popular scientific press. I also discover new interesting papers with scanning scientific conferences presentations<sup>87</sup>.

In the case of quantum technologies, the "tech" media often broadcasts scientific news dressed up with sensationalism and exaggerations. This often stems from the propensity of laboratory communicators or sometimes researchers themselves to make shortcuts between their work and its potential usage that may be very long-term<sup>88</sup>.



It is even stronger when the communication comes from a large company such as Google or when the article was written by the laboratory's communication branch.

The job of the technology screener consists in sorting this out. When your local non-English speaking press relays such information, it is often necessary to start by identifying the original article which is possibly quoted at the end of the article. Sometimes, you discover blatant translation error that entirely twists the scope of the covered scientific advance.

<sup>86</sup> This is the case of these hundreds of publications with the famous Didier Raoult who is cited as the last contributor, as laboratory director but not necessarily thesis director.

<sup>87</sup> Here is an example of IEEE [superconducting technologies](#).

<sup>88</sup> The example below comes from [Scientists take step towards quantum supremacy](#) by National University of Science and Technology MISIS, March 2021. The supremacy from the article title is very far away considering the paper is about some sensing technology to measure the efficiency of some superconducting qubit.

Next, one must find the original scientific article with the methods described above. Once all this has been done, the bulk of the work consists in classifying the information: what is it about and how does it fit into the web of quantum technologies<sup>89</sup>. What is the actual progress made with regards to the state of the art? You can rely on classical recommendations: read the introduction and not just the abstract, identify the problem that the writers are trying to solve and how they are advancing the state of the art, look at the data and identify any missing data, and read the conclusion. If you can't decipher the paper content, make a search of other more generalists web sites mentioning it.

In general, a paper presenting a breakthrough that will allow the quantum computer to be realized at room temperature or ahead of all others becomes a simple very one-time breakthrough in the development of a particular type of qubit. It looks like your tiny hairy dog after the shower!

In many cases, quantum science-related papers are inaccessible, requiring solid mathematical and/or physics background. Even quantum science specialists have a hard time interpreting many papers. You frequently come across a set of Russian dolls concepts with unknown concepts referring to other unknown concepts and so on. However, hopefully, some founding papers do not use too much jargon and manage to deal with a big fundamental question by making it understandable to many specialists in their discipline and well beyond. This is often the case with publications in Nature.

How can I check the whole thing, particularly given the specialists in my own network have not yet had the time to do so? You either have to be patient, do it on your own, or look for someone who has done the job. For big news related to quantum computing, one can wait for the next post from Scott Aaronson or a laconic tweet from John Preskill.

Finally, I use Arxiv as soon as I come across a startup that defines in too broad terms what it does without any technology specifics. It's so commonplace now! A search starts with finding the startup scientific founder, then with identifying their research work that they are probably willing to package in their freshly created startup.

(1) MARCH 18, 2021

## Scientists take step towards quantum supremacy

by National University of Science and Technology MISIS



Qubit production process. Credit: Sergey Gruskov/NUST MISIS

A Russian-German research team has created a quantum sensor that grants access to measurement and manipulation of individual two-level defects in qubits. The study by NUST MISIS, Russian Quantum Center and the Karlsruhe Institute of

this would mean they are building some sort of quantum computer...

... but it's just about a new sensor measuring the quality of superconducting qubits using some new materials

Article | Open Access | Published: 05 February 2021

## Quantum sensors for microscopic tunneling systems

Alexander Bilmes, Serhii Volosheniu, Jan David Brehm, Alexey V. Ustinov & Jürgen Lisenfeld

*npj Quantum Information* 7, Article number: 27 (2021) | Cite this article

836 Accesses | 8 Altmetrics | Metrics

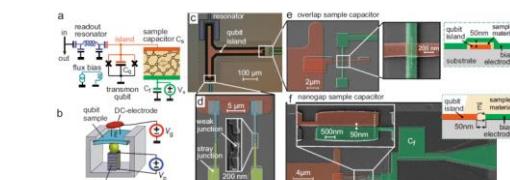


Fig. 1 Experimental setup and qubit sample. a Schematic of the transmon qubit circuit to study TLS in deposited materials. The qubit island is connected to ground by an additional small capacitor containing the material to be studied. b Setup for tuning TLS by applied magnetic field. c Schematic of the readout resonator. d Cross-section of the qubit island. e Schematic of the qubit island with zoomed onto one of the small Josephson junctions. The large Josephson junctions are highlighted in light green. f Sample capacitor in overlap geometry as used in this work. It employs a 50-nm thick layer of AlO<sub>x</sub> as the sample dielectric. g An alternative sample capacitor design consists of two coplanar electrodes separated by a so-called 'nanogap' of a few tens of nm. Here, the sample material can be deposited in a last fabrication step (see inset), or the nanogap can be left uncovered to study individual TLS in native surface oxides.

In the hundreds footnotes in this ebook, I otherwise take the liberty of not using the cryptic description conventions that appear in the abundant bibliographies of scientific publications, sometimes using authors, publication references but not the title! I use a clear title convention followed by first

<sup>89</sup> Various tools attempt to automate this sorting work, such as [In Laymans Terms: Semi-Open Relation Extraction from Scientific-Texts](#) by Ruben Kruiper et al, May 2020 (13 pages). It is currently applied to the field of biology.

author/authors, sometimes their research laboratories or companies, publication date and then number of pages or slides, which allows you to identify at a glance the volume and depth of the referenced documents<sup>90</sup>.

We must recognize our limits and understand that we're not protected from believing scientific hoaxes like the famous one created by **Alan D. Sokal** in 1996. It merged social sciences and quantum gravity and was published in a social science publication, not a quantum physics one<sup>91</sup>.

Hopefully, quantum scientific publications are way more serious than most of the quantum hype that is conveyed by general news with their amazing amplification capabilities. You'll read time and again that quantum computing will drive autonomous cars, create quantum intelligent robots, reduce CO<sub>2</sub> emissions, cure cancers, help Tesla (but not others) build top-notch batteries or that quantum communications will teleport your data faster than light around the Earth. Most of these assertions will flourish when the IBMs and Googles of this world make fancy announcement or after your government launches its own “billion dollars” national quantum plan. But they are at least unproven if not entirely false. Who's going to reveal it to you?

## Roles

In most countries and in all disciplines, several roles can be distinguished in research organizations.

**Doctoral students** are students who are undertaking a doctoral thesis (PhD, for Philosophy Doctorate, for any science). It lasts from three to five years depending on the country. This thesis completes a higher education program in the University.

**Post-docs** or post-doctoral researchers are researchers who, after having obtained their PhD, conduct research in a laboratory under a fixed-term contract. They sometimes do several post-docs in different locations, frequently out of their originating country. It is the anteroom of a full-time research position.

**Researchers** in some countries like France are civil servant researchers recruited through open competitions in major public research institutions such as the CNRS or Inria.

**Habilitation to Direct Research** (HDR in France) allows a tenured researcher to direct the thesis of one or more doctoral students as a thesis director and to obtain a university professorship. The rules vary from country to country, such as having completed two doctoral theses and having published internationally recognized work in one's field<sup>92</sup>.

**Principal Investigator** or **Research Director** are researchers with the possibility to autonomously determine the field of their research work. They supervise several doctoral students when they are successful with finding the related public and/or private funding. They are also selected by competition in research institutions. Depending on the country and research organization, there are several grades in the function, linked to advancement over time and merit.

In France, a **Joint Research Unit** (UMR, Unité Mixte de Recherche) is a research laboratory that associates a CNRS laboratory and a third-party laboratory such as a University, another research organization or a private company. It is an administrative entity resulting from the signature of a multi-year contract, usually four years, between the parties involved. Most of the research laboratories associated with Grandes Ecoles (LKB of the ENS for example) or Universities that are cited in this document are UMRs.

---

<sup>90</sup> This is a feature I'm surprised is not yet provided by search engines like Google Search.

<sup>91</sup> See [Transgressing the Boundaries: Towards a Transformative Hermeneutics of Quantum Gravity](#) by Alan D. Sokal, 1996 (39 pages).

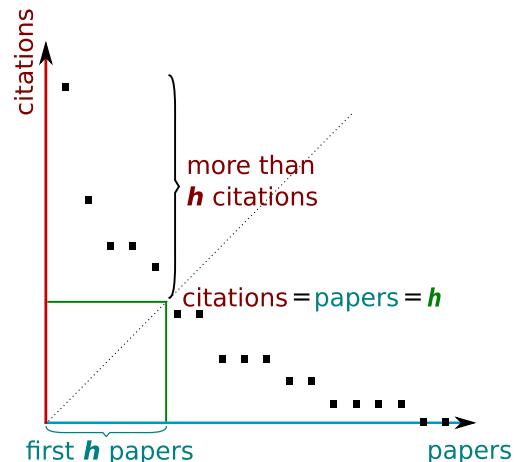
<sup>92</sup> This habilitation replaced the Doctorat d'Etat in 1984 in France. The HDR is considered to be a diploma. It is awarded on free application by the research commission of the Universities which deliberates in the form of a jury.

In addition to these roles, let's not forget the **laboratory technicians** who set up the experiments and about whom less is said and the **engineers** who can play a role in the creation of many scientific instruments.

## **h-index**

The h-index, named after its creator Jorge Hirsch in 2005, is an index that quantifies a researcher's productivity and scientific impact. It is based on the level of citations of his scientific publications in peer-reviewed journals. It is a bit like a PageRank for a website, but a simpler one. It is an integer corresponding to the number of papers  $h$  that have each obtained more  $h$  citations in other papers.

The level of h-index can be used as a quantitative data for obtaining a position as a resident researcher (10-12), professor ( $>18$ ) or member of an academy of science ( $>45$ ).



As with any composite index<sup>93</sup>, it generates side effects: a race to “publish or perish” papers of little incremental value, cross-referencing between researchers, self-citation, an abundance of co-authors<sup>94</sup>, etc.

Some alternatives indexes have been proposed like the recent h-frac, but not yet adopted<sup>95</sup>. It remains, however, an interesting indicator of the influence of researchers and their production volume.

On average, the h-index of a researcher in physics is close to the length of his career since his PhD. It obviously evolves over time. It is full of flaws like all quantitative indicators. For example, the basic h-index does not distinguish between main author and co-author. Hence the abundance of authors cited in many papers, some of them having made only marginal contributions.

The index is usually calculated from **Google Scholar** data, but it is sometimes found calculated only on the SemanticScholar website. The most serious index is provided by the Website of **Science** because its database is the cleanest.

## **Fake news**

Science is not exempt of fake news. In all scientific fields, some researchers may publish questionable results for their experiments, aggregate and compile tinkered data, or simply avoid taking into account embarrassing data, generating a survivor bias. This can happen in quantum technologies, particularly when evaluating the quality of experimental qubits or, for instance, finding Majorana zero modes, *aka* fermions. In general, you need to be an expert in the field to identify this kind of abuse. They however seem rare in quantum technologies.

<sup>93</sup> The Shanghai ranking list of universities comes to mind.

<sup>94</sup> This example comes from Google with 85 co-authors: [Implementing a quantum approximate optimization algorithm on a 53-qubit NISQ device](#) by Bob Yirka, February 2021 (19 pages). It's a bit too much and we can wonder about their all contributions!

<sup>95</sup> See [The h-index is no longer an effective correlate of scientific reputation](#) by Vladlen Koltun and, David Hafner, Intel Labs, February 2021 (26 pages). Among other things, the authors found out that the correlation between h-index and scientific awards in physics is declining. They propose an alternative index named **h-frac**, for h-fractional, that improves the correlation between the index and other scientometric measures like scientific awards. It allocates citations fractionally and evenly among all coauthors of scanned papers to avoid the phenomenon of low-contribution hyperauthors.

With a generalist technological knowledge in the domain, one can start to detect tricks of the trade or exaggerations. This is easier to do with commercial vendors like with IBM and their quantum volume, Honeywell and their "*most powerful quantum computer in the world*" or with the Google and Chinese quantum supremacy experiments.

## Poster sessions

In a scientific conference, a "poster session" is usually a part of the conference dedicated to the presentation of researchers' projects during a break, in a dedicated area.

Researchers display a poster describing their research work and talk with conference participants as they stroll through the conference exhibition area during dedicated breaks. It is an exercise in humility reminding what Jehovah's witnesses are doing in the streets.

## Figures of merit

This common expression broadly describes a set of specifications and the success metrics to be achieved to bring a given technology to fruition. DiVincenzo's qubit technology criteria can be considered a figure of merit for success for quantum computing. It usually provides a roadmap and set of goals for researchers and technology vendors.

## International

Nowadays, all modern countries have crafted their "quantum national plan" with a certain willingness to better control their sovereignty. It's like being the first with the atomic bomb during World War II.

But let's remember that international collaboration between researchers is intense. Most of those I met in French laboratories collaborate with colleagues either in Europe within the framework of Europe 2020 projects, the European Flagship or for some ERCs. They also collaborate with researchers outside the European Union, particularly in Asia (Japan, Singapore), as well as in the USA, UK, Switzerland and Australia<sup>96</sup>.

Quantum science knowledge is quite open and is rather well shared on a global scale. This is encouraged by many international scientific conferences where knowledge is being built, researchers get to know each other and joint projects are being launched. This is one of the reasons why I don't believe in the existence of a supposed quantum computer whose capabilities would defy understanding and which would be hidden in the basement of a secret NSA datacenter to break all the RSA keys of the Internet.

Scientific nationalism in quantum technologies finally comes into play further downstream of research, when it comes to transforming it into industrial advantage. Technologies often have their "magic sauce", as in semiconductor manufacturing processes. This has always been the case in digital technologies.

## Technology Readiness Level

This technology readiness level notion is commonly used in deep techs. It describes the level of maturity of a technology with a scale from 1 to 9. It follows a relatively standardized classification initially created by NASA in 1975<sup>97</sup>, then used by the European Union and various other organizations. It was initially mainly used in the aerospace, defense and energy industries.

---

<sup>96</sup> This can also take the form of CNRS International Mixed Units such as those established in Japan and Singapore.

<sup>97</sup> See [Technology Readiness Levels at 40: A Study of State-of-the-Art Use, Challenges, and Opportunities](#) by Alison Olechowski et al, 2015 (11 pages) which is the source of the diagram.

This scale can have several use cases. It is used to assess the level of risk and maturity for an investor in a startup. Very advanced deep techs are also the playground of TRL and quantum technologies are no exception.

Pre-concept Refinement			Concept Refinement	Technology Development		System Development & Demonstration		Production & Deployment	
◆ A			◆ B			◆ C			
TRL 1	TRL 2	TRL 3	TRL 4	TRL 5	TRL 6	TRL 7	TRL 8	TRL 9	

The TRL scale has 9 levels<sup>98</sup>:

- **TRL 1:** basic principles are described or observed, at the theoretical or experimental stage.
- **TRL 2:** technological concepts are formulated and not yet necessarily tested.
- **TRL 3:** proof of concept is carried out in a laboratory, at the level of the technical process.
- **TRL 4:** the technology is validated in the laboratory as a whole.
- **TRL 5:** a technology model in a production grade environment is created.
- **TRL 6:** a technology prototype is demonstrated in an environment representative of the intended use case.
- **TRL 7:** a prototype is evaluated in an operational environment.
- **TRL 8:** a complete system has been evaluated and qualified.
- **TRL 9:** a complete system is operational and qualified in production.

The relevance of the solution to market needs is missing at this scale, but it is a marketing rather than a technical consideration<sup>99</sup>. Most of the time, it more or less coincides with TRL levels 7 to 9 since reaching this scale requires funding and finding customers willing to test the solution.

**Kristel Michielsen** has proposed a scale suitable for quantum computing, the [QTRL](#), for the Quantum Technology Readiness Level *below*<sup>100</sup>. Her assessment of some technologies can be argued.

For example, she places D-Wave's quantum-annealed computers in TRL 8 and 9. This is commercially correct since these computers are well marketed. This being said, if they are well available physically, it is not proven that they are of much use at the moment.

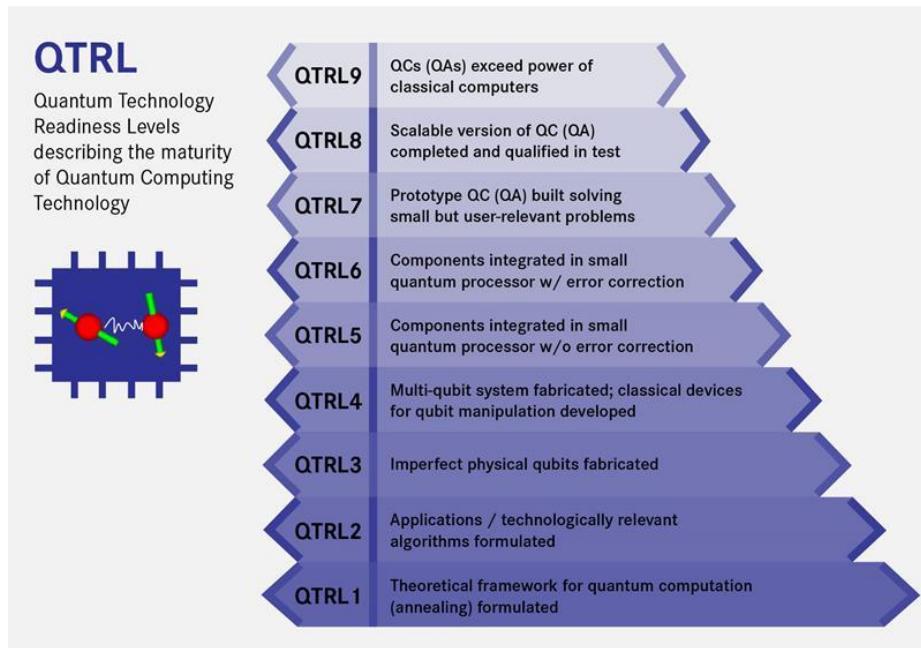
The specificity of quantum technologies is that many hardware startups are created with very low TRLs. This is particularly true for those who are starting to design qubits using technologies that have not yet been proven, even in the labs. In quantum technologies, the notions of "MVP" (minimum viable product) are very different from the classical digital world. It's based on scientific rather than functional metrics. We have many such startups around in quantum technologies because of the famous FOMO (fear of missing out) syndrome with investors.

---

<sup>98</sup> Source of the diagram [above Some explanations on the TRL \(Technology readiness level\) scale](#), DGA, 2009 (15 pages). See also [Technology Development Stages and Market Readiness](#) by Surya Raghu, June 2017 (35 slides).

<sup>99</sup> See [TRL, MRL, POC, WTF?](#) by Massis Sirapian of the Defense Innovation Agency, April 2019.

<sup>100</sup> See her presentation [Simulation on/of various types of quantum computers](#) by Kristel Michielsen, March 2018 (40 slides).



This shows up with investors who fear of missing the future golden goose or unicorn. They are ready to overinvest in companies they perceived will be the future market champion. This explains for example the level of funding for startups like **Rigetti** and **PsiQuantum** or the new SPAC funding mechanism (special purpose acquisition company) implemented by **IonQ** and the recent quantum business spin-off from **Honeywell** and its merger with **CQC** (becoming Quantinuum as of December 2021).

### Quantum physics history and scientists key takeaways

- A first wave of 19<sup>th</sup> century scientists laid the groundwork that helped create quantum physics afterwards (Young, Maxwell, Boltzmann, mathematicians). The photoelectric effect, black body spectrum and atoms emission or absorption spectrum were not explained with the current theoretical frameworks.
- Starting with Max Planck, a second wave of scientists (Einstein, De Broglie, Schrodinger, Heisenberg, Dirac, Born, Von Neumann) created quantum physics to describe light/matter interactions, energy quantification and wave-particle duality. It solved most of the 19<sup>th</sup> century unexplained physics experiments.
- These scientists were theoreticians while many lesser-known researchers were experimentalists with landmark discoveries (superconductivity, electron interferences, Stern-Gerlach experiment, ...).
- After World War II all digital technologies (transistors, lasers, telecommunications) were based and are still based on quantum physics, as part of what is now called the first quantum revolution.
- Since the 1980s and thanks to advances in individual quantum objects control and the usage of quantum superposition and entanglement, a new breed of technologies were created, most of which belong to the “quantum information science” field and are part of the second quantum revolution.
- Many of these research studies were funded by governments after Peter Shor’s factoring algorithm was created.
- While the first quantum revolution was driven by research coming mostly out of Europe, the last wave comes out of all developed countries across several continents (North America, Europe, Asia/Pacific).

# Quantum physics 101

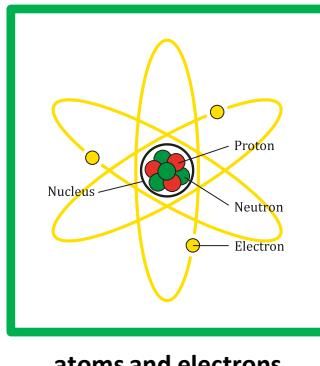
After a historical review of quantum physics and computing with its most important contributors, let's look at the fundamentals of quantum physics in a more structured way. Whatever the ups and downs, this field has gone through the test of time for nearly a whole century. Thousands of experiments have validated the theory and mathematical formalism behind it even though we still can't explain what's happening at a physical level, particularly with quantum entanglement or, even, with the wave-particle duality phenomenon with electrons and photons.

Several years of undergraduate and graduate studies are usually necessary to master quantum physics notwithstanding its rich mathematical foundations. This part will save you some of this time and provide some scientific background knowledge that will help you better understand the various quantum information systems exposed in the remainder of this book.

As seen before, quantum physics appeared at the beginning of the 20<sup>th</sup> century to explain the dynamics of elementary particles, particularly to study how **photons**, **electrons** and **atoms** behave and interact<sup>101</sup>. Quantum physics also deals with elementary particles from the standard model like quarks and neutrinos, but it's out of scope in the second quantum revolution and quantum information science. In some cases, we still care about atom nucleus spins, which relates to proton spins, itself linked to its quark constituents. Nucleus spin plays a role in NV centers-based technologies. We also care about it with electron spin-based qubits since nucleus spin can have a detrimental impact on electron spins handling qubits information. It relates to the kinds of isotopes of carbon and silicon that are used in carbon nanotubes and silicon wafers used to create electron spin qubits.

**quantum physics deals with atomic and sub-atomic particles, and photons**

at this scale, matter behaves differently than macro objects in classical physics



elementary particles standard model			
three generations of matter (fermions)			interactions / force carriers (bosons)
QUARKS	LEPTONS	SCALAR BOSONS	GAUGE BOSONS
I mass: $\approx 2.2 \text{ MeV}/c^2$ charge: $\frac{2}{3}$ spin: $\frac{1}{2}$ <b>u</b> up	II mass: $\approx 1.28 \text{ GeV}/c^2$ charge: $\frac{2}{3}$ spin: $\frac{1}{2}$ <b>c</b> charm	III mass: $\approx 173.1 \text{ GeV}/c^2$ charge: $\frac{2}{3}$ spin: $\frac{1}{2}$ <b>t</b> top	0 0 1 <b>g</b> gluon
mass: $\approx 4.7 \text{ MeV}/c^2$ charge: $-\frac{1}{3}$ spin: $\frac{1}{2}$ <b>d</b> down	mass: $\approx 96 \text{ MeV}/c^2$ charge: $-\frac{1}{3}$ spin: $\frac{1}{2}$ <b>s</b> strange	mass: $\approx 1.48 \text{ GeV}/c^2$ charge: $-\frac{1}{3}$ spin: $\frac{1}{2}$ <b>b</b> bottom	0 0 1 <b>H</b> higgs
mass: $\approx 0.511 \text{ MeV}/c^2$ charge: -1 spin: $\frac{1}{2}$ <b>e</b> electron	mass: $\approx 105.66 \text{ MeV}/c^2$ charge: -1 spin: $\frac{1}{2}$ <b>μ</b> muon	mass: $\approx 1.7768 \text{ GeV}/c^2$ charge: -1 spin: $\frac{1}{2}$ <b>τ</b> tau	0 0 1 <b>Z</b> Z boson
mass: $\approx 1.0 \text{ eV}/c^2$ charge: 0 spin: $\frac{1}{2}$ <b>ν<sub>e</sub></b> electron neutrino	mass: $\approx 0.17 \text{ MeV}/c^2$ charge: 0 spin: $\frac{1}{2}$ <b>ν<sub>μ</sub></b> muon neutrino	mass: $\approx 18.2 \text{ MeV}/c^2$ charge: 0 spin: $\frac{1}{2}$ <b>ν<sub>τ</sub></b> tau neutrino	$\approx 80.39 \text{ GeV}/c^2$ $\pm 1$ 1 <b>W</b> W boson

Quantum physics first helped explain various observations such as the **black-body radiation** (solved by Max Planck in 1900), the **photoelectric effect** (solved by Albert Einstein in 1905) and the **sharp spectral lines** observed with excited atoms like hydrogen (solved by Niels Bohr and its atom model in 1913).

Later on, in the mid 1920's, quantum physics was built upon a **mathematical formalism** using multi-dimensional Hilbert spaces and vectors. It centered around the **Schrödinger wave equation** which describes how a massive particle like the electron behaves over space and time, using complex number probability amplitudes and differential equations over time and space.

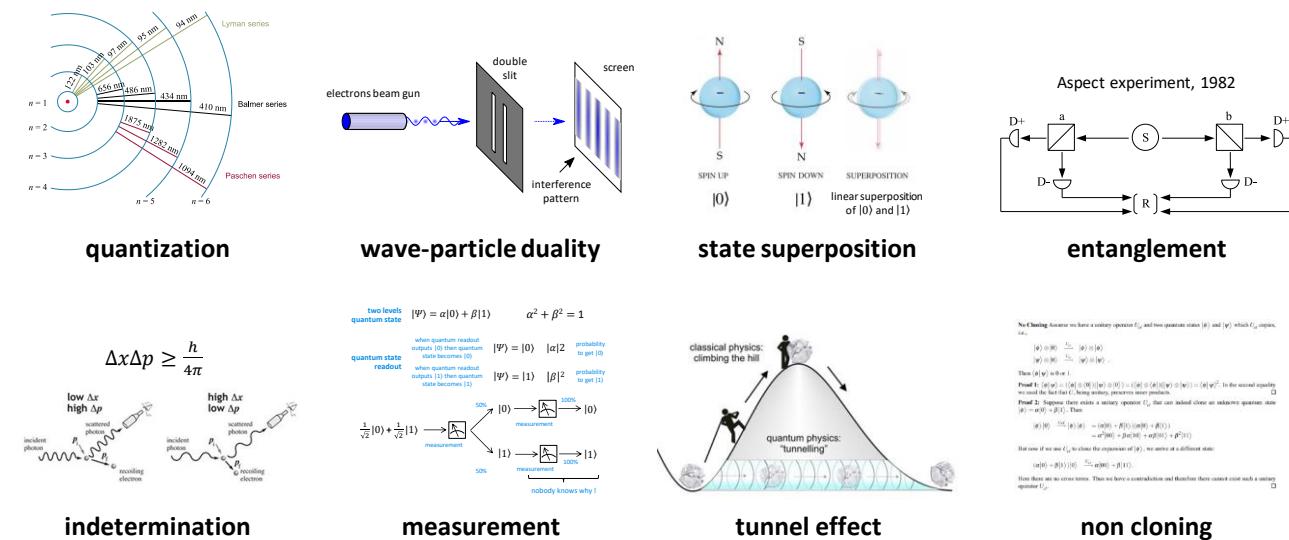
<sup>101</sup> As a reminder, here are the dimensions of elementary particles:  $10^{-10}\text{m}$  for an atom,  $10^{-15}\text{m}$  for the diameter of a hydrogen atom nucleus, thus of a single proton, and  $10^{-18}\text{m}$  for that of an electron.

These provide a probabilistic insight on the outcome of the measurement of a particle's energy, momentum and many other physical properties.

Quantum mechanics differs from classical physics with demonstrating how and why particles energy, momentum, angular momentum and other metrics are restricted to discrete values (**quantization**), objects can behave as particles or waves depending on the context (**wave-particle duality**), and there are limits to how accurately the value of a physical quantity can be predicted prior to its measurement, given a complete set of initial conditions (**indeterminacy principle**).

It also refers to **state superposition** which is at the basis of qubit operations and one of the sources of the quantum computers processing parallelism, **entanglement** which is a direct consequence of superposition applied to several quantum objects and is used with multi-qubits quantum gates and is also related to quantum communications and cryptography. Quantum objects **non-cloning** is a particular aspect of quantum physics that limits what we can do with qubits and how memory is managed. At last, **quantum tunnelling effect** has some impact in quantum technologies, like with the Josephson junctions used in superconducting qubits and with D-Wave quantum annealers.

Quantum physics explains other physical phenomena belonging to the broad **quantum matter** category, like **superconductivity** which plays a key role in superconducting qubits, **superfluidity**, used with liquid helium in dilution refrigerators and **quantum vacuum fluctuation** and its role in quantum decoherence. It also enabled the creation of **lasers**, used in many places like for controlling cold atom and trapped ion qubits and for all photonic based quantum computing and telecommunications. At last, **polaritons** are sets of interactions between light and semiconductors which could become useful in quantum sensing and quantum simulation. The quantum objects bestiary also includes **skyrmions** and **magnons**!



## Postulates

Quantum physics formalism is based on a set of postulates that follows<sup>102</sup>. Why are these postulates and not laws? Mainly because they describe a mathematical formalism that cannot be proved per se.

<sup>102</sup> Source: [Wikipedia](#), but there are many variations of these postulates in shape, form, name and number, like with [Quantum mechanics distilled](#) by Andy Matuschak and Michael Nielsen on the [Quantum Country](#) site. Quantum State becomes State Space, Physical Quantities becomes Unitary Dynamics. And they list 4 postulates while most sources have 5 or 6. John Preskill [has](#) five ‘axioms’, considering the postulates are axioms since they are not contradicted experimentally. All in all, there is not really a single “bible” of quantum postulates even when reading quantum physics founders writings (Bohr, Heisenberg, others) who didn’t agree on all of it.

One of the other reasons is that quantum physics does not rely on an ontology describing the physical objects it's based upon. I'll try whenever possible to connect these postulates with some physical meaning.

**Postulate I - Quantum state:** the state of an isolated physical system is represented, at a given time  $t$ , by a state vector  $|\psi\rangle$  (psi) belonging to a Hilbert space  $H$  called the state space with vector of length 1, using complex numbers. This is the canonical definition of a quantum state. What is this vector representing physically? For a single object, it defines its wave amplitude and phase. Quantum states help determine the probabilistic distribution of the various values its compatible properties can take. This postulate immediate consequence is the notion of superposition where any linear superposition of several  $|\psi\rangle$  vectors can form another quantum state. The  $|\psi\rangle$  vector contains the knowledge we can have of a quantum system, represented by the values taken by its measurable and compatible properties. A broader definition of a quantum state is the ensemble of values taken by compatible physical properties of a system made of one or several quantum objects. These compatible properties must be measurable simultaneously or in any order.

For a single qubit,  $|\psi\rangle$  is a vector combining the famous  $|0\rangle$  and  $|1\rangle$  basis states with complex number values in a two-dimensional Hilbert vector space.

**Postulate II - Physical quantities:** are related in quantum physics with observables that are mathematical operators  $\hat{A}$  acting on the  $|\psi\rangle$  function as  $\hat{A}|\psi\rangle$ . With the quantum matrix formalism,  $\hat{A}$  is a Hermitian (linear) matrix operator acting on the state vector  $|\psi\rangle$  to evaluate quantized or continuous physical properties of quantum objects. This operator is a self-adjoint matrix, with the implication that several consecutive measurements generate the same (vector) result. A projector operator like a Pauli matrix  $x, y$  or  $z$  used to measure a qubit state is a specific case of an observable operator.

By the way, let's clearly define properties and their variations:

**Properties** correspond to a quantum system's various observables. For a photon, it can be, for example its phase, polarization and wavelength. In quantum physics, it is not possible to evaluate the values of all properties of quantum systems to describe it, due to Bohr's complementarity principle. Properties can also be continuous like a quantum object momentum or position.

**Exclusive property values** are the possible results of a quantum measurement of a quantized property. The classical examples are vertical and horizontal polarization for a photon, or spin up or down for an electron spin component. These are mutually exclusive since it corresponds to two results of a physical measurement. Mathematically speaking, two properties are exclusive if their projector operators (*aka* observables...) are orthogonal. Otherwise, these are non-exclusive properties.

**Compatible properties** of a quantum system can be measured in any order or simultaneously<sup>103</sup>. In that case, their observable operators  $A$  and  $B$  commute ( $AB=BA$ ), or their commutator is equal to zero ( $[A,B]=AB-BA=0$ )<sup>104</sup>. Compatible properties have commuting observables. Measuring a complete set of commuting observables (CSCO) constitutes the most complete measurement of a quantum system.

**Incompatible properties** aka conjugate variables cannot be measured simultaneously and their observable operators  $A$  and  $B$  do not commute ( $AB \neq BA$  or  $[A,B] \neq 0$ ). This is a particularity of quantum mechanics.

---

<sup>103</sup> The notion of properties compatibility must not be confused with complementarity. There is complementarity between incompatible properties, like position and momentum! Incompatible observables are related to conjugate variables, defined by one being a Fourier transform of the other and Heisenberg's indeterminacy principle being consequently applied to both these variables measurement. See [Bohr's Complementarity and Kant's Epistemology](#) by Michel Bitbol and Stefano Osnaghi, 2013 (22 pages) which lay out well these different concepts.

<sup>104</sup> Compatible properties are well explained in [Mathematical Foundations of Quantum Mechanics: An Advanced Short Course](#) by Valter Moretti, 2016 (103 pages).

However, revealing one property value with a measurement doesn't exclude revealing another property afterwards. But it is not possible to obtain exact knowledge of both properties at the same time. At least one will be probabilistic. For a single particle, one example of incompatible properties or observables are two different spin components (X and Y or X and Z). After measuring the X spin component, a Z measurement will yield a random result. Also, the energy and position of an electron are incompatible properties.

**Postulate III - Measurement:** is the result of a physical quantity measurement with an observable operator A. The measurement result is one of the observable operator eigenvalues. We define eigenvalues [later](#) and cover the related mathematical formalism in the [measurement section](#) of this ebook. This postulate is sometimes embedded or associated with the previous one. The observable operator doesn't generate a measurement result per se. It helps create a probabilistic distribution of the possible measurement outcomes of a property given what is mathematically known of the quantum object state vector. When applied to a quantum object vector, it creates another state vector along the eigenvectors of the observable operator. It can then serve to create a series of real numbers describing the probabilities of the various exclusive values a given property can take. The [expectation value](#), or [predicted mean value](#), is the average value of repeated measurements that would be obtained with the physical implementation of the observable. We'll come back to this [later](#). The measurement postulate is also named the Von Neumann measurement postulate.

**Postulate IV - Born rule:** when the physical quantity A is measured on a system in a normalized state  $|\psi\rangle$ , the probability of obtaining an eigenvalue  $\alpha_n$  for discrete values or  $\alpha$  for continuous values of the corresponding observable A is given by its squared amplitude of the related wave function. It is a projection on the corresponding eigenvector. This is related to Max Born's probability rule. A quantum state can be generally represented by a density operator, which is a square matrix, nonnegative self-adjoint operator  $\rho$  normalized to be of trace 1. The average expected value of A in the state  $\rho$  is  $tr(A\rho)$ , the trace (sum of diagonal matrix values) of the observable operator applied to the density matrix<sup>105</sup>. This postulate is sometimes merged with the measurement postulate. This postulate is associated with the principle of spectral decomposition. For a single qubit, the Born rule is simple to describe with  $\alpha^2$  being the probability of getting a  $|0\rangle$  and  $\beta^2$  of getting a  $|1\rangle$  when the qubit state is described as  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  with  $\alpha$  and  $\beta$  being complex numbers. And due to probabilities normalization,  $\alpha^2 + \beta^2 = 1$ .

**Postulate V - State collapse:** only one result is obtained after a quantum measurement. Two sequential measurements based on the same observable operator will always output the same value. For a qubit, after we measure its state, whatever it is, we get a  $|0\rangle$  or a  $|1\rangle$  and this becomes the new qubit state after measurement.

**Postulate VI - Time evolution:** the time evolution of the state vector  $|\psi(t)\rangle$  is governed by the Schrödinger wave equation<sup>106</sup>. We don't directly deal much with time evolutions to understand quantum computing with qubits and gates but it still plays a key role in quantum annealing and quantum simulation and, behind the scene, in gate-based computing, with qubits decoherence, quantum noise, quantum error corrections mechanisms and measurement.

There is also a **Composition** postulate, which defines the notion of tensor product applied to separable composite quantum systems. *Aka* "Composite Systems" with John Preskill's axioms. We'll talk about it abundantly when covering [linear algebra](#) and [qubit registers](#).

<sup>105</sup> There are variations of this postulate for various quantum spectrum (discrete and nondegenerate, discrete and degenerate, continuous and non degenerate). Degenerate spectrum is defined in the glossary.

<sup>106</sup> As a result, the postulates are applicable for massive non-relativistic particles. Relativistic massive particles time evolution is described by the Dirac and Klein-Gordon equations while photons are covered by Maxwell's equations and their various derivations.

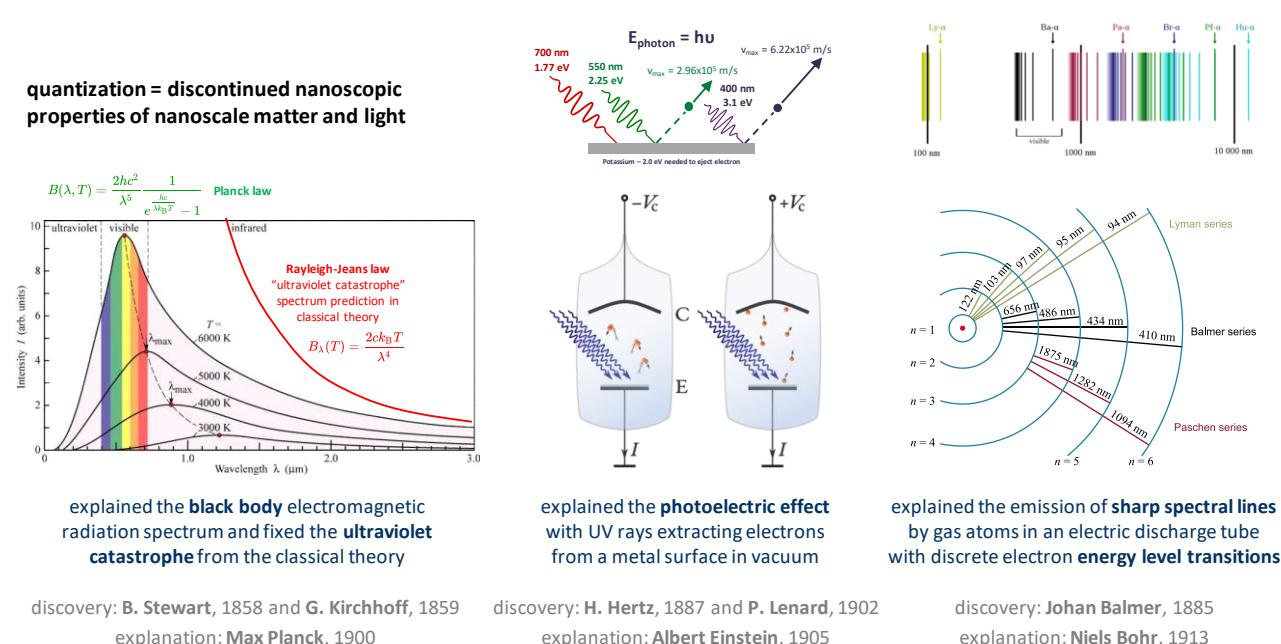
Mostly covered in [linear algebra](#) section, the main related quantum physics mathematical tools are:

- **Linear algebra:** complex numbers, eigenvectors, eigenvalues and eigenstates.
- **Functional analysis:** Hilbert spaces, Hermitian matrices, linear operators, spectral theory.
- **Differential equations:** partial differential equations, separation of variables, ordinary differential equations, Sturm–Liouville problems, eigenfunctions.
- **Harmonic analysis:** Fourier transforms and series.

## Quantization

In quantum physics, material or immaterial quantum objects have some physical properties that are discontinuous and not continuous like distances in classical physics. This frequently corresponds to the orbits of electrons around atomic nuclei which are defined in a discrete way, to atom energy levels, but also deals with photons polarizations, particles spins and other properties of matter and waves.

There is a correspondence between the discontinuous energetic transitions of electrons in orbit around atoms and the related absorbed or emitted photons. Quantization shows up in other various places like in crystals. Atoms also form harmonic oscillators and vibrate at quantified amplitudes in crystalline structures, according to a model Einstein developed in 1907.

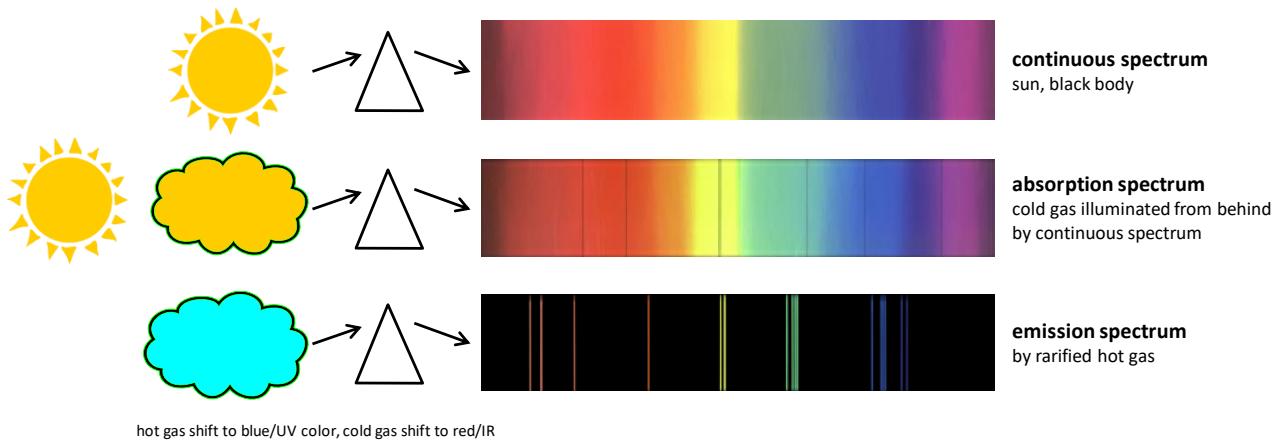


Quantization was a way to progressively explain experiments done beforehand, the first being the blackbody radiation spectrum. This one marked the beginnings of quantum physics.

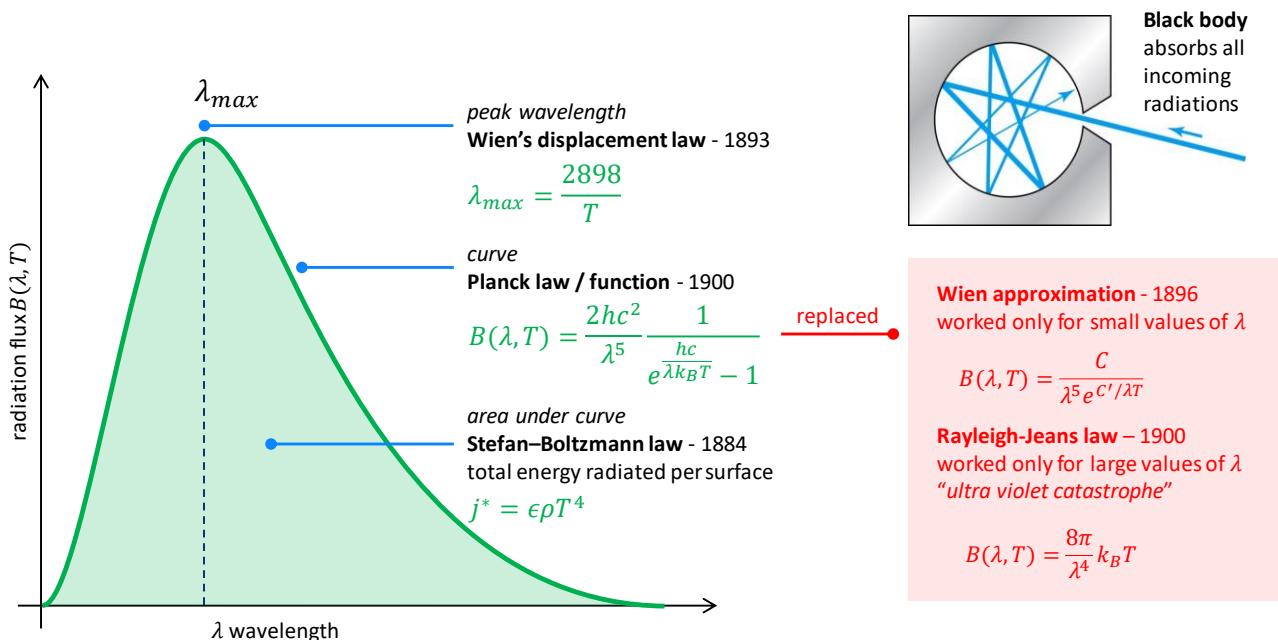
Before explaining black body spectrum, let's recall the three kinds of spectrum that can be usually found experimentally.

- A **continuous spectrum** comes from a hot and dense body like the sun, a heated solid or a perfect such body *aka* black body. It contains light in all visible frequencies that come from the random excitement of atoms in the examined body.
- An **absorption spectrum** is usually made of a continuous source of light traversing an absorbing medium like a cold gas. The resulting spectrum will be a continuous one with black lines corresponding to the frequencies absorbed by the medium.

- An **emission spectrum** is created by some rarified hot gas. It shows discrete spectrum lines corresponding to photons emitted by the excited gas atoms at specific frequencies.



Black bodies were theorized by **Gustav Kirchhoff** in 1859. These are ideal physical bodies in thermal equilibrium that absorb all incident electromagnetic waves radiations and reflects or transmits none. Since it absorbs all wavelengths, it's supposed to be black, although stars like the Sun are good approximations of black bodies and are not black at all. In usual experiments, a black body has a little hole that emits radiations which are analyzed by a spectrograph. The challenge which took four decades to be resolved was to evaluate the spectrum of the cavity radiation.



It was first discovered that the spectrum didn't depend on the body radiation and only on its temperature  $T$  and wavelength  $\lambda$ . Also, it did prove that thermal radiation was an electromagnetic one. Hot objects like light-bulbs and heated metals are close to black bodies.

As the temperature increases, the black body color shifts from red to blue. There were various attempts to explain the blackbody radiation with thermodynamics and oscillators and to predict the spectrum curve.

Before Planck's work, Stefan-Boltzmann's law (1884) described the relation between temperature and total energy radiated per surface area ( $\epsilon\rho T^4$ ) and Wien's displacement law (1893) described the relationship between peak wavelength and temperature. These two laws worked well. **Wilhelm Wien** (1864-1926, Germany) even won the 1911 Nobel Prize in physics for this discovery.

Predicting the spectrum curve didn't work so well. First, Wien devised another law in 1896, Wien's approximation or radiation law that didn't work well with large wavelengths. The Rayleigh-Jeans formula created in 1900 didn't work for small wavelengths, leading to the so-called ultra-violet catastrophe. It was based on Boltzmann's statistical methods.

To make a better curve prediction, Max Planck guessed that the energy of the oscillators in the cavity was quantized and was a multiple of some quantity with the formula  $E = nhv$ ,  $n$  being an integer,  $h$  being Planck's constant and  $v$  the wave frequency. With this discretization, oscillators couldn't afford having many energy quanta for high energy levels. Thus, their number decreased as the frequency increased instead of growing exponentially as in Rayleigh-Jeans's law.

But at this point in time, there was no clear explanation on the origin of these quanta. The second step was Albert Einstein's work on the photoelectric effect in 1905, explaining how light and electrons interacted in quantized form. He guessed that the energy from an electromagnetic field is not spread over a spherical wavefront but is localized in individual directional quanta, which were later described as wavepackets with a speed (of light) and length. But light quantization can show up in many other photon's characteristics: their polarization, their frequency, their phase and other various characteristics.

At last, the Niels Bohr's atomic model in 1913 helped describe the electron energy transitions within atoms that explained the various hydrogen emission spectra discovered by **Johan Balmer** in 1885, **Theodore Lyman** in 1906 and **Friedrich Paschen** in 1908, corresponding to transitions starting from the second, first and third atom electron layers. These are known as Balmer series, Lyman series and Paschen series.

Later on, during the 1920s, a better understanding of the quantum nature of electrons was achieved. It was progressively discovered that electrons had four quantum numbers:

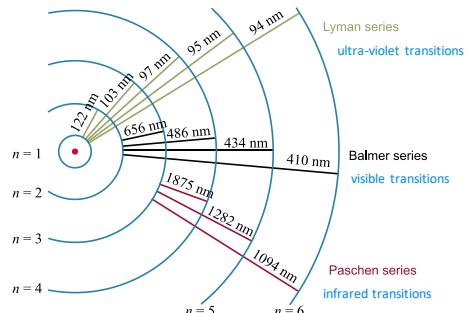
- **$n$  = principal quantum number** corresponding to their energy level or electron shell in the atom electron shells, numbered from 1, 2, 3 to  $n$ ,  $n$  being very high for so-called Rydberg (high-energy) states close to atom ionization<sup>107</sup>. This number may correspond to some energy levels used in cold atoms and trapped ions qubits.
- **$\ell$  = angular momentum**, numbered from 0 to  $n-1$  or letters (s, p, d, f, g, h, i, etc.) also named azimuthal or orbital quantum number, describes the electron subshell. These correspond to different types of elliptic orbitals around the atom.
- **$m_l$  = magnetic quantum number** describing the electron energy level within its subshell.
- **$m_s$  = spin projection quantum number**, being either +1/2 or -1/2, in a given spatial direction (usually x, y or z in an orthonormal basis), called spin component, also named intrinsic angular momentum. This is the property used in so-called electron spin or silicon qubits.

In quantum information systems, we use quantum objects which can usually have two different separable states that can be initialized, modified and measured. Even superconducting loops in superconducting qubits rely on two systems levels clearly distinct for the oscillating current flowing through their Josephson effect insulator.

We describe photons quantum numbers in the section dedicated to [photon qubits](#), page 332.

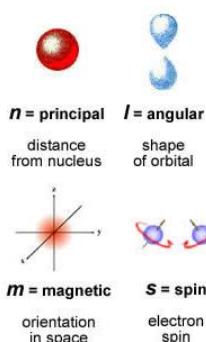
---

<sup>107</sup> The principal quantum number is limited to 7 for non-excited atoms and is theoretically illimited with excited atoms. A record of  $n=766$  was observed with hydrogen atoms in interstellar medium.



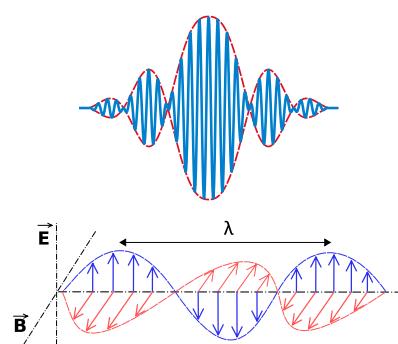
### atoms and ions

discrete transitions energy levels between electron shells observed in spectrography



### electrons

spin (up, down), magnetic orientation, angular momentum, superconducting loops



### photons

polarization (H, V), wavelength, phase, number, orbital angular momentum

=> used to create qubits with distinct states and at the particle scale (atoms, electrons, photons).

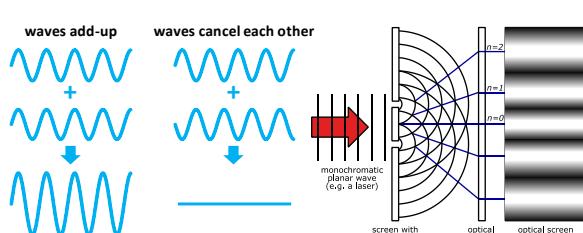
## Wave-particle duality

We often read and hear that quantum objects like photons and electrons are both waves and particles.

The right manner to describe this would be to say that they behave differently depending on the way they are observed. In some experiments, these quantum objects behave like classical waves, are not localized in space and generate interferences when added together, a bit like colors can mix (photons) and sounds can mix (acoustic waves). In other experiments, they behave as classical particles and can be localized in space and have a kinetic momentum and mass<sup>108</sup>.

Various experiments such as Young's double-slit experiment show that both photons and electrons behave both as particles and as waves depending on the context and measurement system, generating interference fringes when observed as waves. You can observe the path of a quantum object or the interferences it creates, but not both simultaneously.

This is the Bohr's principle of complementarity according to which it is not possible to apply observables simultaneously in terms of particles and waves. It shows up in the Young experiment: if we let the quantum object traverse both slits, it behaves like a wave and creates interferences.

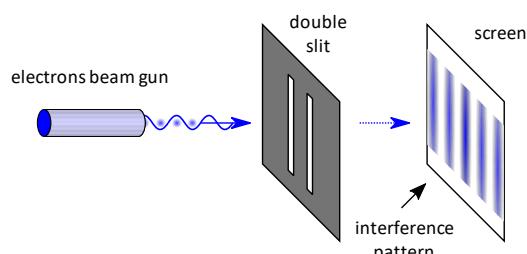


### interferences observed with photons

experiment: Thomas Young, 1801

### photons acting as particles

experiment: Compton scattering effect, 1923



### interferences observed with electrons

concept and equation: Louis de Broglie, 1924

experiment: George Paget Thomson, Clinton Davisson and Lester Germer, 1927 (crystal diffraction), Clauss Jönsson, 1961 (double-slit experiment) and Pier Giorgio Merli (same, with a single electron)

<sup>108</sup> Usually, it's impossible to observe these two behaviors simultaneously although there are some exceptions.

If we detect the quantum object in each of the slits, practically done with closing one of the slits, it creates a measurement-based decoherence and the quantum object behaves and is observed as a particle. And the classical probabilities of the particles observation don't add up to make for the interferences observed with the wave observation. This wave-particle duality is linked to the quantum physics mathematical formalism that relies on vectors that can add up linearly like waves.

It led to a still unsolved mystery, the “which-way” question. When interference fringes appear on the screen, by superposition of paths coming from the two slits, which path did the single photon or electron take?

The wave-particle duality is used in many quantum computers to make physical qubits such as trapped ions interact with energy in the form of photons emitted by lasers. Qubits can also interfere with each other thanks to interferences.

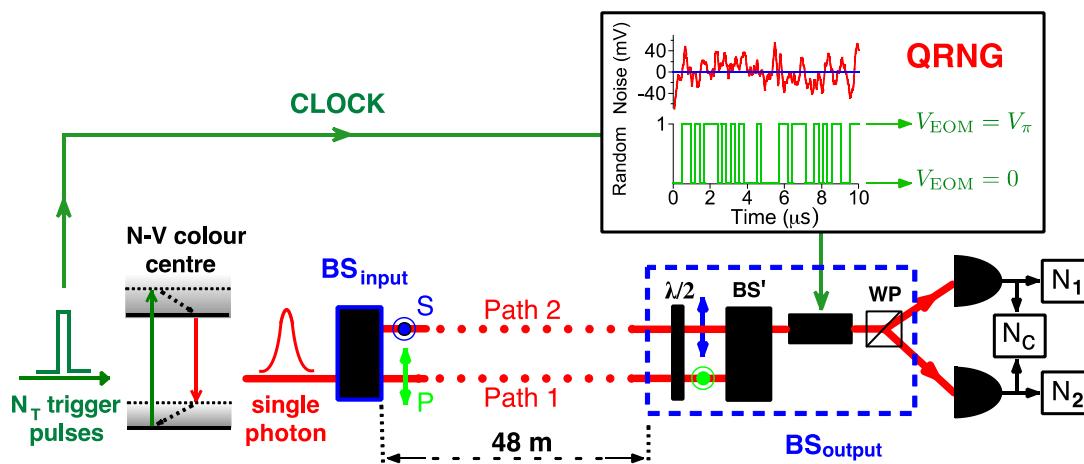
### Delayed choice experiment

John Wheeler proposed various thought experiments between 1978 and 1984 to determine if light chooses its path with sensing the experimental devices. The Wheeler's delayed-choice or which-way experiment asked the question: when does a quantum object decide to travel as a wave or as a particle?

It led to various experiments like the 1999 quantum eraser but the most decisive experiment was conducted by a team of French researchers in 2006<sup>109</sup>.

They generated pulses of single photons with an NV centers source created by Jean-François Roch, a pioneer in this domain, that were sent through a first beam splitter ( $BS_{input}$ ) and a delay line of 48 meters. Then, the two beams traversed a dynamic-controlled beamsplitter by electro-optical modulator driven ( $BS_{output}$ ) by a quantum random number generator (QRNG). At last, two photon detectors ( $N_1$  and  $N_2$ ) could determine if the photon behaved as a particle (no interference due to the inactive beamsplitter) or as a wave (with interferences due to the activated beamsplitter).

The QRNG clock was near the photon source but the QRNG was positioned close to the dynamic beamsplitter. The experiment determined that the wave/particle behavior of the photons in the interferometer was dependent on the choice of the measured observable at the end of the photon journey, not the beginning.



<sup>109</sup> See [Experimental realization of Wheeler's delayed-choice GedankenExperiment](#) by Vincent Jacques, Frédéric Grosshans, Philippe Grangier, Alain Aspect, Jean-François Roch et al, 2006 (9 pages). The experiment used a single photon source using NV centers. The experiment has been reproduced many times since then with many variations. See for example [A generalized multipath delayed-choice experiment on a large-scale quantum nanophotonic chip](#) by Xiaojiang Chen et al, 2021 (10 pages) which is based on a nano-photonics component.

And even when that choice was made at a position and a time sufficiently separated from the entrance of the photons in the interferometer. Although it's still debated, it does not require a backward in time effect explanation.

Other more delayed-choice sophisticated experiments are regularly done. A Chinese team demonstrated a generalized multipath wave-particle duality implemented by a large-scale silicon-integrated multipath interferometers<sup>110</sup>.

## Schrödinger's wave equation

The wave-particle duality led Schrödinger to create his famous wave equation which describes a massive non-relativistic quantum object with a wave function with the probabilities of finding the particle at a particular position in space at a given time.

Here's how to understand the components of this equation and their implications:

- Its **unknown** is the wave function of the particle  $\psi(x, t)$  that describes its probabilistic behavior in space and time.  $x$  indicates the position of the particle in space, with one, two or three dimensions depending on its constraints, and  $t$  is the time. This function returns a complex number that encodes the wave amplitude and phase.
- The full Schrodinger wave equation illustrates the principle of **energy conservation**. The item to the left of the equation describes the total energy of the particle at a given time and place. The element on the right includes the kinetic energy of the particle and its potential energy. Like said about the quantum physics [postulates](#), starting page 89, the Schrodinger's Hamiltonian, which is a time-dependent unitary matrix operator, is expressed differently with photons and with relativistic massive particles.

The diagram shows the Schrödinger wave equation:

$$i\hbar \frac{\partial \Psi(x, t)}{\partial t} = -\frac{\hbar^2}{2m} \frac{\partial^2 \Psi(x, t)}{\partial x^2} + V(x)\Psi(x, t)$$

Annotations explain the components:

- $i$  = imaginary number, its square equals -1
- $\hbar$  = Dirac constant
- $\hbar = \frac{h}{2\pi}$
- $h$  = Planck constant
- $m$  = particle mass
- first derivative of the wave function vs time
- second derivative of the wave function vs position (laplacian)
- potential energy function depends on the particle, its physical constraints and its position
- total energy of particle
- kinetic energy (« impulsion » observable)
- potential energy (« position » observable) equals zero for a free particle
- massive non relativistic particle wave function defining its evolution in time and space, returning a complex number, this is the equation unknown variable
- « hamiltonian » : function applicable to the particle wave function  $\Psi(x, t)$  to evaluate its total energy

(cc) Olivier Ezratty, 2020

- The **wave function square** is equal to the probability of finding the particle at location  $x$  at time  $t$ . For an electron, which is the most commonly analyzed particle with this equation, it is an indication of the probability of finding it at a given distance from the nucleus of the atom around which it orbits. Logically, as a result, the sum of the probabilities of finding the particle somewhere is equal to 1.

<sup>110</sup> See [A generalized multipath delayed-choice experiment on a large-scale quantum nanophotonic chip](#) by Xiaojiong Chen et al, 2021 (10 pages).

This is called a normalization constraint. One of its derivatives is the Max Born function that we will see later. The modulus of a complex number is the size of its vector. If  $z = a + ib$ , the modulus  $|z|$  of  $z$  is thus the square root of the sum of the squares of  $a$  and  $b$ , see *below*.

$$z = a + ib \quad |z| = \sqrt{a^2 + b^2}$$

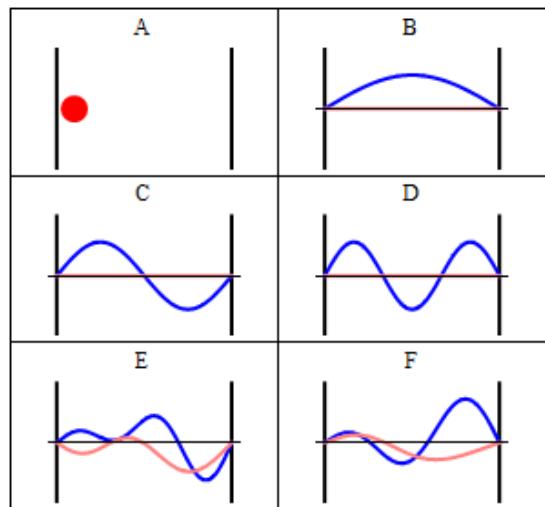
complex number module  
size of its vector in two dimensional space

$$|\psi(x, t)|^2$$

wave function module square  
probability to find the particle at position  $x$  at time  $t$ .  
If it's time independant, the system is in a stationary state.

$$\int_{-\infty}^{+\infty} |\psi(x, t)|^2 dx = 1$$

integral of the probability to find the particle  
in any position equals 1



example of  $V(x)$  potential energy constraints  
in cavities

- It is a **partial differential equation**, i.e. it connects its components via derivative functions, in this case of first degree (a slope on a curve) and second degree (an acceleration). The particle wave function appears three times in the equation: to the left of the equation with a first derivative on the time of the wave function, to the right with a second derivative on its position and with a simple multiplication with the function  $V(x)$ .
- The **potential energy of the particle** is defined by the function  $V(x)$  which depends only on the particle position in space and its physical constraints, in particular electromagnetic ones. When a particle is free and moves without constraints, this function returns zero. This function  $V(x)$  is the main variable of Schrödinger's equation.
- Schrödinger's equation is **analytically solved** in a limited number of cases such as for the electron of a hydrogen atom, a free particle, a particle in a potential well or box or a quantum harmonic oscillator. In the most complex cases, the resolution of the equation requires non-analytical methods, raw calculation and simulation. It is one of the fields of application of quantum simulators to solve the Schrödinger equation in cases where analytical methods are not available. Any micro or macro object has a Schrödinger wave function, all the way to the entire Universe. But the equation only makes practical sense for nanoscopic objects.
- The equation is **linear** over time. This means, among other things, that any combination of solutions of the equation becomes a new solution of the equation. This makes it possible to decompose a wave function into several elementary wave functions that are called the "eigenstates" of the quantum object. They correspond to the different energy levels of the particle that are discrete when the particle is constrained in space, like the electrons in an atom. One can indeed in this case derive the notion of quantification of the particle states from the Schrödinger equation ([demonstration](#)). The linearity of this equation has a lot of consequences like superpositions, entanglement as well as the non-cloning theorem.
- The operator who acts on the right side and accumulates the second derivative and the potential energy function is called a **Hamiltonian**, which describes the total energy of the system. We find this expression in the quantum annealing calculation with D-Wave and with quantum simulators.

- This equation is a **general postulate** that has been experimentally validated in a large number of cases. Its interpretation has given rise to much debate, namely, is it a simple probabilistic model or does it describe reality? We deal with this in the chapter on the [philosophy of quantum physics](#).
- The generic Schrödinger equation presented so far is said to be **time-dependent**. This equation is presented in various ways depending on the needs and annotations. The second derivative of the wave function on the position of the particle is sometimes presented with the nabla sign squared ( $\nabla^2$ ). A nabla operates a derivative on a scalar or vector function.

The  $\nabla^2$  operates a second derivative, also called Laplacian. The most concise form of Schrödinger's equation is on the bottom right, with a Hamiltonian operator on the left ( $\hat{H}$ ) and the energy operator on the right ( $\hat{E}$ ), both of which apply to the particle wave function.

$$\left[ -\frac{\hbar^2}{2m} \nabla^2 + V \right] \Psi = i\hbar \frac{\partial}{\partial t} \Psi$$

$$\hat{H}\Psi(x, t) = \hat{E}\Psi(x, t)$$

- There is a **time-independent** form of Schrödinger's equation that applies to particles in a stationary state<sup>111</sup>. In this version of Schrödinger's equation, the energy operator E is a simple constant, a real number.
- The Schrödinger equation is **symmetric** or **asymmetric** depending on the particle type. When applied to two quantum objects  $r_1$  and  $r_2$ ,  $\psi(r_1, r_2) = \psi(r_2, r_1)$  when the equation is symmetric (meaning, the wave equation is not differentiated by the given particles order) and  $\psi(r_1, r_2) = -\psi(r_2, r_1)$  when it's asymmetric. The first case corresponds to bosons which can be indistinguishable and "live" together and have a zero or integer spin and the second, to fermions, which can't cohabit with the same quantum state at the same location and have half-integer spins. All this is a consequence of Pauli's exclusion principle.
- The  $\psi(x, t)$  function must be a **continuous function** and "filled" everywhere in space. Its value is bounded by 0 and 1, with no infinite value anywhere. It also has a single value, even in the case of superposition. In that case, the  $\psi(x, t)$  is a linear superposition of two Psi functions and is itself a psi function. A quantum superposition is just another wave function!

$$\left[ -\frac{\hbar^2}{2m} \nabla^2 + V(r) \right] \Psi(r) = E\Psi(r)$$

For a system with several quantum objects, the wave function describes the quantum system state, or quantum state. According to the Copenhagen interpretation of quantum physics, the wave function from the Schrödinger equation contains the best description possible of a quantum system.

If electrons and photons both can behave as waves, they have not the same wavelengths. Indeed, a photon with an energy of 1 eV (electron-volt) has a wavelength  $\lambda$  of 1240 nm (in the infrared spectrum) while an electron with the same energy has a much shorter wavelength of 1.23 nm (in the X-ray spectrum). This short wavelength explains why we use electron microscopes to probe matter with a much better resolution than light-based microscopes.

Relativistic particles obey to Dirac and Klein-Gordon wave equations while photons are described with Maxwell's equations combined with a formalism coming from the so-called second quantization which regroups superposed photons, use photon numbers, and creation/annihilation operators. We quickly cover this formalism in the [photronics background](#) section, starting page 332.

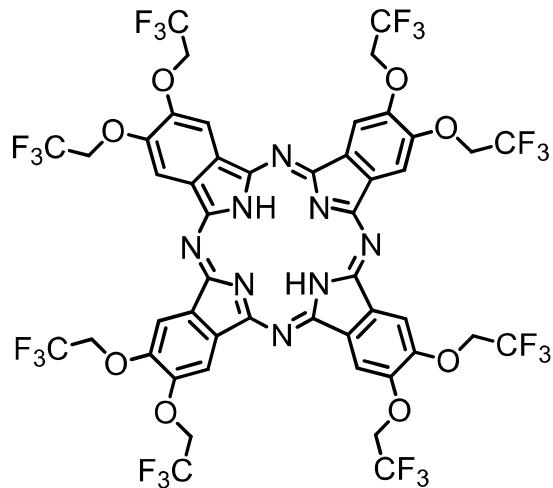
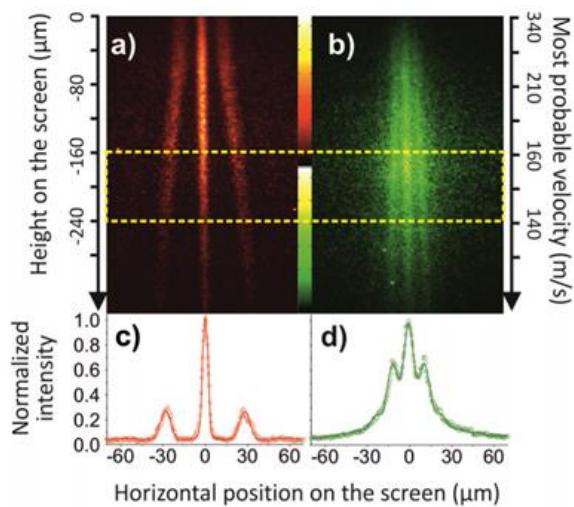
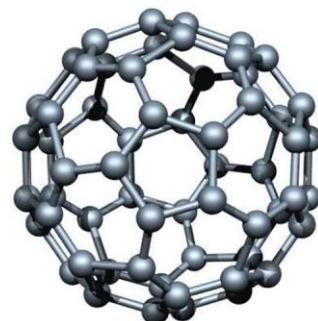
---

<sup>111</sup> According to Wikipedia: "A standing wave is the phenomenon resulting from the simultaneous propagation in opposite directions of several waves of the same frequency and amplitude, in the same physical medium, which forms a figure, some elements of which are fixed in time. Instead of seeing a wave propagating, we see a standing vibration but of different intensity at each observed point. The characteristic fixed points are called pressure nodes. ».

## Large objects wave behavior

The wave-particle duality was verified with atoms in 1991 in interferometry experiments involving lasers and classical optics. A Young double-slit experiment was also carried out in Austria in 2002 with fullerene molecules ( $C_{60}$ , formed of 60 carbon atoms<sup>112</sup>, but also with a 70 atoms variant) and in 2012 with molecules containing 58 and 114 atoms, the latter named  $F_{24}PcH_2$  is made of fluorine, carbon, oxygen, hydrogen and nitrogen<sup>113</sup>.

The illustration *below* shows the shape of the molecule. In 2019, the same kind of experiment was done with a slightly more complex molecule, a polypeptide of 15 amino acids which serves as an antibiotic, gramicidin A1<sup>114</sup>.



In 2021, other experiment led to the creation of larger quantum objects, sized 100 and 140 nm, and cooled at ultra-low temperatures<sup>115</sup>.

## Photon's wave-particle duality

On the other hand, photons can behave under certain conditions like particles. When they reach an atom, they can transmit it some kinetic motion. This is what makes it possible to generate the somewhat counter-intuitive physical phenomenon of atoms laser cooling using lasers and a Doppler effect. Temperature is related to the movement of atoms in their gaseous, liquid or solid medium. Lowering the temperature means slowing down the movement of atoms. A Doppler effect is used to do this. The moving atoms are illuminated with a laser whose frequency is tuned just below the energy absorption level of the atoms.

<sup>112</sup> See [Quantum interference experiments with large molecules](#) by Olaf Nairz, Markus Arndt and Anton Zeilinger, 2002 (8 pages).

<sup>113</sup> See [Real-time single-molecule imaging of quantum interference](#) by Thomas Juffmann et al, 2012 (16 pages). See also the [video of the experiment](#). [Highly Fluorinated Model Compounds for Matter-Wave Interferometry](#) by Jens Tüxen, 2012 (242 pages) describes the experimental device for the verification of the wave-matter duality of large molecules.

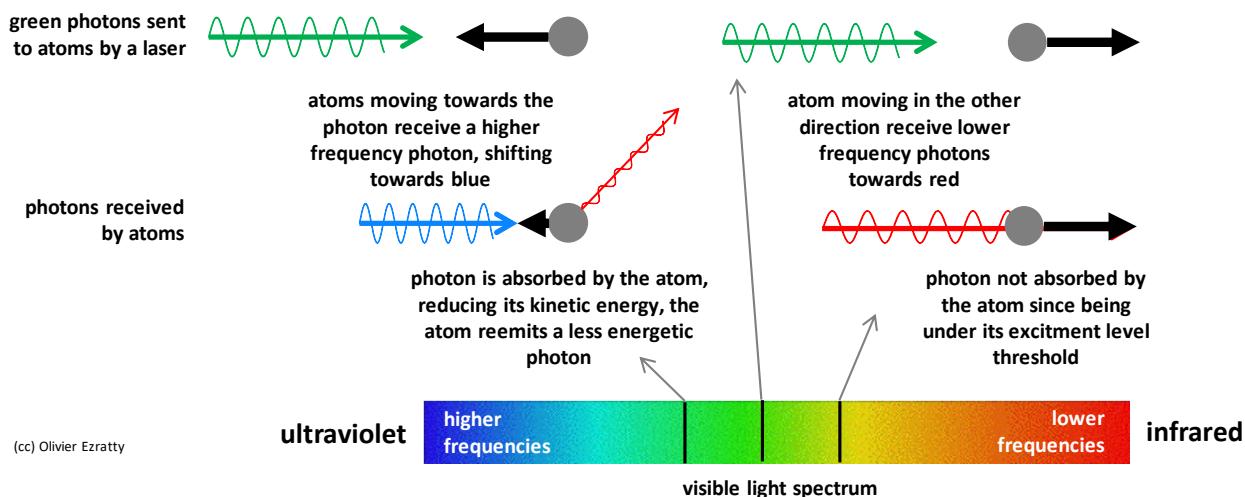
<sup>114</sup> See [A natural biomolecule has been measured acting like a quantum wave for the first time](#), November 2019, which refers to [Matter-wave interference of a native polypeptide](#) by Armin Shayeghi et al, October 2019 (10 pages).

<sup>115</sup> See [How Big Can the Quantum World Be? Physicists Probe the Limits](#) by Philip Ball, Quanta Magazine, July 2021, Real-time optimal quantum control of mechanical motion at room temperature by Lorenzo Magrini et al, July 2021 (36 pages) and [Quantum control of a nanoparticle optically levitated in cryogenic free space](#) by Felix Tebbenjohanns et al, Nature, July 2021 (26 pages).

The atoms moving towards the light will absorb the photons because these have an apparent frequency that is higher than the absorption level. This reduces the kinetic energy of the atoms receiving the photon.

The photons moving in the other direction will not absorb them because the apparent frequency of the incident photon is below the absorption level, so it's unable to change the energy state of the atoms.

Thanks to the random movement of the atoms in all directions, after a certain time, the overall temperature drops. This phenomenon slows down once the velocity of the atoms falls below a certain threshold, which explains the Doppler effect attenuation ("Doppler shift").



These techniques are used to cool atoms to temperatures close to absolute zero<sup>116</sup>. It is used to prepare cold atoms and trapped ions used in certain types of quantum computers, often in combination with magnetic and/or electronic traps to control the atoms position<sup>117</sup>.

The record low temperature was reached in 2019 with 50 nK, achieved by researchers from JILA, the joint laboratory of NIST and the University of Colorado<sup>118</sup>.

## Superposition and entanglement

Superposition and entanglement are directly related to the wave nature of quantum objects and to the linearity of the underlying mathematical models expressed in quantum physics postulates.

When you have a quantum system made of two subsystems, the mathematical representation of the system is represented by the tensor product of the two subsystems, meaning, a large vector or matrix :  $H_{AB} = H_A \otimes H_B$ . The system AB can be described by its individual parts A and B. A linear combination of quantum states becomes a new quantum state.

<sup>116</sup> Source of illustration: <https://sites.ualberta.ca/~ljleblan/background/laser-cooling.html>.

<sup>117</sup> Doppler measurement is also used to evaluate the speed at which stars and galaxies move away from each other and to evaluate the rate of expansion of the Universe. Other atoms laser-based cooling methods crafted to reach lower temperatures include sisyphus cooling first proposed by Claude Cohen-Tannoudji in 1989 and using two counter-propagating lasers using orthogonal polarization, evaporative cooling using magneto-optical traps (MOT) and optical molasses with 3D Doppler effect.

<sup>118</sup> See [JILA Researchers Make Coldest Quantum Gas of Molecules](#), February 2019. The 50 nK record was obtained with laser cooling of a gas containing 25,000 potassium-rubidium molecules.

The strawman's version of superposition is that quantum objects can be simultaneously in several states such as the direction of electron spin, upward or downward, the linear polarization of photons, horizontal or vertical, or the frequency, phase or energy of an oscillating current in a superconducting loop traversing a Josephson junction.

It is not correct according to canonical interpretations of quantum mechanics. Superposition is above all a mathematical consequence of quantum postulates and wave-particle duality. It results from the fact that a linear combination of solutions to the Schrödinger equation is also a solution to this equation. A quantum state of a given quantum object can be added together or superposed. Superposition explains the interferences obtained with electrons in the 1961 double-slit experiment. Superposition is a direct consequence of the wave incarnation of quantum objects.

A quantum object is not per se in a superposition of various states. It has a single and predictable quantum state described by a probability distribution of a given observable. Measuring this property can provide different values according to the probability distribution. That's all.

According to the Copenhagen interpretation of quantum physics, one shouldn't try to give a physical meaning to superposition before any measurement. In a classical physics interpretation, superposition could be explained by a very high frequency of quantum state changes. It is considered to be totally inaccurate for specialists, but it is still an intuitive way to figure out how superposition looks like in the physical world.

#### **quantum objects can be in superposed states**

it is a consequence of wave-particle duality.

since the Schrödinger wave equation is linear, any linear combination of solutions is also a solution.

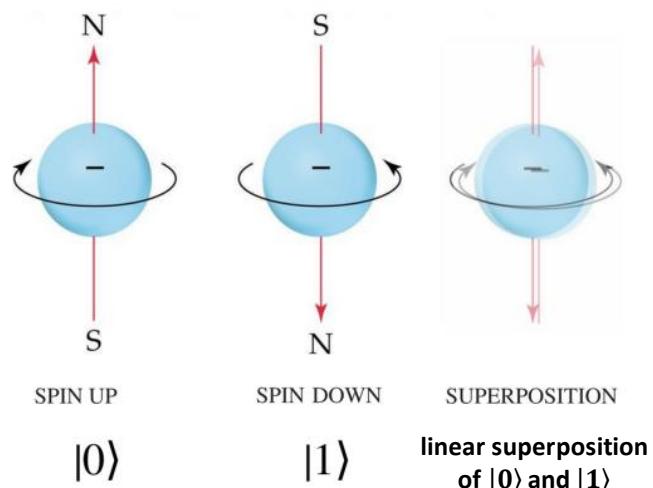
qubit example:  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

corresponds to a linear superposition of  $|0\rangle$  and  $|1\rangle$  with complex amplitudes  $\alpha$  and  $\beta$  containing information on their phase difference.

=> handles information in qubits and qubits registers.

=> enables parallelism on registers superposed states.

concept: Paul Dirac, 1930



In quantum computing, superposition is used in qubits, allowing them to have the value 0 and 1 at the same time instead of having only one of the two values as with traditional bits. This is what enables quantum computers to parallelize computing much better than classical supercomputers. It looks like it should enable some exponential computing capacity but it's not the case. Superposition alone is not sufficient. We also need entanglement and some specific quantum gates to really bring some exponential acceleration as we'll see later.

There are cases when such a state can't be anymore defined as the tensor product of two states. It means that the state is inseparable. It can't be expressed as the tensor product of two subsystems. That's where entanglement shows up! Entanglement is a direct consequence of superposition applied to multi-object systems. In the case of a single quantum object, superposition is a combination of states corresponding to several exclusive states of an observable. Coherence is another name describing a superposition. And decoherence is a phenomenon that destroys superposition, particularly with quantum measurement.

Quantum objects can be prepared to be entangled with various means. Photons can be prepared to be entangled with being generated by some excitement of atoms like cesium which will generate a couple photons of different wavelength but with some correlated properties like their polarization. Also, different quantum objects can be entangled<sup>119</sup>.

Entangled quantum objects cannot be considered as separated objects. With a pair of entangled quantum objects, a measurement made on one quantum will instantly have an effect on the other quantum, without waiting for a delay in the transmission of information at the speed of light between the two quanta. This is the principle of the "non-locality" of quantum properties that disturbed Einstein in 1935 and spurred his famous EPR paper with Rosen and Podolsky.

The entangled particles are not "linked" by chance. They usually have some common past. For example, two entangled photons can be produced with a birefringent mirror and separated by dichroic mirrors, creating two photons of orthogonal polarizations. The action on one of the two photons has an impact on the other photon as demonstrated by Alain Aspect in his famous 1982 experiment. But let's remember that the values that are generated are completely random! It is not defined at one end and transmitted to the other end. It's a random value that can be uncovered at two different places with some quantum measurement.

A 2019 experiment conducted at the University of Glasgow has even allowed to photograph a representation of the state of entangled photons<sup>120</sup>. Nevertheless, we are still able to entangle particles that do not necessarily have a common past<sup>121</sup>.

In quantum information systems, entanglement is used in multi-qubits quantum gates to conditionally link them together. Once entangled, qubits have inseparable quantum states. Without it, no quantum algorithm could work. Entanglement is also the basic physical feature used in quantum cryptography and quantum telecommunications. But quantum entanglement does not mean we can transmit some useful information faster than light since the entangled objects properties are random.

The classical entangled two-qubit states are called Bell pairs, like  $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$  or  $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ . If you measure the first qubit in both cases, you have an even 50%/50% chance to get a  $|0\rangle$  or a  $|1\rangle$ . When you measure the second qubit, you then have a 100% chance to get respectively the same value of the opposite values  $|1\rangle$  or  $|0\rangle$ . But you can't decide in advance what is the first measurement outcome (on Alice's side). So you have synchronicity between two measurements but no determinism on the first readout value. It's all about having two simultaneous synchronized random values. All this is described as the "no-signaling principle": there is no statistical difference between a "first" or "second" measurement of entangled pairs, meaning Bob doing the measurement before or after Alice, meaning Alice didn't send any actual pre-determined information to Bob when doing the measurement on her side. However, despite this randomness, we'll see how it can be useful in many parts of this book. In a particular physical setting, entanglement is verified with conducting correlation statistic tests called a **Bell test** (see [glossary](#), page 802).

In science at the frontier of science fiction, some imagine exploiting quantum entanglement to analyze a quantum state inside a black hole<sup>122</sup>! This is beyond the scope of this book<sup>123</sup>!

---

<sup>119</sup> In 2017, researchers in Warsaw were able to entangle a photon with billions of rubidium atoms. See [Quantum entanglement between a single photon and a trillion of atoms](#), 2017.

<sup>120</sup> See [Scientists unveil the first-ever image of quantum entanglement](#) by Paul-Antoine Moreau, July 2019.

<sup>121</sup> See [Qubits that never interact could exhibit past-future entanglement](#) by Lisa Zyga, July 2012.

<sup>122</sup> See [Can entangled qubits be used to probe black holes?](#) by Robert Sanders, 2019.

<sup>123</sup> Superposition also happens within benzene  $C_6H_6$  with two carbon-carbon links with their neighbors, using one or two electrons.

# Indetermination

Heisenberg's principle of indeterminacy or indetermination states that one cannot accurately measure both the position and velocity of a particle or two complementary quantities describing the quantum object state.

It's mathematically described as an inequality showing that the multiplication of both precisions can't be lower than the Planck constant divided by  $4\pi$ . Surprisingly, this inequality was not created by Werner Heisenberg but devised by **Earle Hesse Kennard** in 1927.

The indeterminacy principle has another consequence: one cannot observe at the same time a quantum object in its particle state and in its wave state, per the principle of complementarity enacted by Niels Bohr around 1928, that we already mentioned in the wave-particle duality section.

For purists, the notions of particle speed and position are even meaningless for electrons. Its characterization is based on its wave nature and its probabilistic description via Schrödinger's wave function. Don't even try to understand where it is at a given place and time.

$$\Delta x \Delta p \geq \frac{\hbar}{4\pi}$$

location precision      momentum precision      Planck constant

**at nanoscopic scale, the speed and position measurement precisions are antinomic, the greater one is, the smaller is the other**

applicable to any quantum objects physical quantities (position, momentum, polarisation, wave length, ...)

direct consequence of wave-particle duality

explained with electro-magnetic waves thanks to Fourier transforms: the shorter a pulse is, the larger its electro-magnetic spectrum is, and vice-versa.

formalism: **Werner Heisenberg**, 1927.

inequality: **Earle Hesse Kennard**, 1927 and **Hermann Weyl**, 1928.

**Heisenberg microscope thought experiment:** a photon sent on the electron will change its trajectory and measurement

**derivation:** at nanoscopic scale, measurement apparatus impacts measurement output  
also works with opinion polls...

- => used in "squeezing" like with photons to increase one precision against the other.
- => quantum sensing to increase measurement precision on one dimension, like photon squeezing in LIGO/VIRGO interferometers.
- => also indirectly explains quantum vacuum fluctuations.

When it deals with velocity and position, Heisenberg's indeterminacy principle is closely related to a characteristic of Fourier transforms: a nonzero function and its Fourier transform cannot both be sharply concentrated, so, precisely measured. The more concentrated a signal is in the time domain, the more spread out it is in the frequency domain and vice-versa. We have here a mathematical balance between a pulse length precision and its spectral analysis precision.

Since complementary (or incompatible) properties can't both be measured with an arbitrary precision, we can improve one property measurement precision with decreasing the measurement precision of the complementary property. It's being implemented with the so-called photons squeezing technique, put in place in the latest LIGO (USA) and VIRGO (Italy) huge interferometers that are used to measure gravitational waves coming from huge astrophysical phenomena like dual black hole collapses. They increase the precision of photons time arrival in the interferometer at the price of a greater imprecision in the number of photons<sup>124</sup>.

<sup>124</sup> See [Squeezing More from Gravitational-Wave Detectors](#), December 2019.

## Measurement

Measuring quantum object properties follows a very different path than with classical physics due to the back action induced by quantum measurement on the measured system and to its probabilistic dimension.

With classical mechanics, you can usually predict the measurement of macro-objects (dimension, speed, position) based on their dynamics. In quantum mechanics, given the knowledge of the position of the measured object, one cannot measure precisely its momentum. More generally, the knowledge we have about two non commuting observables is bounded such that we can never assign them a well define value simultaneously, due to the Heisenberg uncertainty principle.

Moreover, a quantum measurement readout requires some interaction with a macroscopic object that selects automatically one specific outcome. Measuring the same initial state several times can lead to different outcomes. However, even if each measurement yields a probabilistic result, when repeated several times, their statistical distribution is not probabilistic. It corresponds to the knowledge that can be obtained from the evaluated quantum state.

Before measurement, a single isolated quantum object is said to be in a pure state, represented by a vector in a Hilbert space, or its “Psi” vector. It is a superposition, or linear combination of basis states or one of the object basis state, like “ground state” or “excited”. When a quantum object is measured against one observable, the state of the quantum object become one of the observable basis states, like a spin direction up or down or a discrete energy level. The quantum object collapses in a probabilistic way into one of the available basis states. If we conduct another measurement, we'll always get the same result being the basis state that was obtained beforehand in the first measurement. This is also called "*Schrödinger wave function collapse*" or "*wave packet collapse*".

With a photon of intermediate polarization between horizontal or vertical linear polarization, it will become a horizontally or vertically polarized photon after its polarization measurement.

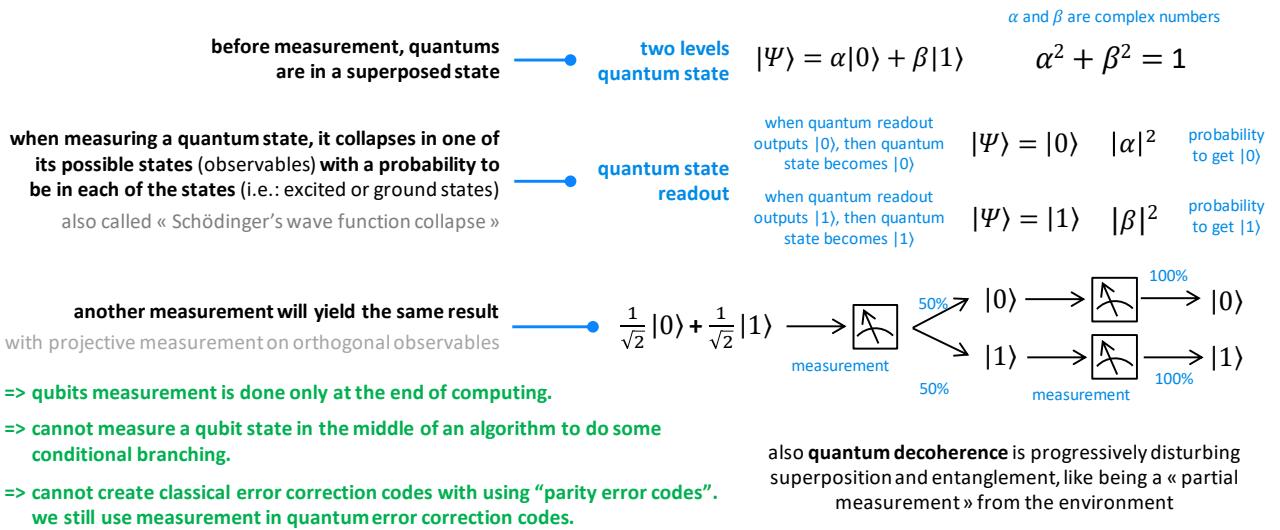
In quantum computing, this principle of reduction is implemented when measuring the state of a qubit. It modifies its value by collapsing it to the basis states  $|0\rangle$  or  $|1\rangle$ . The outcome is probabilistic with a chance of retrieving a  $|0\rangle$  or a  $|1\rangle$  depending on the qubit state. However, when the quantum state is a basis state, say  $|0\rangle$  or  $|1\rangle$  for a qubit, its measurement should return this basis state in 100% of the cases and is therefore not probabilistic but deterministic. This works however only in a perfect world without any quantum noise. Even when a qubit is in a basis state, its measurement doesn't return a perfect basis state 100% all the time. You get a % that is inferior to 100% and corresponds to the readout qubit fidelity. It turns a basis state measurement into a probabilistic one.

The subtle information contained in a qubit that is represented by a complex number or a two-dimensional vector is reduced to  $|0\rangle$  or  $|1\rangle$  at the time of its measurement. It becomes a classical bit. A single measurement is then making us lose all the wealth of information contained in the qubit. We turn the equivalent of two floating point numbers to a single bit! However, this measurement is supposed to happen only at the end of quantum algorithms. During computing, the whole wealth of qubit internal information is leveraged, particularly with the creation of interferences between qubits.

All this is illustrated in the diagram *below*. We will come back to the meaning of  $\alpha$  and  $\beta$  complex numbers in the next section on qubits.

This reduction should occur theoretically only at the end of computing. During computing, qubits are modified by quantum gates preserving the richness of their information, the combinatorial nature of their values based on superposition and entanglement. However, quantum measurement is to be implemented during computing with systems implementing quantum error corrections.

The subject of quantum measurement is quite broad. In a [forthcoming more detailed section](#), we'll cover several additional concepts such as projective measurements, non-selective measurement, weak measurement, gentle measurement and non-destructive measurement.



## No-cloning

The no-cloning theorem prohibits the identical copy of the state of a quantum object onto another quantum object. The theorem is mathematically demonstrated in [six lines](#) (below). It is also described page 133.

As a consequence, it is impossible to copy the state of a qubit to exploit it independently of its original, contrarily to a classical bit that can be copied from/to memory and from/to storage.

The theorem was demonstrated in 1982 in a paper published in [Nature](#) by William Wootters, Wojciech Zurek and Dennis Dieks. The article is still not available in open-source on a site such as Arxiv, self-applying the no-cloning principle! But a summarized version is available [here](#).

In quantum computers, qubits can be duplicated via quantum gates and entanglement, but the resulting qubits are entangled and therefore somehow synchronized, inseparable and... random. Reading the copy destroys the original by projecting the state of the two qubits to the 0 or 1 closest to their initial state and in a probabilistic way.

a quantum's state can't be replicated independently onto another quantum

only possible copy is through entangled states creation  
easy to demonstrate mathematically

=> qubit teleportation.

=> secures telecommunications  
with quantum key distribution.

=> creates significant constraints in quantum computing (memory, cache, error correction, ...).

**No Cloning** Assume we have a unitary operator  $U_{cl}$  and two quantum states  $|\phi\rangle$  and  $|\psi\rangle$  which  $U_{cl}$  copies, i.e.,

$$\begin{aligned} |\phi\rangle \otimes |0\rangle &\xrightarrow{U_{cl}} |\phi\rangle \otimes |\phi\rangle \\ |\psi\rangle \otimes |0\rangle &\xrightarrow{U_{cl}} |\psi\rangle \otimes |\psi\rangle. \end{aligned}$$

Then  $\langle \phi | \psi \rangle$  is 0 or 1.

**Proof 1:**  $\langle \phi | \psi \rangle = (\langle \phi | \otimes |0\rangle)(|\psi\rangle \otimes |0\rangle) = (\langle \phi | \otimes \langle \phi |)(|\psi\rangle \otimes |\psi\rangle) = \langle \phi | \psi \rangle^2$ . In the second equality we used the fact that  $U$ , being unitary, preserves inner products.  $\square$

**Proof 2:** Suppose there exists a unitary operator  $U_{cl}$  that can indeed clone an unknown quantum state  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Then

$$\begin{aligned} |\phi\rangle |0\rangle &\xrightarrow{U_{cl}} |\phi\rangle |\phi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|00\rangle + \beta\alpha|10\rangle + \alpha\beta|01\rangle + \beta^2|11\rangle \end{aligned}$$

But now if we use  $U_{cl}$  to clone the expansion of  $|\phi\rangle$ , we arrive at a different state:

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle \xrightarrow{U_{cl}} \alpha|00\rangle + \beta|11\rangle.$$

Here there are no cross terms. Thus we have a contradiction and therefore there cannot exist such a unitary operator  $U_{cl}$ .  $\square$

discovery : James Park in 1970

then William Wootters and Wojciech Zurek in 1982

This has a direct impact on the design of quantum algorithms and in particular on the error correction codes of quantum computers. These error-correction codes use the trick of projective measurement on a different computational basis as we'll see later.

A derivative of non-cloning is non-deleting. In the case of a qubit, it means it's impossible to reset a qubit from an entangled set of two qubits  $|\psi\rangle$ , meaning to transform  $|\psi\rangle|\psi\rangle|0\rangle$  into  $|\psi\rangle|\psi\rangle|0\rangle$ .

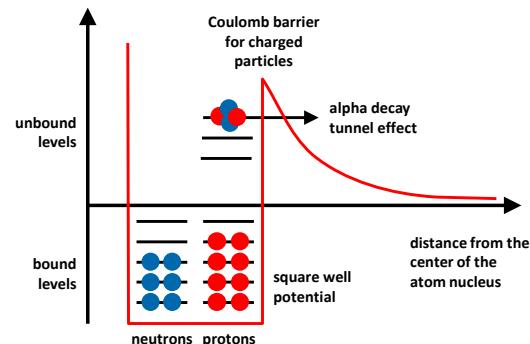
## Tunnel effect

The wave-particle nature of matter allows it to cross physical barriers also known as energy walls in some circumstances, depending on the wall thickness and quantum object wavelength. The transmitted wave is usually attenuated after crossing the barrier and its strength depends on the wavelength with regards to the barrier length and composition.

This phenomenon was first accidentally unveiled by **Henri Becquerel** in 1896 when he discovered radioactivity. It did show up with uranium salts decaying, producing alpha rays comprised of two neutrons and two protons. This phenomenon was explained later thanks to quantum physics and wave-particle duality by **George Gamow** in 1928.

Just before in 1927, the German physicist **Friedrich Hund** (1896-1997) created the formalism explaining electron based tunneling effect.

It took two more decades to turn this into transistors, invented in 1947 by scientists from the Bell labs.

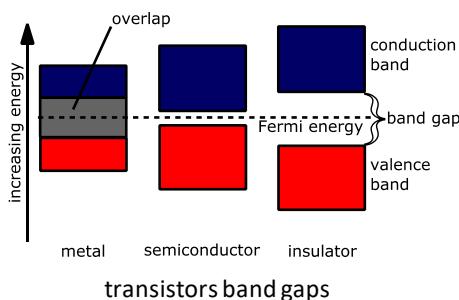


radioactive alpha decay across the Coulomb barrier

discovery: **Henri Becquerel** with uranium salts, 1896.

explanation: **George Gamow**, 1928.

electron tunneling formalism: **Friedrich Hund**, 1927.



**wave-particle duality enables particles to cross physical barriers**

these are energy walls.

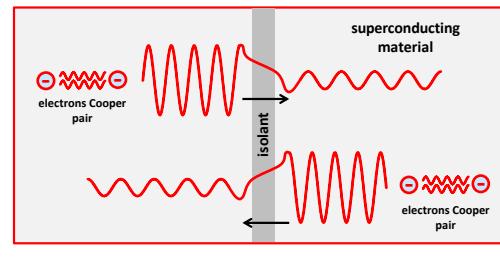
wave is usually attenuated after crossing the barrier.

depends on the wave length with regards to the barrier length and composition.

=> **tunnel effect transistors and tunnel effect microscopes.**

=> **Josephson junctions and superconducting qubits.**

=> **used in quantum annealing computers (D-Wave).**



Josephson junction

It's also implemented in superconducting Josephson junctions and exploited in D-Wave quantum annealers where it is used to converge a system of spin qubits ("Hamiltonian", with a given total energy level) towards an energy minimum corresponding to the resolution of a complex combinatorial problem or a search for energy minimum as in chemistry or molecular biology.

# Quantum matter and fluids

Quantum matter and fluids refer to materials and phenomena that are described with quantum mechanics and are at the crossroads of statistical physics.

The study of quantum matter falls into the field of condensed matter physics. Quantum fluids include superconductors, superfluid Helium, Bose-Einstein condensates and ultra-cold atoms.

They exhibit quantum mechanical effects at the macroscopic “collective level”. These phenomena usually happen at very low temperatures and sometimes high-pressure. There are even solid quantum fluids where electrons or protons can behave like a fluid. This happens with superconductive materials with macro quasi-particles made of pairs of electrons (“Cooper’s pairs”) and with skyrmions or magnons.

This field also contains polaritons, which are also quasi-particles resulting from the coupling of photons and electric or magnetic dipole-carrying excitation, usually found in semiconducting materials.

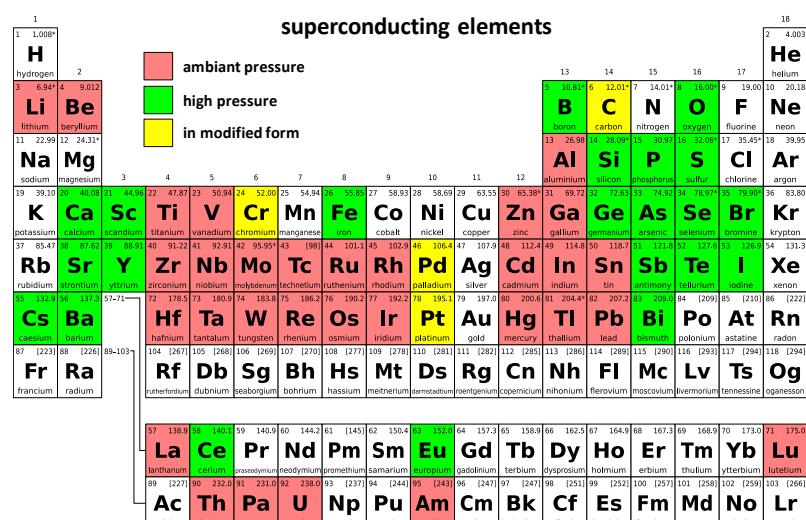
At last, it also contains quantum topological matter. We’ll have a chance to further investigate this broad domain in a future edition of this ebook.

## Superconductivity

Superconductivity occurs when under a low-level temperature, some conducting materials no longer oppose resistance to electric current. With usual electric current, electrons move from atom to atom and transform part of their kinetic energy into heat related to the movement of the atoms hit by electrons.

With superconductivity, electrons arrange themselves in pairs, called Cooper’s pairs, circulating between atoms without friction. The structure of the atoms of the conductive metal is also modified. Waves of atoms occur that follow and accompany the movement of Cooper’s pairs.

These are called phonons<sup>125</sup>. Cooper’s pairs are electrons of opposite spins forming composite bosons, allowing them to have the same quantum state<sup>126</sup>.



Superconductivity was discovered experimentally in 1911 by **Heike Kamerlingh Onnes** (1853-1926), Cornelis Dorsman, Gerrit Jan Flim and Gilles Holst at the University of Leiden in the Netherlands, with solid mercury at 4.2K. Kamerlingh Onnes also discovered that a magnetic field whose level depends on temperature could make the superconducting effect disappear<sup>127</sup>.

<sup>125</sup> Source of illustration: Superconducting properties of ZrNi<sub>2-x</sub>TM<sub>x</sub>Ga (TM = Cu, Co) and ZrNi<sub>2</sub>Al<sub>x</sub>Ga<sub>1-x</sub> Heusler Compounds (77 pages). Link removed because site generating a detection in the Avast antivirus.

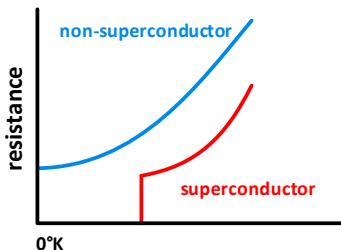
<sup>126</sup> Cooper’s pairs can also be formed with atoms as with helium 3, a fermion, in its superfluid state named a fermionic condensate.

<sup>127</sup> See this detailed presentation: [Superconductivity and Electronic Structure](#) by Alexander Kordyuk, 2018 (145 slides).

Its interpretation was formulated much later, in 1957, by **John Bardeen**<sup>128</sup>, **Leon Neil Cooper** and **John Robert Schrieffer** of the University of Illinois. They built the so-called **BCS theory**<sup>129</sup>.

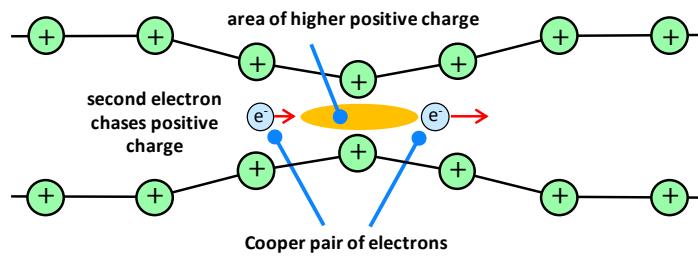
About 50 elements are superconducting at low temperature but the superconductivity temperature and pressure thresholds are very variable.

Superconductivity is also possible with composite materials such as germanium, titanium and niobium alloys or copper-based materials (as cuprates). This is particularly the case with aluminum and mercury. The most common superconducting material is a niobium and titanium alloy<sup>130</sup>.



some materials have zero resistivity below a threshold temperature ( $T_c$ )

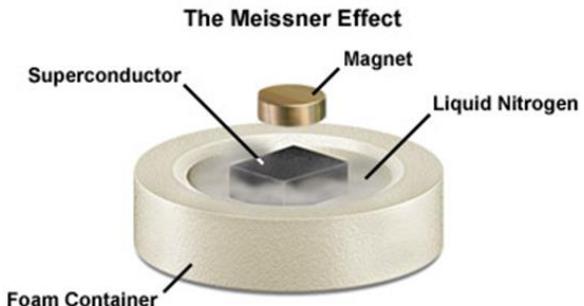
discovery: H. Kamerlingh Onnes et al, 1911



explained by Cooper pairs of electrons with opposed spins flowing in crystal lattice, creating bosons

theory: Bardeen, Cooper, Schrieffer (BCS) theory, 1957

The superconducting effect is maximum for atoms that have a large number of valence electrons, i.e. in the last orbital layer, with the highest quantum number. Superconductivity explains unexpected phenomena such as the levitation of magnets above superconductors immersed in liquid nitrogen. Superconducting ceramics, discovered since 1986, can be used in this striking experiment<sup>131</sup>.



<sup>128</sup> John Bardeen holds two Nobel prizes in physics, one in 1956 for the invention of the transistor with William Shockley and Walter Brattain and the other for the interpretation of superconductivity in 1972 with Leon Neil Cooper and John Robert Schrieffer. Cooper co-created the BCS theory at the age of 27 and won the corresponding Nobel Prize at the age of 42. Born in 1930, he is still with us today.

<sup>129</sup> An accurate timeline of the discovery of the principle of superconductivity is provided in the presentation [50 Years of BCS Theory "A Family Tree" Ancestors BCS Descendants](#), by Douglas James Scalapino, John Rowell and Gordon Baym, 2007 (52 slides). See also the excellent book [The rise of superconductors](#) by P.J. Ford and G.A. Saunders 2005 (224 pages) which tells the story of the discovery and then interpretation of superconductivity. Before the BCS theory, many physicists had broken their teeth on the explanation of superconductivity: Albert Einstein, Niels Bohr, Lev Landau, Max Born, Felix Bloch, Léon Brillouin, John Bardeen (co-inventor of the transistor), Werner Heisenberg and Richard Feynman.

<sup>130</sup> See [Superconductivity 101](#). The superconducting properties of the niobium-titanium alloy were discovered in 1962. It is widely used in the cooling of MRI scanners but also in many scientific instruments, notably in the ITER experimental nuclear fusion reactor at Caradache. The Periodic Table of Elements comes from Wikipedia.

<sup>131</sup> High-temperature superconducting ceramics were discovered in 1986 by Georg Bednorz and Alex Müller, combining lanthanum, barium, copper and oxygen, and superconducting at 30K, a record for the time. This earned them the Nobel Prize in 1987, a very short time after their discovery.

The magnetic field is then expelled from inside the superconducting material. This is the Meissner effect, discovered in 1933 by **Walther Meissner** (1882-1974, German), which only applies to certain so-called type I superconductors. It explains the repulsion demonstrated in numerous experiments.

Type II which does not generate this phenomenon includes niobium titanium alloys which are frequently used with a 1:1 ratio of each in the alloy.

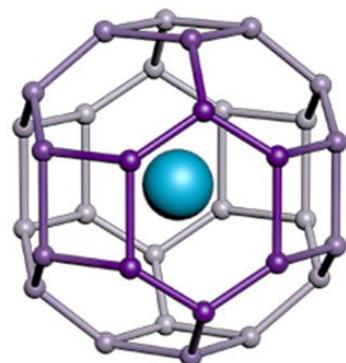
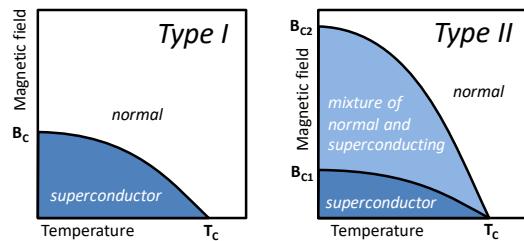
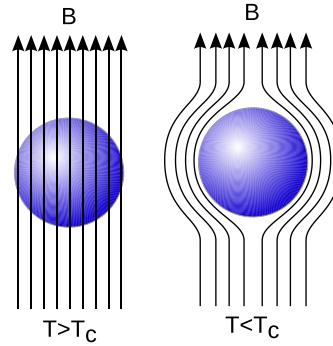
In type II superconductors, an intermediate phase between the classical metallic phase and the superconducting phase allows the magnetic field to pass partially<sup>132</sup>. The Holy Grail of superconductivity would be to obtain it at room temperature, allowing, for example, to reduce transmission losses in grid electric power lines.

Out of the various metals used in quantum technologies, titanium becomes superconducting at 390 mK, aluminum at 1.2K, indium at 3.4K and niobium at 9.26K.

Scientists began discovering superconducting metal alloys above 77K in the late 1980s, the temperature of liquid nitrogen. Most of them are cuprates alloys (copper-based). A record was achieved in 2019 with a molecule combining lanthanum and hydrogen ( $\text{LaH}_{10}$ ) and at -23°C, thus a near-ambient temperature. In the latter case, however, it works at a huge pressure of 218 GPa, representing more than 2 million times the atmospheric pressure, which is 101,325 Pascals<sup>133</sup>. Another record was broken with metallic hydrogen in 2020 by CEA researchers, operating at 17°C and at an even greater pressure of 400 GPa<sup>134</sup>.

So it's not very practical! Hence the willingness to use quantum simulators or computers to run superconductivity quantum equations and identify materials that would be superconducting at room or near-room temperature<sup>135</sup>.

By the way, we may wonder why scientists are not using high-temperature superconducting materials to build superconducting qubits? The main reason is that their low temperature of about 15 mK is related to the controlled noise environment linked to using driving micro-waves in the 5-10 GHz range. These microwaves have the benefit of being photons adapted to the anharmonic excitement levels of Josephson gates and to be transportable on coaxial cables which are themselves made of superconducting materials like niobium-titanium. The superconducting qubits cooling temperature of 15 mK creates an ambient thermal noise that is one order of magnitude lower than the temperature corresponding to these controlling microwaves.



<sup>132</sup> [Source of the illustration](#).

<sup>133</sup> See [Quantum Crystal Structure in the 250K Superconducting Lanthanum Hydride](#) by Ion Errea, July 2019 (20 pages).

<sup>134</sup> See [Here comes metallic hydrogen - at last!](#) by Jean-Baptiste Veyrieras, May 2020. Another record was broken in 2019 with  $\text{YH}_6$  (yttrium hybrid) at a pressure of 110 GPa. See [Anomalous High-Temperature Superconductivity in  \$\text{YH}\_6\$](#)  by Ivan A. Troyan et al, 2019 (36 pages).

<sup>135</sup> Another fancy solution consists in lowering the room temperature as described in [Novel approach to Room Temperature Superconductivity problem](#) by Ivan Timokhin and Artem Mishchenko, April 1st, 2020 (4 pages).

Superconductivity is commonly used in **MRI scanners**<sup>136</sup>, using large superconducting magnets that are cooled with liquid helium. Scanners are encased in a protective coating to constrain the magnetic field inside the scanner. The niobium-titanium coil wiring is enveloped in a copper matrix.



Source of illustration on the right: [Helium Reclaiming Magnetic Resonance Imagers](#) by Dan Hazen, MKS Instruments (5 pages).

This combination is also used in large physics instruments like the **CERN LHC** in Geneva with 1200 tons of NbTi cable including 470 tons of NbTi, the rest being copper, in cables totaling 21 km. Superconductivity creates a current of 11,850 A generating a powerful magnetic field of 8.33 tesla creating a centripetal force holding the accelerated particles. These magnets are cooled by 10,000 tons of superfluid helium-4 at 1.9K. Their cables are made of niobium-titanium filaments surrounded by copper. The whole unit power is 40MW with an electricity consumption estimated at 750 GWh per year according to CERN. It is the largest and most powerful refrigerator in the world!

Superconductivity is operated in the **Chuo Shinkansen** Maglev high-speed train in Japan, which has been undergoing trials since 2013 and is expected to reach a commercial speed of 505 km/hr. It uses a superconductive based magnetic suspension with a rather expensive infrastructure. Power consumption per passenger/kilometer is three times that of traditional Shinkansen, but it is still competitive with airplanes. A 286 km Tokyo-Nagoya line is planned for commercial service in 2027.

Superconductivity has also been studied to improve the efficiency of electric motors and generators with HTS Synchronous Motors (High-Temperature Superconducting). It allows a reduction of motors size and efficiency improvements. It is based on superconducting materials that only require liquid nitrogen cooling, but some systems still use helium-based cooling. Studies began in the 1980s and these engines and generators are beginning to be deployed in the military navy and in wind power generation, notably at **AMSC**, **Sumitomo Electric**<sup>137</sup> and with the European **EcoSwing** project, which involves Sumitomo's cryostat division.

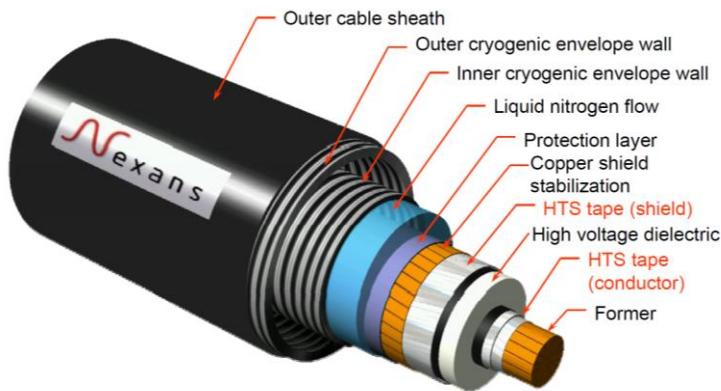
Superconducting cables have also been introduced to transmit electricity without power loss and greater capacity to meet the ever-increasing demand. They are offered by the French cable manufacturer **Nexans**, which installed one in Long Island. Their 600 m underground cable has been in operation since 2008. It can supply electricity to 300,000 homes<sup>138</sup>. But it is rather complex to implement and was not seemingly replicated in many places. The project cost was \$46.9M.

<sup>136</sup> Nuclear magnetic resonance imaging.

<sup>137</sup> See [Design of MW-Class Ship Propulsion Motors for US Navy by AMSC](#) by Swarn S. Kalsi, 2019 (50 slides).

<sup>138</sup> Information Source: [Long Island HTS Power Cable](#), Department of Energy, 2008 (2 pages). In addition to Nexans, the cryogenic system was supplied by Air Liquide.

### Low temperature dielectric inside cryogenic envelope



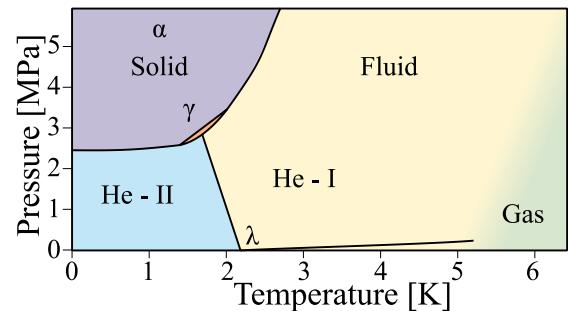
As far as quantum computers are concerned, superconductivity is used in particular in superconducting qubits that exploits the Josephson effect that we have already described in a previous section. This technology is also used in variations of SQUIDs (superconducting quantum interference device) in quantum sensing. We also find it in the type II niobium-titanium based superconducting cables used for reading the state of superconducting and electron spin qubits.

Superconductivity could also be used to create processors operating at low temperatures and capable of operating up to 700 GHz, much faster than current server processors running at a peak 4 to 5 GHz<sup>139</sup>. An MIT team announced in July 2019 a proposal for a technique to create spiking neurons with superconducting Josephson effect circuits using nanowires<sup>140</sup>. This is still a research field with very few industry applications at this point.

We'll investigate this field in a specific section on unconventional computing. Superconducting electronics could be very useful to create and analyze the microwaves used in superconducting and electron spin qubits.

## Superfluidity

Superfluidity is yet another quantum physics phenomenon to cover here. It occurs only with superfluid helium which, at ambient pressure, never freezes, no matter how low the temperature. Superfluid liquid has zero viscosity and flows without any loss of kinetic energy. When poured into a recipient, it tends to rise up by capillary action on its rim and flow out of it. It can even pass through very fine capillaries (illustration source: [Wikipedia](#)).



Helium was first liquefied in 1908 at 4.2K by Heike Kamerlingh Onnes, the discoverer of superconductivity in 1911.

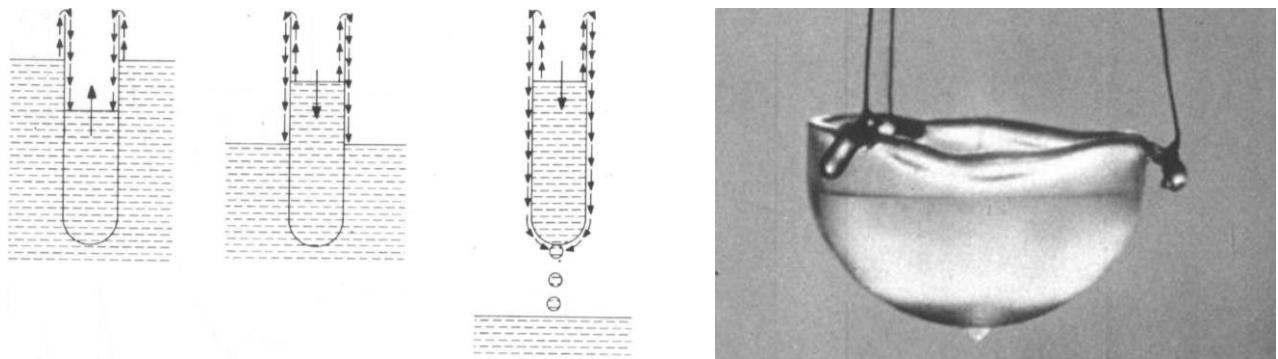
Its superfluidity was highlighted independently in 1938 by **Pyotr Kapitsa** (1894-1984, USSR), **John Frank Allen** (1908-2001, USA) and **Don Misener** (1911-1996, USA)<sup>141</sup>.

<sup>139</sup> See [Superconductor ICs: the 100-GHz second generation](#) by Darren Brock, Elie Track and John Rowell of Hypress, 2000 (7 pages).

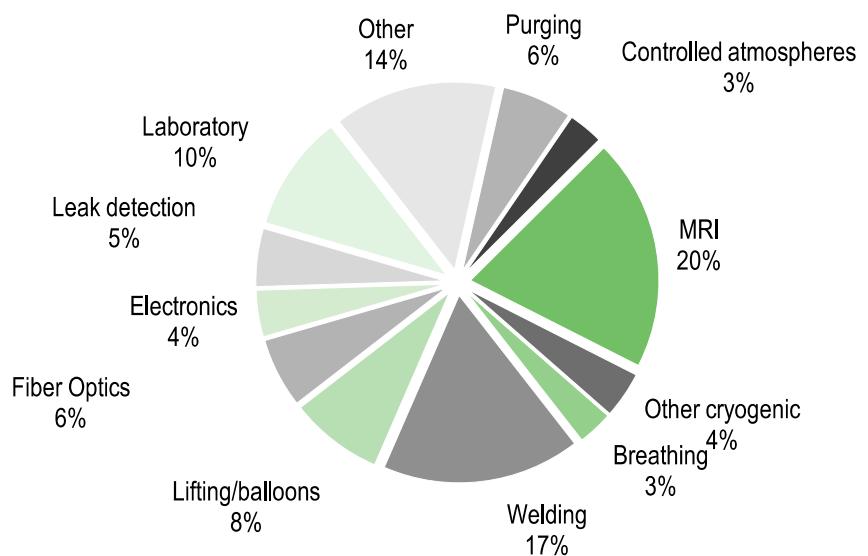
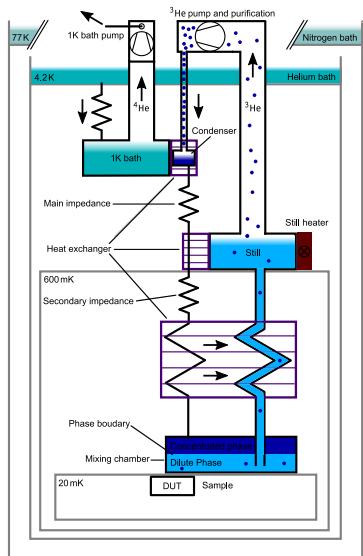
<sup>140</sup> See [A Power Efficient Artificial Neuron Using Superconducting Nanowires](#) by Emily Toomey, Ken Segall et Karl Berggren, 2019 (17 pages).

<sup>141</sup> See [Viscosity of Liquid Helium below the  \$\lambda\$ -Point](#), Piotr Kapitsa, Nature (1938) and Flow of liquid helium II, Joan F. Allen, Don Misener, 1938 (1 page). Pyotr Kapitsa was awarded the Nobel Prize in 1978 for his work in the field of low temperatures.

There are two isotopes of helium:  $^3\text{He}$  with a single neutron, which is the least abundant in nature, and  $^4\text{He}$ , with two neutrons, the most common. The latter is a boson, with an integer spin, giving it different properties from helium 3, which is a fermion with a half-integer spin. At low temperature,  $^3\text{He}$  behaves like Bose-Einstein condensates. It becomes superfluid at lower temperatures than  $^4\text{He}$ , at around 1 mK in the absence of a magnetic field (see diagram *above*), vs. 2.17K for  $^4\text{He}$ . Its superfluidity was only discovered in 1973<sup>142</sup>. The different properties of  $^3\text{He}$  and  $^4\text{He}$  are used to operate the dilution cryogenics systems that equip many quantum computers whose operating temperature is between 10mK and 1K. We will study this in [detail](#) in this ebook<sup>143</sup>.



Industrial demand for helium is spread across many industries: medical imaging for MRI systems magnets cooling, then microelectronics industries.



left diagram source: [Wikimedia](#), right diagram source: [Edison Investment Research](#), February 2019, referring to [Kornbluth Helium Consulting](#).

## Bose-Einstein Condensates

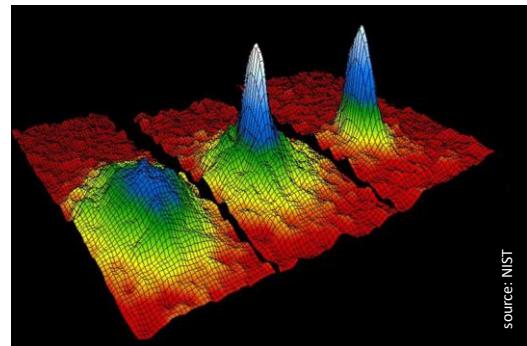
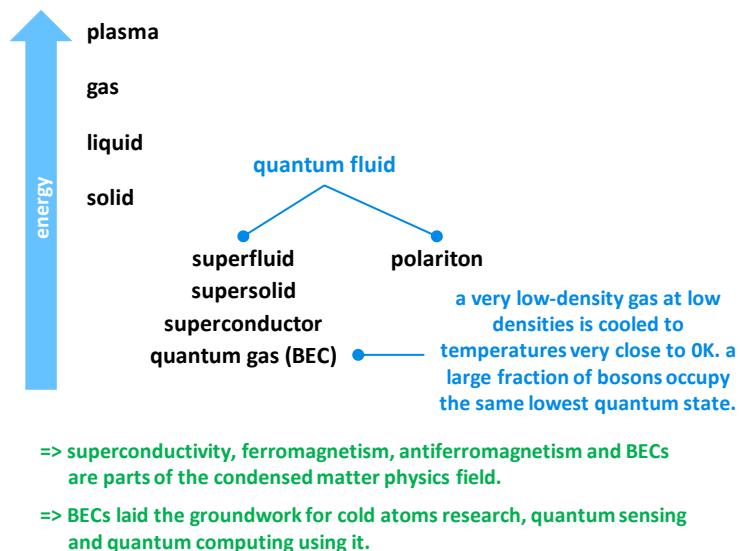
Bose-Einstein condensates are extremely low-density gases of bosons cooled down to very low temperatures, at the lowest energy level we can set matter in, below solid state.  $^4\text{He}$  is the most famous element that was experimented in this matter state. It took a while between the work of Bose and Einstein in 1924 and the experimental discovery of BECs in 1995 by **Karl Weiman, Wolfgang**

<sup>142</sup> David Morris Lee (1931), Douglas Dean Osheroff (1945) and Robert Coleman Richardson (1937-2013) were awarded the Nobel Prize in Physics in 1996 for their discovery of helium-3 superfluidity.

<sup>143</sup> Source of the schema below: [Helium 4](#) (14 slides).

**Ketterle** and **Eric Cornell** with rubidium 87 at 170 nK. It was cooled with laser-based Doppler effect and magnetic evaporating technique.

BECs play an important role in quantum technologies. They led to the control of individual atoms that are used in quantum simulators and in quantum gravimeters. With superfluids and supersolids, BECs belong to the field of quantum hydrodynamics.



**Bose-Einstein condensation at 400, 200 and 50 nK**

prediction: Satyendra Bose and Albert Einstein, 1924

discovery: Karl Weiman, Wolfgang Ketterle and Eric Cornell, 1995

## Supersolidity

Supersolidity is another weird quantum state of matter showing up at ultracold temperatures, when atoms behave as a crystal and as a superfluid at the same time. This is made possible with crystal lattice with holes (like in an NV center). The vacancies behave quantumly as bosons and can switch position in a quantum manner like a Bose Einstein Condensate. It's a vacancies quantum tunnelling phenomenon.

This state of matter was predicted in 1969<sup>144</sup> and it was first demonstrated, although debated for a long time, in 2004 with <sup>4</sup>He at a pressure of about 60 bar and below 170 mK<sup>145</sup>. The related fundamental research is going on in various places in the world like in the USA, Innsbruck<sup>146</sup>, Pisa<sup>147</sup>, Stuttgart, Warsaw, Geneva and Paris. It is now possible to create supersolids with ultracold dipolar quantum gases of highly magnetic lanthanide atoms like erbium and dysprosium. The supersolidity effect can be controlled by a magnetic field.

There are no known practical applications of this phenomenon to date although it could lead to new forms of quantum simulation systems like the ones using cold atoms.

## Polaritons

Polaritons is a field of quantum physics that is rarely mentioned in the context of quantum technologies. It mostly belongs to fundamental research but could be of interest in various fields such as quantum computing and quantum sensing.

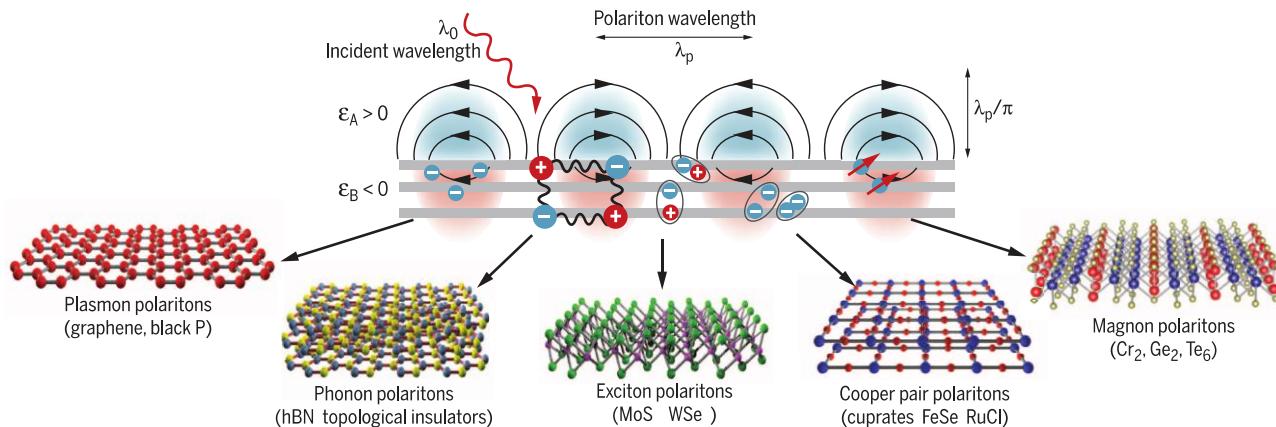
<sup>144</sup> By David J. Thouless (1934-2019, British, 2016 Nobel prize in physics) and, independently, by Alexander Andreev (1939, Russian) and Ilya Mikhailovich Lifshitz (1917-1982, Russian). See [The flow of a dense superfluid](#) by David J. Thouless, 1969 (25 pages) and [Quantum theory of defects in crystals](#) by Alexander Andreev and Ilya Mikhailovich Lifshitz, 1969 (7 pages).

<sup>145</sup> See [Probable observation of a supersolid helium phase](#) by E Kim and M H W Chan, 2004, [The enigma of supersolidity](#) by Sébastien Balibar, Nature, 2010 (7 pages) and the review paper [Saga of Superfluid Solids](#) by Vyacheslav I. Yukalov, 2020 (26 pages).

<sup>146</sup> Research in Austria is led by Francesca Ferlaino from the University of Innsbruck, IQOQI.

<sup>147</sup> See [The supersolid phase of matter](#) by Giovanni Modugno, 2020 (37 slides).

Polaritons are quantum quasi-particles in the domain of strong interactions between light and matter. They result from the coupling between photons and an electrical polarization wave.



These waves occur in particular in plasmons (oscillations of free electrons in metals), phonons (oscillations of atoms, especially in crystal structures) and excitons (pairs of electron holes generated by photons in semiconductors<sup>148</sup>). The materials can be atoms gas, massive classical semiconductors, thin films inserted in optical cavities or superconducting Josephson junctions.

Excitation photons have a wavelength corresponding to the resonance frequency of the associated medium, often in the visible light or infrared ranges. Polaritons have mixed properties of photons dressed by electronic excitations.

They behave like bosons (having an integer spin) that can occupy the same quantum state and operate in groups, such as superconducting currents forms with paired electrons named Cooper pairs or Bose-Einstein condensates (BEC).

Depending on the interaction scale, polaritons operate in a semiclassical or quantum regime. In the first case, the electromagnetic field interacts with a macroscopic polarization field. The polariton field then has the properties of a classical field but its elementary quantum is the result of a dipole-photon "wrapping" that can only be described by quantum mechanics. In the second case, the electromagnetic field interacts with a single polarization field quantum that has been isolated in one way or another, such as a superconducting qubit or an exciton in a quantum box. We are then in the quantum regime of strong coupling, known as the "Jaynes-Cummings Hamiltonian", where the energy levels are discrete and each correlates to a given number of excitation quanta in the system. Cavity-excited polaritons are generally in the first regime.

In polaritons, semiconductor matter receives photons that excite it. It then emits photons to get out of its excited state, all of this in a very fast iterative cycle, the photons circulating in a closed circuit in the cavity. In practice, electromagnetic and polarization fields co-propagate in the medium in an identical way, notably in polarization and frequency, and with a fixed phase relation (without phase shift or with a 180° phase shift, i.e.  $\pi$ ). Polaritons are particularly interesting for generating strong non-linearities which are searched in photonics<sup>149</sup>.

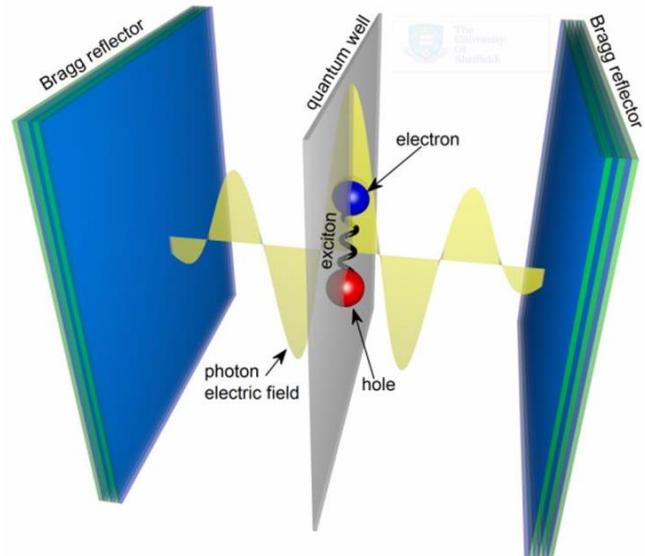
<sup>148</sup> The name of polariton was created by Joseph John Hopfield (1933, American) in 1958 and at that time concerned polariton excitons. See [Theory of the Contribution of Excitons to the Complex Dielectric Constant of Crystals](#) by Joseph John Hopfield, 1058 (14 pages). Hopfield is also known in the field of neural networks in AI with his "Hopfield networks".

<sup>149</sup> Source of the illustration: [Polaritons in van der Waals materials](#) by D. N. Basov et al, 2016 (9 pages) which, in passing makes a good inventory of different types of polaritons and their fields of application. See also this very dense review paper [Quantum Fluids of Light](#) by Iacopo Carusotto and Cristiano Ciuti, 2013 (68 pages).

Thanks to the degenerate states in which polaritons can be prepared and to the fact that they interact with each other, polaritons constitute an out-of-equilibrium quantum fluid called "light quantum fluid", often abusively referred to as "liquid light". Polaritons can thus generate surface waves and propagation phenomena typical of quantum fluids such as superfluids. Polaritons also interact with each other, which is not the case for photons in vacuum<sup>150</sup>. We can experimentally control the spatial distribution of the density, phase and velocity of these fluids of light<sup>151</sup>.

There are many variants of polaritons which depend on the nature of the electronic excitation of the matter:

- **Phonon-polaritons** resulting from the coupling between an infrared photon and an optical phonon caused by the mechanical oscillation of two adjacent ions of opposite charge in a crystalline structure. This oscillation produces an oscillating electric dipole moment. This phenomenon was discovered by **Kirill Tolpygo** (1916-1994, Russian) in 1950 and, independently, by **Kun Huang** (1919-2005, Chinese) in 1951.
- **Exciton-polaritons** result from the coupling of a photon with an exciton in a semiconductor cavity. An exciton is a quasi-particle consisting of an electron-hole pair connected by Coulomb forces, generated by excitation photons. The notion of exciton was created by **Yakov Frenkel** (1894-1952, Russian) in 1931. Like all types of polaritons, these have two energy bands: the high and low polariton. It is a general property of the strong coupling regime between electric dipole and electromagnetic field. Here, the level is high when the photon and the semiconductor are excited and in phase, and low when they are in opposite phase<sup>152</sup>.



Researchers are trying to create transistors using polariton-exciton ([source of the schematic](#)) as well as on single quantum control<sup>153</sup>.

- **Surface plasmon polaritons** (SPP) result from coupling surface plasmons and photons. A plasmon is a quantized oscillation of high-density electron gases. A surface plasmon is a coherent electron oscillation occurring at the interface between two different materials, often a metal and a dielectric or between metal and air. A surface plasmon polariton is an oscillation caused by an incident photon<sup>154</sup>.

---

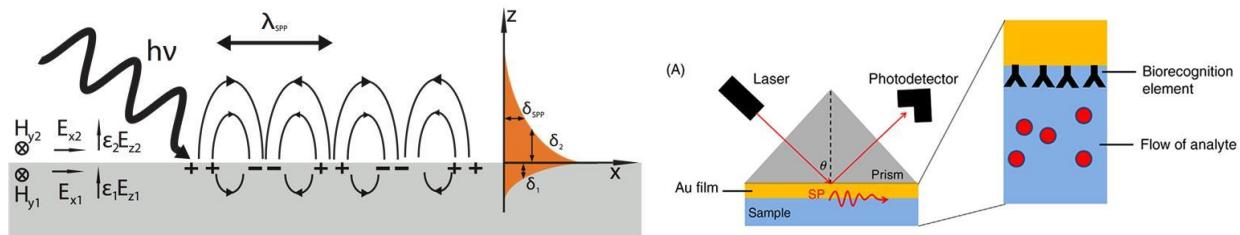
<sup>150</sup> See the pedagogical presentation [Swimming in a sea of light: the adventure of photon hydrodynamics](#) by Iacopo Carusotto, 2010 (28 slides). Presentation realized with the help of, among others, Elisabeth Giacobino and Alberto Bramati from CNRS. See also the very well-illustrated presentation [Quantum fluids of light](#) by Jacqueline Bloch, February 2020 (58 slides).

<sup>151</sup> Source: description of the ANR project: [Quantum Light Fluids - QFL](#) launched in 2016.

<sup>152</sup> Source of illustration: Low Dimensional Structures & Devices Group, University of Sheffield, mentioned [here](#).

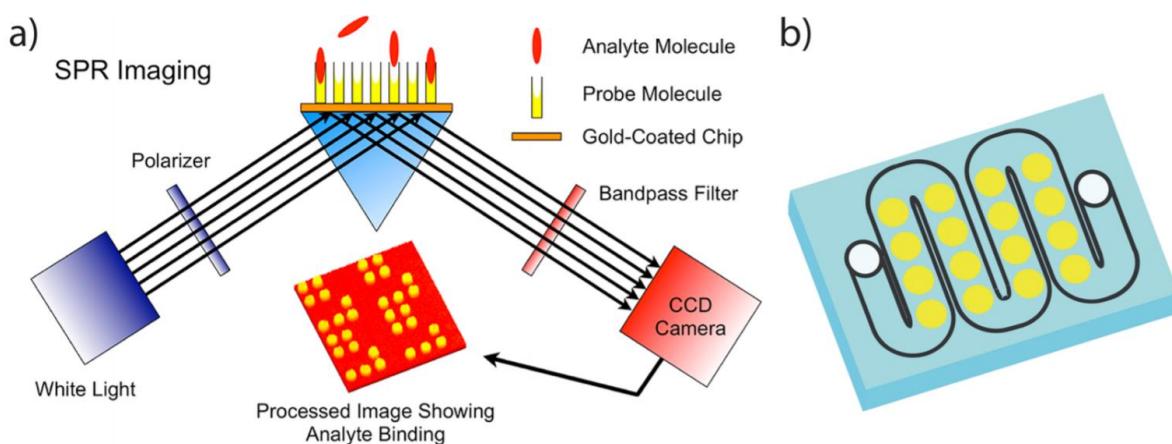
<sup>153</sup> The "polariton blockade" mechanism allows in principle to manipulate excitonic cavity polaritons at the single quantum scale. See [Towards polariton blockade of confined exciton-polaritons](#) by Aymeric Delteil, 2019 (4 pages).

<sup>154</sup> Source of the diagram: [Wikipedia](#).



SPPs are used in optical quantum sensors for temperature and for the detection of the concentration of different components by refractivity and then spectroscopy, especially in medtechs (detection of various organic molecules and of interactions between proteins), biological analyses (toxins, drugs, additives) or for the detection of gases<sup>155</sup>.

SPRs (Surface Plasmon Resonance Plasma) can be much more powerful than near-infrared spectroscopy sensors such as those from Scio<sup>156</sup>. They measure the polarized light reflected from a laser diode in terms of intensity, angle, wavelength, phase and polarization.



As in many biological analysis systems, it is possible to create 2D matrices (microarrays) integrating a large number of detection molecules and to detect a lot of components in the sample to be analyzed<sup>157</sup>.

SPRs are commonly marketed by companies such as **Cytiva** (USA), **Carterra** (USA), **Horiba** (Japan)<sup>158</sup>, **IBIS Technologies** (Netherlands), **Lifeable** (USA), **Polaritons Technologies** (Switzerland) and **XanTec** (Germany).

- **Cavity polaritons** are a variant of the polariton excitons where the photon is trapped in a microcavity and the exciton is confined in a quantum well. They are made of III-V semiconductors like indium, arsenic and gallium.

<sup>155</sup> Source of illustration: [Surface Plasmon Resonance \(SPR\)](#) by Lifeable. The general principle of this instrument is to use a laser diode to illuminate a gold surface at an angle (via a mechanically controllable angle) and to capture the reflected beam with a detector. The gold surface is coated with a specific molecule ("biorecognition element" in the diagram) that tends to associate itself with a molecule that we want to detect (in the liquid phase "flow of analyte"). The molecules detected can be peptides, polypeptides, proteins, enzymes, vitamins, DNA or RNA sequences, or antibodies (in particular for cancers diagnosis). The association modifies the reflectivity of gold and allows the detection of the target molecule.

<sup>156</sup> See [Recent advances in Surface Plasmon Resonance for bio sensing applications and future prospects](#) by Biplob Mondal and Shuwen Zeng, August 2020 (31 pages). The second author is from the Limoges XLIM laboratory in France.

<sup>157</sup> See [Surface Enzyme Chemistries for Ultra sensitive Microarray Biosensing with SPR Imaging](#) by Jennifer B. Fasoli et al, 2015 (10 pages) where the associated illustration comes from.

<sup>158</sup> Whose European research center is located in Palaiseau next to the C2N of the CNRS, Télécom Paris, Thales and the Institut d'Optique.

Photons trapping is often performed using two Bragg mirrors facing each other to create an optical cavity using layers of dielectrics to reflect light very efficiently and of all wavelengths. These mirrors are fabricated from molecular beam epitaxy allowing coherent crystal growth on a gallium arsenide (GaAs) crystal substrate. The result is monocrystalline and can contain more than a hundred layers of different alloys, with thicknesses ranging from 5 nm to 50 nm, controlled to the nearest atomic monolayer<sup>159</sup>. These microcavity polaritons were discovered in 1992 by Claude Weisbuch (France)<sup>160</sup>.

- **Intersubband-polaritons** result from the coupling of an infrared or terahertz photon with an intersubband excitation. They can be used in particular to create infrared detectors.
- And then **Bragg-polaritons** ( Braggoritons ), **plexcitons** (plasmons + excitons), **magnon polaritons** (magnon, spin waves in ferromagnetic materials + photons) and **similaritons** (amplified photons in optical fibers).

In short, all these "-ons" are the result of the interaction between photons and different forms of matter, noticeably electrons. What does this have to do with quantum computing? Polaritons are used in various optical devices related to photon qubits, including photon transport and single photon detectors.

They could eventually allow the creation of photon qubits that can interact with each other. This is what emerged from an MIT and Harvard publication by Vladan Vuletic and Mikhail Lukin in 2018 which demonstrated the interaction of three photons in an atom placed in a Rydberg state, constituting a "Rydberg polariton"<sup>161</sup>. Another research project in Singapore uses polariton excitons to create photon qubits with the particularity of being able to operate at room temperature, using single-qubit gates and  $\sqrt{\text{SWAP}}$  two-qubits gates<sup>162</sup>.

Microcavities polaritons can be used to create quantum simulators<sup>163</sup>. They are implanted in III-V semiconductor structures as 2D arrays. One field of application is the simulation of gravitational structures such as a Hawking radiation on the horizon of a black hole. And why not, to simulate the operation of a dilution refrigerator associating helium 3 and 4 at very low temperature.

Polaritons are also the field of topological behaviors of matter and are perhaps an alternative way to the Majorana fermions to create error corrected qubits. These are longer term pathways than the qubit technologies studied in this book, but worthy of interest.

Other applications, already mentioned, target the very diverse field of quantum sensing.

In France, polaritons are the specialty of **Elisabeth Giacobino** (CNRS, ANR), **Jacqueline Bloch** (CNRS C2N<sup>164</sup>), **Alberto Bramati** (LKB ENS), **Alberto Amo** (Phlam-CNRS Lille), **Le Si Dang** and **Maxime Richard** (CNRS Institut Néel Grenoble).

<sup>159</sup> See [Cavity polaritons for new photonic devices](#) by Esther Wertz, Jacqueline Bloch, Pascale Senellart et al, 2010 (12 pages).

<sup>160</sup> See [Observation of the coupled exciton-photon mode splitting in a semiconductor quantum microcavity](#) by Claude Weisbuch et al, 1992 (4 pages).

<sup>161</sup> See [Physicists create new form of light](#) by Jennifer Chu, 2018 referencing [Observation of three-photon bound states in a quantum non linear medium](#) by Qi-Yu Liang et al, 2018 (5 pages).

<sup>162</sup> We will define this type of quantum gate in a [dedicated section](#) of this ebook. See [Quantum computing with exciton- polariton condensates](#) by Sanjib Ghosh and Timothy C. H. Liew, October 2019 (6 pages). Tim Liew is a researcher at the joint MajuLab laboratory between CNRS and the National University of Singapore.

<sup>163</sup> See [Microcavity Polaritons for Quantum simulation](#) by Thomas Boulier, Alberto Bramati, Elisabeth Giacobino, Jacqueline Bloch et al, May 2020 (21 pages) as well as [Polaritonic XY-Ising machine](#) by Kirill P. Kalinin, Alberto Amo, Jacqueline Bloch and Natalia G. Berloff, 2020 (12 pages).

<sup>164</sup> The clean room of the C2N in Palaiseau, France, allows the prototyping of a whole bunch of nanostructures. The semiconductors used to manage polaritons are moreover manufactured with techniques similar to the single photon sources of Pascale Senellart's team, also from the C2N, and the associated startup, Quandela.

## Magnons

Quantum matter is an endless field. It also includes **magnons**, a category of quasi-particles that take the form of quantized spin waves in magnetic materials, usually crystal lattices. Magnons were conceptualized by **Felix Bloch** in 1930 and experimentally detected in 1957 by **Bertram Brockhouse** (1918-2003, Canadian). These objects which behave as bosons could be used in quantum information systems, with not many details available so far.

Current physics experiments are done at the control low-level like with controlling these magnons with microwaves<sup>165</sup> or measured with superconducting qubits<sup>166</sup>.

Magnons can also be used at low temperature to create some topological materials<sup>167</sup>. It's far from making qubits in the likes of what Microsoft is looking for with Majorana fermions, but who knows?

## Extreme quantum

Beyond the basics of quantum physics mentioned *above*, many other branches of quantum physics deserve to be examined in this book. They can have various impacts on quantum technologies, noticeably on quantum sensing. They are also used in cosmology. Finally, they are unfortunately used by many false sciences and scams that we will discuss in the section dedicated to [quantum hoaxes](#).

### Quantum field theory

Quantum Field Theory (QFT<sup>168</sup>) is a branch of quantum physics that deals with the physics of elementary particles, including their creation or disappearance during various interactions, such as electron and positron pairs. These phenomena are generally reproduced in particle accelerators<sup>169</sup>.

QFT also covers the mechanisms of condensed matter such as Bose-Einstein condensates or superfluid helium and more generally, the behavior of quasiparticles, complex collective behaviors such as Cooper's (electron) pairs in superconducting materials.

QFT combines elements of quantum mechanics, special relativity and classical notions of electromagnetic fields. It is based on a mathematical formalism that is even more difficult to assimilate than the one of non-relativistic quantum physics.

It exploits the notion of Lagrangian and Lagrangian integrals over time describing the evolution of fields and the interactions between the fields of several particles.

QFT is used to explain or modelize the fine structure of the hydrogen atom (corresponding to close spectral lines not explainable by classical quantum energy jumps), the existence of particle spin (which explains these spectral lines), the spontaneous emission of photons by atoms during their return to their fundamental state and the mechanisms of radioactivity.

The foundations of QFT were created by many scientists starting in 1928: **Paul Dirac**, **Wolfgang Pauli**, **Vladimir Fock** (1898-1974, Russian), **Shin'ichirō Tomonaga** (1906-1979, Japanese), **Julian Schwinger** (1918-1994, American), **Richard Feynman** and **Freeman John Dyson** (1923-2020,

---

<sup>165</sup> See [Floquet Cavity Electromagnetics](#) by Jing Xu et al, Argonne Lab and University of Chicago, October 2020 (9 pages).

<sup>166</sup> See [Dissipation-Based Quantum Sensing of Magnons with a Superconducting Qubit](#) by S. P. Wolsk et al, University of Tokyo, September 2020 (6 pages).

<sup>167</sup> See [Topological Magnons: A Review](#) by Paul McClarty, 2021 (21 pages).

<sup>168</sup> Later on, we'll use the QFT acronym with another meaning, Quantum Fourier Transform!

<sup>169</sup> See [The History of QFT](#), a Stanford site, which summarizes the history of QFT.

American<sup>170</sup>). Shin'ichirō Tomonaga, Julian Schwinger and Richard Feynman received the 1965 Nobel Prize in Physics for their work on quantum electrodynamics which is part of QFT.

In the early 1950s, they solved the problem of infinite energy values generated by the initial QFT models by using an adjustment technique called **renormalization**.

Physicists are still struggling to integrate the theory of general relativity into the QFT, preventing it from becoming a "theory of the whole" or unified theory explaining all known physical phenomena in the Universe.

QFT operates in three main areas:

- In the physics of **high-energy particles** explored in particle accelerators such as the CERN LHC. It has been supplemented on this point by the standard model that we will see below.
- In the **physics of condensed matter** with superconductivity, superfluidity and the quantum Hall effect. This is the framework of **QED** (quantum electrodynamics), launched by Paul Dirac in 1928, which studies in particular the production of positrons and positron/electron interactions (attraction, annihilation, pair creation, Compton effect). The **CQED** (cavity QED) sub-branch studies the relations between matter and photons in optical cavities. It is used by condensed matter physicists working on superconducting qubits.
- In **cosmology** to model the origin and evolution of the Universe as well as certain mechanisms of interaction between black holes and quantum fields.

### Quantum vacuum fluctuation

One of the consequences of QFT is the notion of quantum vacuum fluctuation, also called vacuum energy. Based on Heisenberg's principle of indeterminacy that quanta are in perpetual fluctuation, QFT models zero-point fluctuations or vacuum energy, which is the minimum energy level of quantum systems.

In this framework, Heisenberg's principle can be considered as a generalized predicate. According to these models, total vacuum cannot exist. Elementary fluctuations lead to spontaneous electromagnetic waves creation.

One scenario devised by Paul Dirac is the creation of pairs of virtual electron and positron particles, which rapidly annihilate each other, generating photons in the process. But this is not the only solution to his equations. It can come from electromagnetic fields moving at the speed of light.

Under the influence of a surrounding electromagnetic field, this leads to a polarization of the vacuum. The latter even leads to make the vacuum birefringent, its refractive index depending on the polarization of the light that gets through it. The phenomenon is however potentially observable only with some very intense electromagnetic field.

Theoretical models initially indicated that this vacuum energy would be infinite on the scale of the Universe. They were then corrected using the renormalization method, already mentioned above. These elementary vacuum fluctuations would explain the spontaneous emission of radiation by the electrons in the atoms as well as the spontaneous radioactivity<sup>171</sup>.

---

<sup>170</sup> It also gave rise to the notion of the Dyson sphere, which dimensions the level of technological control of energy sources by extraterrestrial civilizations, with a sphere capturing the totality of a star's energy.

<sup>171</sup> In addition to these elementary fluctuations, vacuum is constantly traversed, even in the remotest regions of space, by electromagnetic waves, not to mention the effects of gravitation. The Universe is thus filled with radiations including the cosmological background noise which is a remnant of the big bang, having a temperature of 2.7K. It is the same in a vacuum-packed box because all matter emits radiation.

The concept of vacuum energy originated with **Max Planck** in 1911 when he published an article containing an energy equation for a medium containing a fixed constant, a kind of energy floor for this medium, without being able to interpret it. It was not until 1916 that the chemist **Walther Nernst** (1864-1941, German<sup>172</sup>) interpreted this constant as the energy level of the vacuum in the absence of any radiation. It happens when you cool down a black body to a very low temperature, below a couple millikelvins (mK).

According to the QFT, the Universe is a vast soup containing constantly fluctuating fields, both fermions (leptons and quarks) and bosons (force fields like gluons that stick together the elementary constituents of atomic nuclei that are protons and photons). This notion of minimum energy level is a modern version of the notion of ether - a not completely empty void - which dominated 19th century physics, notably for James Clerk Maxwell. The electromagnetic bath in which the vacuum is immersed, supplemented by the energy of the vacuum, would give vacuum some viscosity properties.

Still, these theories are less complete than classical quantum mechanics. One of the solutions is to assume that fermions have a negative vacuum energy and bosons have a positive vacuum energy, both balancing each other. But this has not been demonstrated experimentally, particularly with non-relativistic energy particles.

There could also be some link between vacuum energy and the dark energy of the Universe as well as gravity. This is very speculative. It could help explain the 73% of the energy contained in the Universe, sometimes called dark energy. Its density is very low, at  $10^{-13}$  Joules/cm<sup>2</sup>.

There are different ways to verify the existence of quantum vacuum fluctuations. The best-known is related to the Casimir effect that we will study *below*. Recently, French and German scientists have also managed to interact with this quantum vacuum fluctuation in a semiconductor<sup>173</sup>.

## Casimir effect

The physicist **Hendrik Casimir** (1909-2000, Dutch) predicted in 1948 the existence of an attractive force between two parallel electrically conductive and uncharged plates<sup>174</sup>. He obtained his PhD in 1931 at the University of Leiden in the Netherlands.

He also visited Niels Bohr in Copenhagen and was a research assistant to Wolfgang Pauli in 1938. The Casimir effect is interpreted as being related to the existence of quantum vacuum energy.

The experiment imagined by Casimir uses parallel mirrored metal surfaces that are as perfectly flat as possible. They create a Fabry-Perot cavity similar to the one that used in lasers.

The Casimir effect is commonly attributed to quantum fluctuations in vacuum. Temporary changes in the energy level at points in the space between the two mirrors would spontaneously generate pairs of very short-lived particles and antiparticles and photons associated with their annihilation. These vacuum fluctuations take place in and out of the volume of the cavity.

Because of the interference effect induced by the cavity, fluctuations at certain frequencies are reduced. The density of electromagnetic energy in the cavity is thus lower than the density of energy outside the cavity<sup>175</sup>. These are spontaneous quantum fluctuations.

---

<sup>172</sup> Walther Nernst played a key role in launching the Solvay Congresses from 1911 onwards.

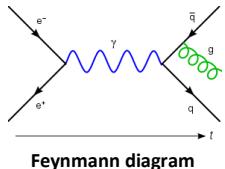
<sup>173</sup> See [Understanding vacuum fluctuations in space](#), August 2020 and [Electric field correlation measurements on the electromagnetic vacuum state](#) by Ileana-Cristina Benea-Chelmu, Jérôme Faist et al, 2018/2020.

<sup>174</sup> <http://aflb.ensmp.fr/AFLB-291/aflb291p331.pdf> See [On the attraction between two perfectly conducting plates](#) by Hendrik Casimir, 1948 (3 pages) and [Electromagnetic vacuum fluctuations, Casimir and Van der Waals forces](#) by Cyriaque Genet, Astrid Lambrecht et al, 2004 (18 pages).

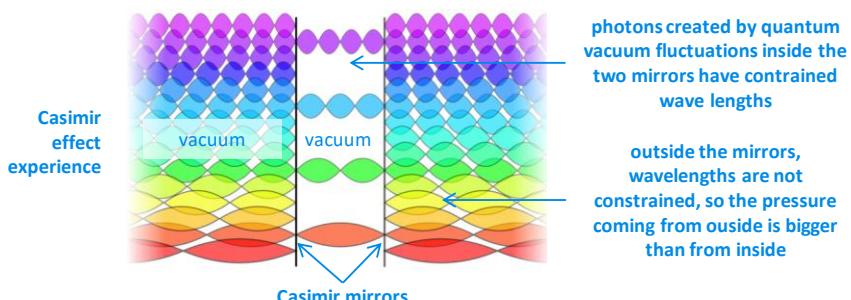
according to quantum field theory and Heisenberg principle, vacuum contains harmonic oscillators with zero-point energy:

$$E = \frac{1}{2} h\nu \quad \Delta E \cdot \Delta t \geq \frac{\hbar}{2}$$

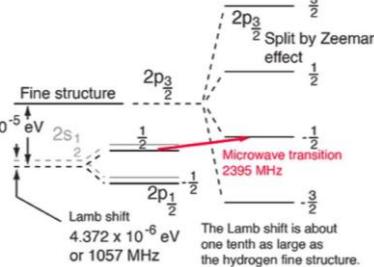
with electrons/positrons spontaneously created and annihilating, creating photons



=> one source of noise and decoherence in most qubits



Lamb shift



energy shift observed between two levels of hyperfine structure in hydrogen atom, explained by quantum vacuum fluctuations impacting electrons

The effect cannot be explained by the simple pressure that is higher on the outside than the pressure between the two plates. In detail, the wavelengths of the photons generated by the vacuum outside the plates can be of any size and especially long while inside the plates, these wavelengths are constrained by the distance between the plates and can only be  $1/n$  of this distance. The spontaneous electromagnetic spectrum of the vacuum is therefore wider outside the plates than inside, creating a stronger pressure inside than outside, which therefore tends to make the plates move closer together, but very slightly.

For two parallel mirrors of surface A and a distance L between the two mirrors, the force of attraction between the two mirrors follows the formula on the right. In practice, L is between 0.2  $\mu\text{m}$  and 5  $\mu\text{m}$  and is usually 1  $\mu\text{m}$ . This is a "macroscopic" scale.

$$F_{Cas} = \frac{\hbar c \pi^2 A}{240 L^4}$$

$$\Delta E \cdot \Delta t \geq \frac{\hbar}{2}$$

According to Heisenberg's principle, which is used to explain the effect, energy and time can be linked by the formula on the right. It shows indirectly that during a very short time, a small amount of energy can be created.

The macroscopic accumulation of these operations is annihilated, making it possible to avoid a violation of the energy conservation principle. So, be uber-skeptical when hearing anyone claiming they can harvest energy from vacuum to produce free electricity.

The experiments are not necessarily 100% conclusive and the data generated do not fit perfectly with the models unlike many classical quantum mechanics experiments. The reason for this is that it is difficult to obtain perfect surfaces.

The first experiments validating the Casimir effect were carried out almost 50 years after the definition of this effect<sup>175</sup>. The first one is that of **Steve Lamoreaux** (American) in 1996, using parallel plates.

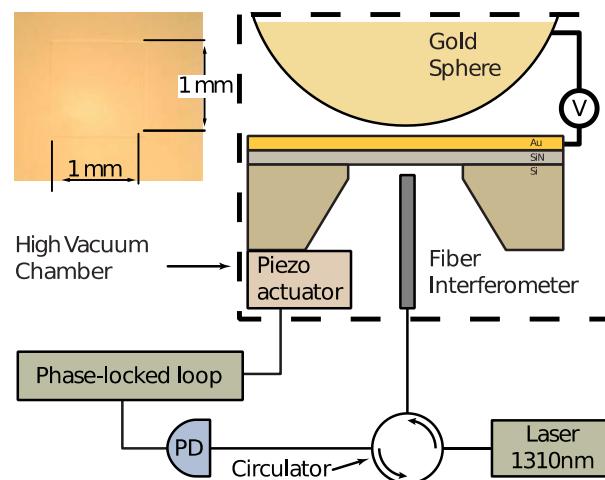
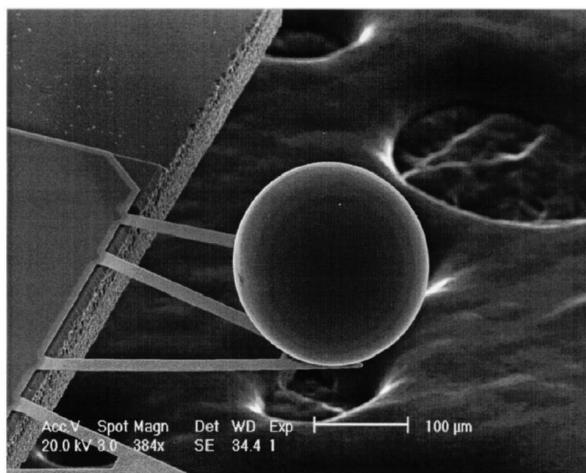
<sup>175</sup> See a good panorama of the Casimir effect with [The Casimir effect and the physical vacuum](#) by G. Takács, 2014 (111 slides). See also [The Casimir Effect](#) by Kyle Kingsbury, 2014 (82 slides) which describes well the experimental devices for the evaluation of the Casimir effect and evokes some cases of use in MEMS. And then [Zero-Point Energy and Casimir Effect](#) by Gerold Gründler, 2013 (47 pages), which casts the history of the Casimir effect, going back to Planck's work in 1911.

<sup>176</sup> The experimental difficulty consists in cancelling out all the other forces between the two plates and they are all much larger than the Casimir effect, particularly electrostatic and van der Waals forces.

His measurement gave a result that was 5% off the predictions. The precision instruments used then detected a force of one billionth of a Newton. The model was improved in other experiments carried out in 1998 and again in 2012 using an electrode geometry combining a plane and a polystyrene sphere with a diameter of 200  $\mu\text{m}$  and covered with gold (diagrams below)<sup>177</sup>. The differences between the models and the measurements decreased to 1%, which remains significant in physics.

The Casimir effect could explain several other commonly observed physical phenomena such as the electron's abnormal magnetic moment and the Lamb shift. The first phenomenon describes a drift of this magnetic moment with respect to Dirac's equations.

The second comes from **Willis Eugene Lamb** (1913-2008, American), Nobel Prize in Physics in 1955, who had done his thesis under the supervision of Robert Oppenheimer. Lamb shift is an energy gap observed between two levels of fine structure of the hydrogen atom, two very close energy levels. The effect is explained with the perturbations coming from vacuum fluctuations and affecting the electron in these two neighboring energy levels, creating the spontaneous generation of photons that are rapidly absorbed by the electron.



The effect was discovered in 1947 by Willis Eugene Lamb and interpreted the same year by **Hans Bethe** (1906-2005, German) for the hydrogen spectrum using the idea of mass renormalization. It was used in the development of post-war quantum electrodynamics<sup>178</sup>.

The polarization of vacuum explains part of this shift at 27 MHz for a total of 1057 MHz<sup>179</sup>. The calculation uses the fine-structure constant  $\alpha$  (about 1/137) which describes the contribution of vacuum energy to the electron's anomalous magnetic moment. The  $\alpha$  constant is also used to quantify the strength of the electromagnetic interaction between elementary charged particles.

There is also a **Dynamic Casimir Effect** (DCE), discovered by **Gerald Moore** in 1969. It generates pairs of particles by the movement of the mirrors used in the Casimir experiment<sup>180</sup>.

As with the Casimir Effect, the energy observed is infinitesimal. For the energy to be significant, the mirrors would have to move at relativistic velocities, which is not very practical. And there is no problem with energy conservation, the necessary energy being provided by the mirror movement. The vacuum simply serves as a non-linear medium!

<sup>177</sup> See [Physicists solve Casimir conundrum](#) by Hamish Johnston, 2012 which refers to [Casimir Force and In Situ Surface Potential Measurements on Nanomembranes](#) by Steve Lamoreaux et al, 2012 (6 pages).

<sup>178</sup> Source of the diagram and associated explanations: [The Lamb Shift](#).

<sup>179</sup> This phenomenon of vacuum polarization in the Lamb effect is described in [The Vacuum Polarisation Contribution to the Lamb Shift Using Non-Relativistic Quantum Electrodynamics](#) by Jonas Frajord, 2016 (61 pages).

<sup>180</sup> See [Electro-mechanical Casimir effect](#) by Mikel Sanz, Enrique Solano et al, 2018 (10 pages).

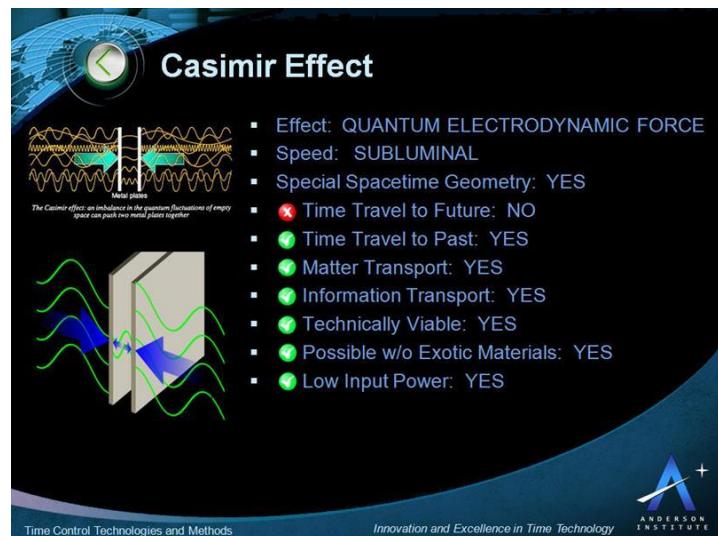
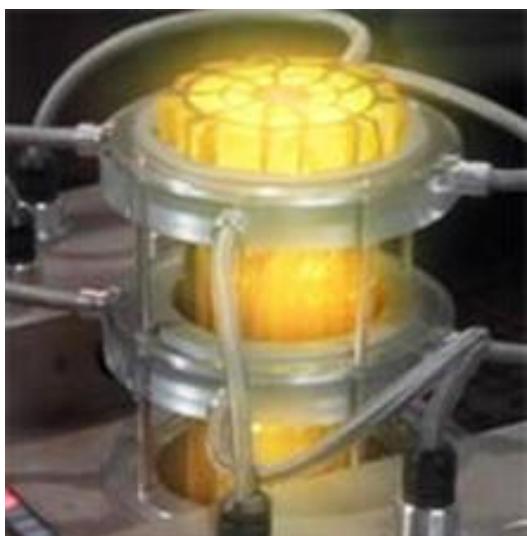
The interpretation of the Casimir effect is still debated. Some physicists explain it by other mechanisms than vacuum energy.

They rely on the **van der Waals** (1837-1923, another Dutch) forces, where atoms attract or repel each other depending on their distances<sup>181</sup>. However, this infinitesimal force works at a microscopic scale, where the Casimir effect operates at a macroscopic scale.

French physicists are quite active in the field, and, in particular **Astrid Lambrecht**, formerly director of the INP of the CNRS, the Institute of Physics which oversees the physics laboratories of the CNRS<sup>182</sup>.

The Casimir effect could be of interest in quantum metrology to create sensors and in particular NEMS/MEMS.

These theories on quantum vacuum fluctuation and the Casimir effect are also fraudulently exploited by the creators of so-called machines capable of capturing vacuum energy, which collect nothing at all in practice. The fluctuation-dissipation theorem ensures that quantum vacuum fluctuations does not violate the second principle of thermodynamics. No energy can be recovered thanks to these fluctuations! Forget it.



For example, you have a certain **David Lewis Anderson**, who started the **Anderson Institute** in 1990, who claims to be able to use the Casimir effect to travel back in time and create a "free" electricity generator<sup>183</sup>.

In other cases, the Casimir effect is exploited in a scientific but borderline way to imagine science fiction scenarios like ways to cross wormholes<sup>184</sup>.

<sup>181</sup> See [The origin of Casimir effect: Vacuum energy or van der Waals force?](#) by Hrvoje Nikolic, 2018 (41 slides) and the even more skeptic [The Casimir-Effect: No Manifestation of Zero-Point Energy](#) by Gerold Gründler, 2013 (15 pages) and [All wrong with the Casimir effect](#) by Astrid Karnassnigg, 2014 (3 pages). Then, [The Casimir effect: a force from nothing](#) by Astrid Lambrecht, 2007 (5 pages).

<sup>182</sup> See [The Casimir effect theories and experiments](#) by Romain Guérout, Astrid Lambrecht and Serge Reynaud, LKB, 2010 (28 slides) and [Casimir effect and short-range gravity tests](#), LKB, 2013 (15 slides). Astrid Lambrecht chaired the [Casimir RNP](#) group, which brought together researchers from around the world working on the Casimir effect. The group was active between 2009 and 2014.

<sup>183</sup> Its website seems to be inactive since 2012. See this radio interview from 2019 with the guy who defies the laws of bullshit in his talk. It shows how an interviewer lacking some scientific background can be fooled by a good talker. In [See Is Time Travel Real?](#) 2019 and the [Anderson Institute](#) website.

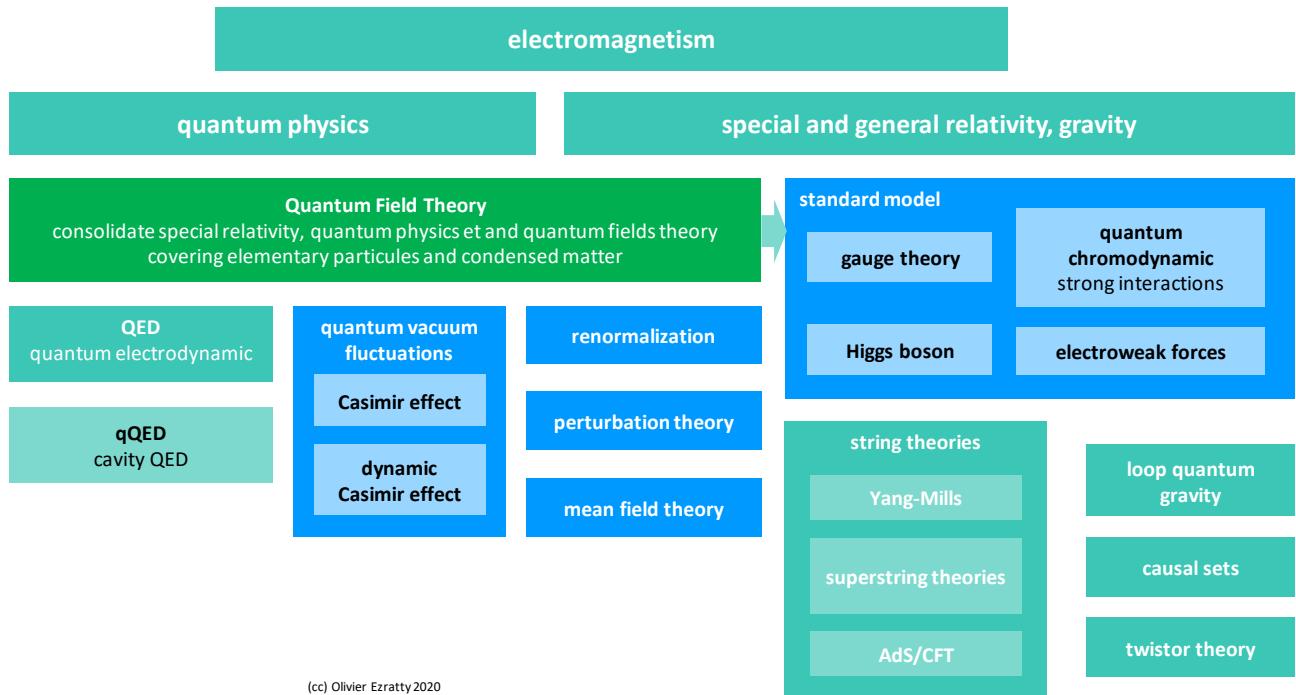
<sup>184</sup> See [One Theory Beyond the Standard Model Could Allow Wormholes that You Could Actually Fly Through - Universe Today](#) by Matt Williams, August 2020, mentioning [Humanly traversable wormholes](#) by Juan Maldacena and Alexey Milekhin, August 2020.

The **NASA** even explored the idea to use sails and vacuum fluctuation to propel a space vessel between 1996 and 2002, to no avail. It was one of the ideas explored as part of the fancy Breakthrough Propulsion Physics Program, which was awarded a tiny budget of \$1.2M and later cancelled.

## Unifying theories

The quest of a **unified theory** has occupied many physicists for nearly a century. Its goal would be to consolidate all the physics theories and in particular, quantum physics, relativity and gravity into a single formalism. In addition to the QFT, a very large number of explanatory and unifying theories of physics have been developed.

No such theory is considered today as being complete. Here's a rough map showing how these different theories are related.



**Quantum chromodynamics** provides a description of the strong interactions binding quarks together via gluons to form particles called hadrons, namely, protons and neutrons. Murray Gell-Mann (1929-2019, American, Nobel Prize in Physics in 1969) and Georges Zweig (1935, Russian then American, former PhD student of Richard Feynman) each proposed the existence of quarks in 1963. Quantum chromodynamics is an extension of the quantum field theory developed in 1972 by Murray Gell-Mann and Harald Fritzsch.

**Standard model** describes the architecture of known elementary particles and their interactions. It models the fundamental weak and strong electromagnetic forces. It only lacks gravity to be complete. This model predicted the existence of quarks, these massive particles forming neutrons and protons, in addition to other elementary particles such as the famous Higgs boson whose existence was proven at CERN's LHC in 2012. The expression "standard model" was created in 1975. It's also called a gauge theory because of its mathematical symmetries.

It is not the first of its kind because Maxwell's electromagnetism is also a gauge theory, between magnetic and electric fields. The standard model particles do not cover the famous dark matter whose nature is not yet known.

**String theory** combines general relativity and quantum physics to propose a quantum explanation of gravity, using a new massless particle, the graviton. According to this theory, elementary particles are tiny strings, open or closed, with vibrations types defining the nature of the particle. Their size is of the order of magnitude of  $10^{-35}$  m, the Planck length. According to this theory, the Universe would be a set of vibrating strings.

The graviton would join the three other forces of nature intermediated by particles without mass: electromagnetic waves by photons, strong interactions by gluons that link quarks together in protons and neutrons and weak interactions provided by the W and Z bosons that govern atomic nuclei and in particular radioactivity<sup>185</sup>. String theory essentially covers bosons of all kinds.

**Superstring theory** is an extension of the string theory that adds fermions to the code theory model that focused on bosons. It is based on the notion of supersymmetry which extends the standard model by making each type of boson correspond to a type of fermion. The theory took shape in 1943 with Werner Heisenberg in the form of the S-matrix theory, and then was reborn in 1984. It uses 10 dimensions to describe physics, far beyond the four classical dimensions (three for position and one for time). It also uses the notion of "branes" which describes point particles in these multi-dimensional spaces. However, this theory is not unique since there are five variants, which some people try to unify in the **M-theory**, which is based on 11 dimensions. A never-ending story!

**Loop quantum gravity theory** competes with the superstring theory to explain gravity. It discretizes the effects of gravity by presenting space as a meshed structure with quantized areas and volumes of space, and gravitational field quanta connected to each other by links characterized by a spin<sup>186</sup>.

#### A brief history of quantum gravity:

- 1952 Flat space quantization (Rosenfeld, Pauli, Fierz, Gupta, ...)
- 1959 Canonical structure of general relativity (Dirac, Bergmann, Arnowit, Deser, Misner)
- 1964 Penrose introduces the idea of spin networks
- 1967 Wheeler-DeWitt equation
- 1974 Hawking radiation and black hole entropy
- 1984 String theory
- 1986 New variables for general relativity (Ashtekar, Sen)
- 1988 Loop representation and solutions to the Wheeler-DeWitt equation (Jacobson, Smolin)
- 1989 Extra dimensions from string theory
- 1995 Hilbert space of loop quantum gravity, geometric operators
- 2000' Spin foam models, group field theory, loop quantum cosmology, ...

For this theory created in 2001, the Universe would be a gigantic spin foam. Its main promoters are **Carlo Rovelli** (Center for Theoretical Physics in Marseille) and **Lee Smolin** (Perimeter Institute for Theoretical Physics in Waterloo<sup>187</sup>).

---

<sup>185</sup> W bosons transform up quarks into down quarks and neutrinos into electrons. The up and down quarks are the two types of quarks. Their proportion is 2 up + 1 down for protons and 1 up + 2 down for neutrons. A quark has a size close to that of an electron, about  $10^{-16}$  cm. Radioactivity emits alpha rays via strong forces, particles comprising two protons and two neutrons (helium 4 atom without electron), beta rays generated by weak forces which are electrons or positrons and finally gamma rays which are photons of very high energy level.

<sup>186</sup> It is reminiscent of the recent theory of the whole built by Stephen Wolfram and published in 2020.

<sup>187</sup> See [Lee Smolin Public Lecture Special:Einstein's Unfinished Revolution](#), 2019 (1h13mn) where he describes the shortcomings of quantum mechanics.

The seeds of the theory date back to 1952, with many intermediate stages<sup>188</sup>. It is, above all, a mathematical and topological model. It does not seem to formulate an experimental validation method.

These are only a few of the many theories being devised. Some amateurs also try to create their own theory of the whole, without usually obtaining any feedback from the scientific community<sup>189</sup>.

## Quantum physics 101 key takeaways

- Quantum physics is based on a set of postulates and a strong linear algebra mathematical formalism. Surprisingly, there are many variations of these postulates. There is not a single bible or reference for these, illustrating the diversity of pedagogies and opinions in quantum physics. But the theory has been validated by an incredible number of experiments.
- Quantum physics describe the behavior of matter and light at nanoscopic levels. It deals not only with atoms, electrons and photons which are used in quantum information technologies but also with all elementary particles from the standard model (quarks, ...).
- Quantumness comes from the quantification of many properties of light and matter that can take only discrete values, from the wave-particle duality of massive (atoms, electrons) and non-massive (photons) particles, and from wave-particle duality and its consequences like superposition and entanglement. By the way, a cat can't be both alive and dead since it's not a nanoscopic quantum object. Forget the cat and instead, learn Schrodinger's equation!
- Indetermination principle states it's impossible to measure with an infinite precision quantum objects properties that are complementary like speed and position. You can use this principle to improve measurement precision in one dimension at the expense of the other. It is used in photons squeezing, itself applied in the LIGO giant gravitational waves interferometer.
- Quantum matter and fluids are showing up with composite elements associating light and matter, or with superfluidity and superconductivity where boson quantum objects can behave like a single quantum object.
- Quantum physics also explains weird effects like vacuum quantum fluctuation, although it doesn't violate the second principle of thermodynamics nor can it lead to the creation of some free energy sources.
- Most of quantum physics phenomena as described in this section have or will have some use cases in quantum information science and technologies.

<sup>188</sup> Chronology source: [The philosophy behind loop quantum gravity](#) by Marc Geiller, 2001 (65 slides).

<sup>189</sup> See, for example, the [Unified Theory Research Team](#) website, which announced the publication in September 2020 of a theory model of the whole called MME for Model of Material and Energy. The site claims that its model, which is presented as an algorithmic approach, can explain everything, from the functioning of all particles to the bricks of life. The team behind this project includes two Pierre and Frédéric Lepeltier from France. The first has been the CEO of the Unified Theory Research Team for 32 years.

# Gate-based quantum computing

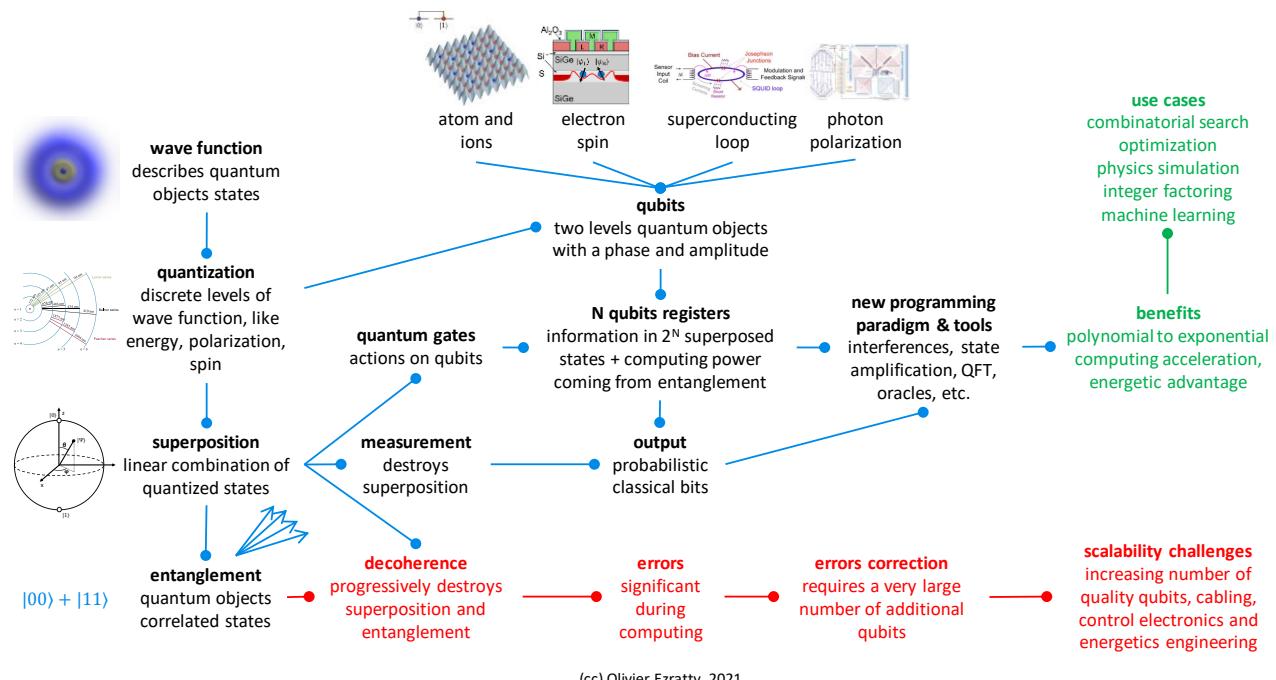
As a computer scientist, you may have skipped all the previous parts to get here right away. One can indeed understand how quantum computers operate without delving too deeply into quantum physics beyond grasping its basic mechanisms. Some mathematical knowledge is however required on trigonometry and linear algebra, including vectors, matrices and complex numbers<sup>190</sup>.

The first basic element of a quantum computer is its inevitable qubit. You've probably already heard about this mysterious object having "simultaneously" the values 0 and 1. As a result, you've been told that a set of N qubits create an exponential  $2^N$  superposed state that explains the power of quantum computing. Unfortunately, most explanations usually stop there and you then end up wondering how it actually works to make some calculation. What comes in and out of a quantum computer? How is it programmed? How do you feed it with data and code? Where is it useful? This book is there to provide you with some educated answers to all these critical questions.

We will cover here the logical and mathematical aspects of qubits, qubit registers, quantum gates and measurement<sup>191</sup>. Each and every time, when possible, we'll draw parallels with traditional computing. In the following part, we'll look at quantum computer engineering and hardware and even describe the complete architecture of a superconducting qubits quantum computer.

## In a nutshell

Before digging into qubits, qubit registers and the likes, here's a tentative to summarize the key elements of gate-based quantum computing that we'll cover in details afterwards. It shows how physics and mathematics are intertwined.



(cc) Olivier Ezratty, 2021

<sup>190</sup> Complex numbers were created by the polymath Girolamo Cardano (1501-1576, Italian) and the Algerian mathematician Raffaele Bombelli (1526-1572, Italian) between 1545 and 1569. Complex numbers were used in particular to solve polynomial equations associating cubes and squares that occupied Italian mathematicians since the end of the fifteenth century. See [A Short History of Complex Numbers](#) by Orlando Merino, 2006 (5 pages).

<sup>191</sup> The name qubit, fusion of 'quantum' and 'bit', appeared in 1995 in [Quantum coding](#) by Benjamin Schumacher, April 1995 (34 pages).

## Wave function

mother equation of quantum physics, created by Erwin Schrödinger. It describes particles properties probabilities in space and time with a complex number. This equation is specific to non relativistic massive particles. We also use photons in quantum computing, whose properties are defined by Maxwell's electromagnetic equations.

## Quantization

properties of quantum objects, having discrete, not continuous and exclusive values. It enables the creation of qubit physical and logical objects having two levels.

## Superposition

qubits are quantized quantum objects having two basis computational states  $|0\rangle$  and  $|1\rangle$ . These can be combined linearly, thanks to the linearity over space of Schrödinger's wave equation. Solutions of this equation can be linearly combined with complex numbers. Thus, a wave adding two solution waves is still a solution. This doesn't mean the qubit is really simultaneously in two states.

## Entanglement

often presented as a situation where several quantum objects have properties that are correlated. Actually, entanglement is the consequence of superposition of several qubits states. This is the phenomenon that provides both a real theoretical exponential acceleration to quantum computing but also enables conditional relations between qubits. Without it, qubits would be independant and no calculus could be done.

## Qubits

mathematical objects with two levels 0 and 1. It's described by two complex number amplitudes. But due to normalization and getting rid of their global phase (we'll explain all of that), they are described by two real numbers for their amplitude and phase. Physical qubits are based on massive (electron, controlled atoms, superconducting currents) or non massive quantum objects (photons) and one of their quantum properties or observables (spin, energy level, current direction of phase, polarity).

## Registers

physical and logical assemblies of several qubits. With N qubits, they can handle computing on  $2^N$  computational basis states together, being the possible combinations of N 0s and 1s. Computing power comes from entanglement which makes it possible to manipulate an ever greater system of  $2^{2N-1}$  complex numbers.

## Quantum gates

logical operations exerted on qubits. We have single qubit gates which are changing single qubit states and several qubit gates conditionnally changing one or two qubits based on the state of a control qubit, and leveraging entanglement. Gates are the only mechanism used to feed a quantum register with data and instructions. These are not separated as in classical computing based on a Von Neumann / Turing machine model.

## Programming paradigms

quantum programming is based on very different paradigms than classical programming. In a nutshell, it's analog-based. We play with interferences, states amplification, quantum Fourier transforms and the concept of oracles.

## Measurement

the way to extract information from qubits. Unfortunately, you can't read the two real numbers describing the qubit state nor the combination of qubit registers computational basis states. You get just classical 0s and 1s for each qubit. Quantum algorithms toy with the wealth of superposition and entanglement during computing to recover a simple result at the end. Measurement is also used during quantum error corrections.

## Output

for a register of N qubits, you get N 0s and 1s. But these are probabilistic results. You usually need to run your algorithm several times and compute an average of the results to get a deterministic result. Noise and decoherence are additional reasons why you need to do this several times.

## Benefit

an acceleration of computing time com-pared to the best classical computers. Accelerations can be from polynomial to exponential. The benefit can also be economic like with the energetic cost of quantum computing that many expect to be fairly low compared to classical computing.

## Use cases

quantum computing will not replace most use cases of classical computing. It brings value for complex combinatorial problems, optimization problems, quantum physics simulation, some machine learning problems and at last, fast integer factoring.

## Decoherence

the enemy with quantum computing. This is when qubit states is degraded, both for superposition and entanglement. It results from the interactions between the qubits and their environment despite of all the care implemented to isolate it.

## Errors

result of decoherence and other perturbations affecting the qubits. Their phase and amplitude is degraded over time. Existing error rates are many order of magnitude higher than with classical computing. These are the reasons why we don't have yet quantum computers with a very high number of functional qubits.

## Error corrections

set of techniques used to correct these errors. It requires assembling so-called logical qubits made of a great number of physical qubits. The needed ratio at this point is about 10,000 physical qubits to create a logical qubit.

## Scalability challenges

assembling these huge logical qubit is the mother of the challenges with quantum computing. It's not easy to assemble that many qubits and keeping them stable, limit their decoherence and the likes. On top of that, assembling a great number of qubits creates huge engineering challenges with cryogenics cooling power, thermal dissipation, cabling and control electronics. These are the reason why quantum computers don't scale yet to bring their expected benefits.

# Linear algebra

Quantum physics and computing requires some understanding of a whole bunch of concepts of linear algebra that we will quickly scan here. They are associated with a mathematical formalism describing quantum phenomena. This mathematical formalism is also the cornerstone of quantum physics postulates, already covered in an earlier section, page 89. It is also essential to create quantum algorithms.

I will try to explain some of these concepts and mathematical conventions that are used with quantum computing. This will mainly allow you to find your way through some of the scientific publications I mention in this ebook.

## Linearity

Linear algebra is the branch of mathematics using vector spaces, matrices and linear transformations. In the case of quantum physics and computing, it also deals with complex numbers.

A phenomenon is linear if its effects are proportional to its causes. This translates into the verification of the two equations *opposite*.

$$f(\lambda x) = \lambda f(x) \text{ for all } \lambda, x \in \mathbb{R}$$

$$f(x + y) = f(x) + f(y) \text{ for all } x, y \in \mathbb{R}$$

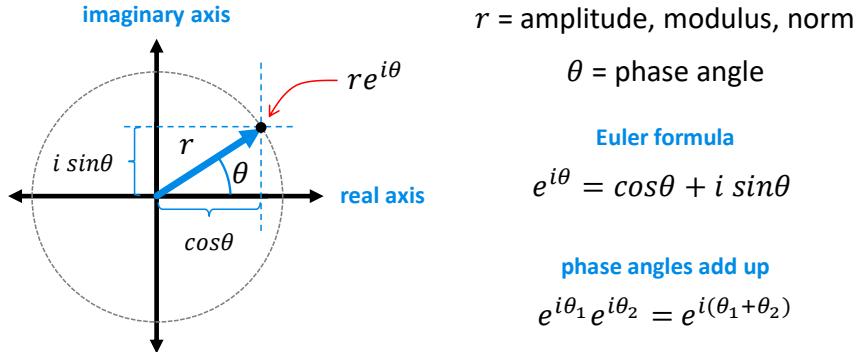
$\mathbb{R}$  being a vector space,  $\lambda$  a real number,  $x$  being a vector of the vector space  $\mathbb{R}$  and  $f(x)$  a function applying to this vector. In a one-dimensional space, a classic example of a linear function is  $f(x) = ax$ . A polynomial function of the type  $f(x) = ax^2 + b$  is obviously not linear because it evolves non-proportionally to  $x$ . Even  $f(x) = ax + b$  is not linear, and for the same reason.

As already defined, an observable is a mathematical operator, a Hermitian matrix, used to measure (mathematically) a property of a physical system. It's frequently assimilated to the measured property. For a qubit, it corresponds to some measurable value by a sensor on a quantum object outputting a classical 0 or 1. The measurement causes the qubit quantum object wave function to collapse on one of the basis states. If the state of a quantum or qubit is measured twice, the measurement will yield the same result. With qubits, observables are usually based on projections on a two-level properties system, mathematically materialized by a  $|0\rangle$  or  $|1\rangle$ , aka qubit computational basis states. But, if the physics permits it, other computational basis can be used. It's the case with photons and polarization measurement where their angle can be easily made different in different parts of an experiment.

## Hilbert spaces and orthonormal basis

Generally speaking, a quantum state of a single or several quantum objects can be described by a vector in a Hilbert space. A qubit state is represented in a two-dimensional orthonormal space formed with the basis states vectors  $|0\rangle$  and  $|1\rangle$ . It is a vector of complex numbers in a two-dimensional Hilbert space allowing lengths and angles measurements. A complex number is defined as  $a+ib$  where  $a$  and  $b$  are real and  $i^2=-1$ .

Complex numbers are very useful in quantum physics. It relates to the wave-particle duality of all quantum objects and to the need to handle their amplitude (complex number norm, vector length or modulus) and phase (the complex number angle when using polar coordinates).



With qubits, it is represented with the complex numbers  $\alpha$  and  $\beta$  associated with the states  $|0\rangle$  and  $|1\rangle$  and whose sum of squares makes 1. This linear combination of the states  $|0\rangle$  and  $|1\rangle$  describes the phenomenon of superposition within a qubit.

This two-dimensional space replaces the infinite-dimensional space that characterizes a Schrödinger wave function  $f(x)$ , where  $x$  can take any value in space. It is thus a simplified representation of the quantum state of a qubit. By manipulating these symbols, the vectors and matrices, we forget a little the wave-like nature of the manipulated quanta, even though it is still present in the phase information embedded in the complex part of  $\alpha$  and  $\beta$  for one qubit. It also can deal with photons which do not obey to Schrödinger's equation but to Maxwell's electromagnetic equations.

An orthonormal basis of a vector space consists of base vectors which are all mathematically orthogonal with each other and whose length is 1. In the representation of a qubit state, the most common orthonormal basis is made of the states  $|0\rangle$  and  $|1\rangle$ .

Other orthonormal reference basis can be used for measurement, particularly with photons, and polarization references different from the starting reference ( $0^\circ/90^\circ$  then  $45^\circ/135^\circ$ , obtained with rotating a simple polarizer).

Another example of an orthonormal basis is the states located on the Bloch sphere on the x-axis and represented with  $|+\rangle$  and  $|-\rangle$ .

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

## Dirac Notation

In Dirac notation, a quantum object state is represented by  $|\Psi\rangle$ , the **ket** of quantum state  $\Psi$ . The **bra** of the same state vector, represented by  $\langle\Psi|$  is the conjugate (or transconjugate, or adjoint) transpose of the "ket". It is the "horizontal" vector  $[\bar{\alpha}, \bar{\beta}]$  where  $\bar{\alpha}$  and  $\bar{\beta}$  are the conjugates of  $\alpha$  and  $\beta$ , inverting the sign of the complex part of the number (-i instead of +i, or the opposite).

The **scalar product** of two qubits  $\langle\Psi_1|\Psi_2\rangle$  is the mathematical projection of the state vector  $\Psi_2$  onto the vector  $\Psi_1$ . This yields a complex number. When the vectors are orthogonal, the scalar product is equal to 0. When the two vectors are identical,  $\langle\Psi|\Psi\rangle$  is  $\Psi$ 's norm and is always equal to 1. A scalar product is also named an inner product.

An **inner product** is a generalization of a dot vector product applied to complex numbers vectors, according to the sigma on the right.

The **outer product** of two vectors representing a qubit, one in bra and the other in ket, gives an operator or density matrix which is a 2x2 matrix.

When the bra corresponds to the transconjugate of the ket, it is a density operator of a pure state. This notion of density operator will then be extended to a combination of qubits.

**vectors**  
**Dirac**  
**notation**

$$|\Psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad \langle\Psi| = \begin{bmatrix} \bar{\alpha}, \bar{\beta} \end{bmatrix}$$

**ψ ket**                                   **ψ bra**

$$(1+i)^* = 1-i$$

**complex number conjugate**

$$\langle\Psi_1|\Psi_2\rangle = [\bar{\alpha}_1, \bar{\beta}_1] \times \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \bar{\alpha}_1 \alpha_2 + \bar{\beta}_1 \beta_2$$

**inner scalar product: vector similarity**

$$\langle\Psi|\Psi\rangle = [\bar{\alpha}, \bar{\beta}] \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha^2 + \beta^2 = 1$$

**inner scalar product**

**complex vectors**  
**dot product**

$$A \cdot B = \sum_i a_i \bar{b}_i$$

$$|\Psi\rangle\langle\Psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \times [\bar{\alpha}, \bar{\beta}] = \begin{bmatrix} \alpha\bar{\alpha} & \alpha\bar{\beta} \\ \beta\bar{\alpha} & \beta\bar{\beta} \end{bmatrix}$$

**outer product**

What are the use cases of this Dirac notation? It is particularly helpful for [manipulating quantum states](#), to simplify tensor products representations and with measurement, which we'll cover [later](#) on page 168.

## Eigenstuff

We also need to define the notions of **eigenvector**, **eigenvalue**, **eigenstate** and **eigenspace** which are often used in quantum mechanics and quantum computing as well as in machine learning, particularly in dimension reduction algorithms such as PCA (Principal Components Analysis). These notions allow to define the structure of certain square matrices<sup>192</sup>.

For a square matrix A, an eigenvector x or eigenvector of A is a vector that verifies the equation  $Ax = \lambda x$ ,  $\lambda$  being a complex number called eigenvalue.

These eigenvectors have the particularity of not changing direction once multiplied by the matrix A. For an eigenvalue  $\lambda$ , the associated eigenspace, or eigenspace, is the set of vectors x that satisfy  $Ax = \lambda x$ . These eigenvalues are evaluated by calculating the determinant of the matrix  $A - \lambda I$ , where I is the identity matrix (1 in the diagonal boxes and 0 elsewhere). We then find the values of which solve  $0 = A - \lambda I$ . It is a polynomial equation having a degree less than or equal to the size of the square matrix<sup>193</sup>.

The reference eigenvectors of a matrix A allow to reconstitute an orthonormal space linked to the matrix. For example, a projection matrix in a 3D plane will have as main eigenvectors two orthogonal vectors located in the plane and one vector orthogonal to the plane. This multiplication gives  $\lambda x$  with  $\lambda$  being non-zero if the eigenvector is in the plane in question and 0 if the vector is orthogonal to the plane<sup>194</sup>. A matrix A can be that of a quantum gate. An eigenvector of a quantum gate is therefore a ket whose value is not modified by the quantum gate.

This is easy to imagine for the S gate, phase change, which we will see later. The  $|0\rangle$  and  $|1\rangle$  kets being in the rotation axis, they are not modified by it.

They are thus eigenvectors of the S gate and the corresponding eigenvalues are 1 and -1. This is always the case for quantum gate matrices since the vectors representing the quantum states, the kets, always have a length of 1. These eigenvalues are the only ones enabling this!

The search for the eigenvectors and eigenvalues of a matrix A is like diagonalizing it. The diagonalization of a square matrix consists in finding the matrix which will multiply it to transform it into a matrix filled only in its diagonal. A matrix A is diagonalizable if we can find a matrix P and a diagonal matrix D such that  $P^{-1}AP = D$  ( $P^{-1}$  being the inverse matrix of P, such that  $P^{-1}P = PP^{-1} = I$ , I being the matrix identity with 1's in the diagonal and 0's elsewhere). A square matrix of dimension n is diagonalizable if it has n mutually independent eigenvectors. The diagonalized matrix diagonal contains the eigenvalues  $\lambda_i$  of the origin matrix, with i=1 to N being the size of the matrix.

A diagonalized quantum state of a quantum object can look like  $A = \sum_i \lambda_i |i\rangle\langle i|$ . This decomposition of a pure state vector in a Hilbert space in eigenstates  $|i\rangle$  and eigenvalues  $\lambda_i$  is also named a **spectral decomposition**. It's linked to the wave-duality aspect of all quantum objects. A quantum object is indeed decomposed into a coherent superposition of elementary waves.

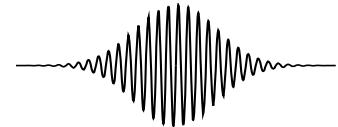
---

<sup>192</sup> See a good quick review of linear algebra in [Linear Algebra Review and Reference](#) by Zico Kolter and Chuong Don 2015 (26 pages).

<sup>193</sup> See this nice visual explanation of eigenvectors and eigenvalues: [Eigenvectors and eigenvalues | Chapter 14, Essence of linear algebra](#), 2016 (17 minutes).

<sup>194</sup> This is well explained in [Gilbert Strang's](#) lecture at MIT, 2011 (51 minutes).

In the case of photons, it's easy to grasp with several photons of different frequencies being superposed and forming a gaussian wavepacket. It constitutes a coherent superposition of the electromagnetic field. These wavepackets are commonly generated by femtosecond pulse lasers<sup>195</sup>.



And the eigenstates? This is another name given to eigenvectors, but by physicists!

## Tensor products

The tensor product of two vectors of dimension m and n gives a vector of dimension m\*n while the tensor product of a matrix of dimension m\*n by a matrix of dimension k\*l will give a matrix of dimension mk\*nl. Tensor products use the sign  $\otimes$ .

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \otimes \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix} = \begin{bmatrix} v_1w_1 & \cdots & v_1w_m \\ \vdots & \ddots & \vdots \\ v_nw_1 & \cdots & v_nw_m \end{bmatrix}$$

**tensor product of two vectors**

$$|\Psi\rangle = \bigotimes_{n=1}^N |i\rangle$$

$|i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle = \begin{bmatrix} \alpha_i \\ \beta_i \end{bmatrix}$

$$|\Psi_1\rangle = \{000 \dots 000\}$$

$$|\Psi_{2^N}\rangle = \{111 \dots 111\}$$

$$\sum_{i=1,2^N} \lambda_i |\Psi_i\rangle$$

$$\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_{2^N} \end{bmatrix}$$

**qubits register state before any entanglement is a tensor product of each qubit 2 dimensions vector**  
dimensionality of  $2N$  real numbers ( $N$  qubits x 2)

**these states can be linearly combined**

**n qubits register pure state  $|\Psi\rangle$  of  $N$  qubits  $|i\rangle$**   
is a point in a Hilbert space with a basis of  $2^N$  orthogonal vectors  $|\Psi_i\rangle$ , these being combinations of  $N |0\rangle$  and  $|1\rangle$ , dimensionality of  $2^{N+1}-1$  real numbers

**a qubit register pure state  $|\Psi\rangle$  representation with its computational basis state vectors amplitudes**

Tensor products are used to compute the state of quantum registers of several qubits that are not entangled. The state of a register of N non-entangled qubits is the tensor product of these N qubits represented by their vertical ket vector.

This gives a ket, a vertical vector that has  $2^N$  different values, each representing the complex number weight of different combinations of 0s and 1s. A quantum register is a superposition of these  $2^N$  different states complex amplitudes. The sum of these squared amplitudes gives 1 per the Born rule.

## Entanglement

Quantum states are separable when they are mathematically the result of the tensor product of each of the pure states that compose it. But these values can be assembled linearly to create another quantum state, modulo a normalization rule. This combines several vectors resulting from tensor products. These combinations can become inseparable.

That's when entanglement comes into play. An entangled state of two or more qubits occurs when it cannot be factorized as the tensor product of two pure states. In other words, it cannot be the combination of independent qubits. The qubits become dependent.

<sup>195</sup> And when the carrier frequency is growing or decreasing through the pulse, it's named a chirp pulse.

This is demonstrated mathematically for the states  $|00\rangle$  and  $|11\rangle$  of a register of two qubits. In these pairs, the measurement of the value of one of the qubits determines that of the other, here identical. The creation of such entangled pairs of qubits requires preparation operations like using a combination of Hadamard and CNOT gates.

Two qubits placed side by side are not magically entangled! The pair used in the example can be generated by two quantum gates, an H gate (Hadamard) and a CNOT gate, as shown just below.

We will define this CNOT gate [later on](#), after page 156. This is described as both qubits having correlated values. But these values are... random since being a perfect superposition of 0 and 1!

Only multi-qubit quantum gates generate entangled qubits in a qubit register, besides the SWAP gate which doesn't. Here with an example of creating a Bell pair associating the states  $|00\rangle$  and  $|11\rangle$  with a mix of Hadamard and CNOT gates.

A so-called **GHZ** state (for Greenberger-Horne-Zeilinger, distinguishable from GHz frequencies with a capital Z) with three entangled qubits is superposing the states  $|000\rangle$  and  $|111\rangle$ . It is prepared with a Hadamard gate and two consecutive CNOTs.

These pairs of Bell and GHZ states are used in error correction codes as well as in telecommunications, among other things.

At last, the level of entanglement of a qubits register depends on the Hamming distance between the basis states involved in the linear superposition of basis states. The far apart they are, with the greater number of non identical 0s and 1s, the greatest the entanglement is.

**an entangled EPR pair can't be a tensor product of two qubits  $|\Psi_1\rangle$  and  $|\Psi_2\rangle$**

$$|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \quad |\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$$

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle)$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

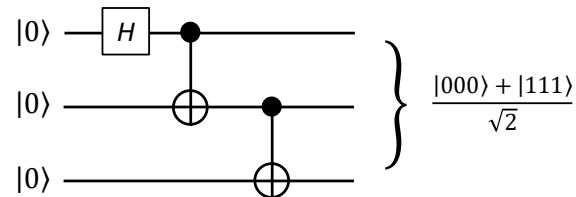
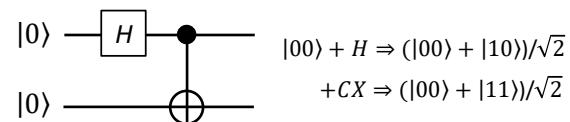
$$\alpha_1\beta_2 = 0 \text{ and } \beta_1\alpha_2 = 0$$

$$\text{are incompatible with } \alpha_1\alpha_2 = \frac{1}{\sqrt{2}} \text{ and } \beta_1\beta_2 = \frac{1}{\sqrt{2}}$$

$$\text{if } \alpha_1 = 0 \text{ then } \alpha_1\alpha_2 = 0$$

$$\text{if } \beta_2 = 0 \text{ then } \beta_1\beta_2 = 0$$

**implications: the density matrix mathematical representation of qubits registers**



## Matrices

Various matrix transformations must be understood here:

- **Matrix conjugate** when all complex numbers see their complex part negated, or  $a_{ij} = a_{ij}^*$ .
- **Matrix transpose** when all matrix  $a_{ij}$  values are transformed into  $a_{ji}$  value, with i=line and j=column indices of matrix “cells”.
- **Matrix transconjugate** which is a conjugate of the transpose or vice-versa, also named adjoint. It's denoted as  $A^\dagger$ , for A « dagger ».
- **Matrix traces** are the sum of their diagonal values, usually normalized to 1, like with density matrices. It's also the sum of their eigenvalues.

We also have three important classes of matrices:

- Hermitian matrices are equal to their transconjugate, meaning that  $a_{ij} = a_{ji}^*$ .

- **Projectors** are matrix operators using a Hermitian matrix that is equal to its square. A diagonalized projector contains only zeros and a single 1. A projector is a non-unitary operation. It relates with the irreversibility of quantum measurement.

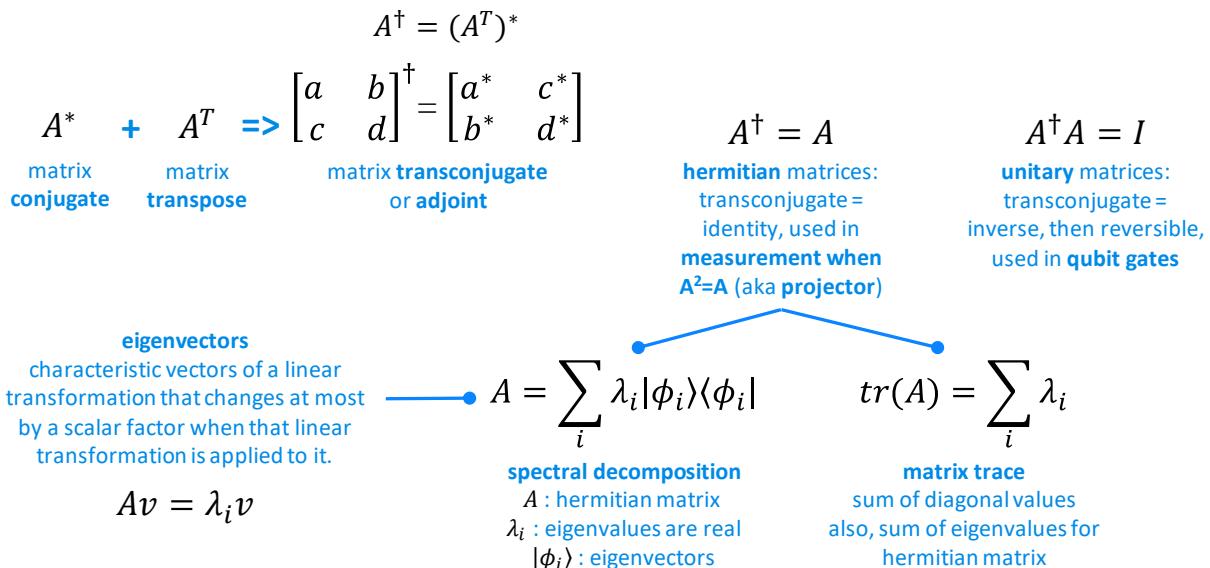
If  $|\psi\rangle$  is a unit vector, the outer product  $|\psi\rangle\langle\psi|$  is a projector that can project any vector  $|\phi\rangle$  on  $|\psi\rangle$ .

Notation	Description
$z^*$	Complex conjugate of the complex number $z$ . $(1+i)^* = 1-i$
$ \psi\rangle$	Vector. Also known as a <i>ket</i> .
$\langle\psi $	Vector dual to $ \psi\rangle$ . Also known as a <i>bra</i> .
$\langle\varphi \psi\rangle$	Inner product between the vectors $ \varphi\rangle$ and $ \psi\rangle$ .
$ \varphi\rangle \otimes  \psi\rangle$	Tensor product of $ \varphi\rangle$ and $ \psi\rangle$ .
$ \varphi\rangle \psi\rangle$	Abbreviated notation for tensor product of $ \varphi\rangle$ and $ \psi\rangle$ .
$A^*$	Complex conjugate of the $A$ matrix.
$A^T$	Transpose of the $A$ matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the $A$ matrix, $A^\dagger = (A^T)^*$ . $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}.$
$\langle\varphi A \psi\rangle$	Inner product between $ \varphi\rangle$ and $A \psi\rangle$ . Equivalently, inner product between $A^\dagger \varphi\rangle$ and $ \psi\rangle$ .

Indeed,  $(|\psi\rangle\langle\psi|)|\phi\rangle = |\psi\rangle(\langle\psi||\phi\rangle) = (\langle\psi|\phi\rangle)|\psi\rangle$ , given  $\langle\psi|\phi\rangle$  is a real number being the inner product of both vectors. Some of these elements are summarized in the table above<sup>196</sup>.

- **Unitary matrices** are square matrices whose inverse equals their transconjugate ( $A^\dagger = A$ ). A unitary matrix has several properties, one of which is to have orthogonal eigenvectors and to be diagonalizable. Unitary matrices define the reversible gates applied to qubits or sets of qubits.

A unitary operation is the application of a unitary matrix to a computational state vector that we'll later see. Quantum computing reversibility comes from this unitary property. A unitary matrix  $U$  can also be expressed as  $U = e^{iH}$ , with  $H$  being a Hermitian matrix, but finding  $H$  given  $U$  is a complicated calculation problem.



<sup>196</sup> It is from [Quantum Computation and Quantum Information](#) by Nielsen and Chuang, 2010 (10th edition, 704 pages).

## Pure and mixed states

Let's now explain what are the three main states of quantum objects, basis, pure and mixed given we'll stick to their qubits implementations, given these notions are valid with any quantum object. We are dealing with mathematical models that describe quantum objects states.

	basis states	pure states	mixed states
definitions	aka computational basis states, are N dimensions vectors combining 0s and 1s, with $2^N$ different such vectors for a N qubits register.	vectors in a Hilbert space of norm 1, specified by a single ket describing coherent superpositions of basis states with complex numbers.	or statistical mixture of pure states, are classical statistical ensemble of combination $p_i$ of pure states $\Psi_i$ . $\Psi_i$ can be any combination of pure states but is usually a set of computational basis states.
randomness origin	no randomness with perfect qubits	quantum	quantum and classical
with a single qubit	$ 0\rangle$ and $ 1\rangle$	$ \Psi\rangle = \alpha 0\rangle + \beta 1\rangle$ $ \alpha ^2 +  \beta ^2 = 1$	$p_1 \psi_1\rangle, p_2 \psi_2\rangle$ we don't add them, it's just a statistical ensemble, statistical mixture or convex sum of several systems.
with a N qubits register $i = 1$ to $2^N$	$ i\rangle$ $ 01101011\rangle$ for $N=8$ all $ i\rangle$ form the computational basis states of the N qubits register, contains N combinations of 0 and 1, all basis states are mathematically orthogonal.	$ \Psi\rangle = \sum_i \alpha_i i\rangle$ $\sum_i \alpha_i^2 = 1$ $\alpha_i$ = complex number a pure state is a linear superposition of computational basis states.	$\{(p_i \Psi_i\rangle\}$ ensemble notation $\sum_i p_i = 1$ $p_i$ = positive real number probability to find $\Psi_i$ in the mixed state given all $p_i$ are 0 or a 1 in a pure state.

(cc) Olivier Ezratty, September 2021

**Basis states** correspond to given combinations of 0 and 1 values in a qubits register. For a single qubit, these are the states  $|0\rangle$  and  $|1\rangle$ . For a register of N qubits, it is one of the  $2^N$  different basis states combinations of 0s and 1s, or a tensor product of N single qubit basis states. It constitutes the computational basis in a complex numbers Hilbert space of dimension  $2^N$ . The vectors of this basis are all mathematically orthogonal. A basis state is also named a computational basis state. When measuring individual qubits in these states, you get a deterministic result, at least with theoretically perfect qubits.

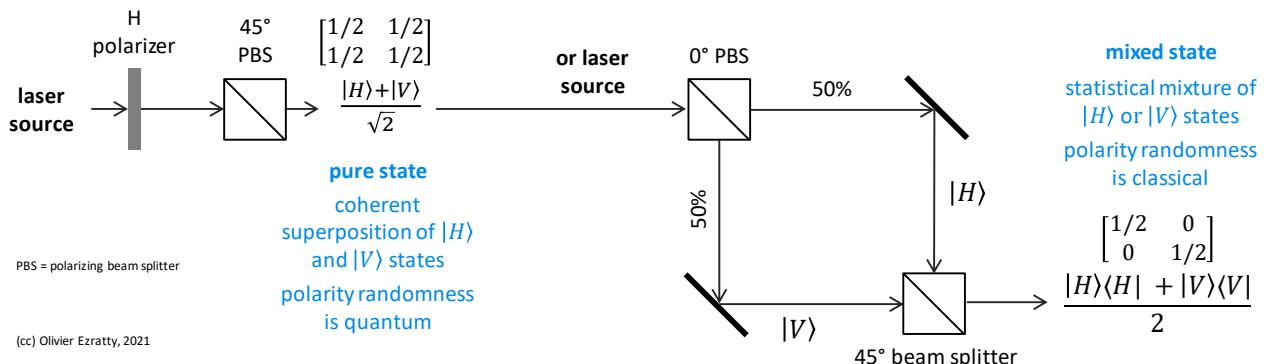
**Pure states** describe the state of an isolated quantum system of one or several objects as a linear superposition of the states from its computational basis. It's a vector in a Hilbert space. That's when superposition and entanglement come in. With massive particles, basis and pure states are solutions to Schrödinger's equation. It's applicable to one or several quantum objects or qubits. During computation, a qubit register is theoretically in a pure state, but quantum decoherence will gradually turn it into a mixed state. A pure state is also presented as a quantum state where we have exact information about the quantum system. This information corresponds to the famous  $\psi$  vector in the Hilbert space. When preparing a quantum state, we indeed know the parameters of the vector  $\psi$  even though actual property measurements will generate random results if the quantum state is not measured along with one of its eigenstates. The information we have about measurement potential results is their probabilistic distribution.

**Mixed states** are weird beasts. Literally, these are “statistical ensembles of classical probabilistic combinations of pure states”, these being usually computational basis states, but they can also be expressed as real number linear combinations of any pure states. Basis states and pure states describe the information available for a single quantum object or qubit, or a group of such objects. A mixed state describes a large number of such systems, prepared in a similar manner, and the states they could be in when repeating an experiment followed by some measurement.

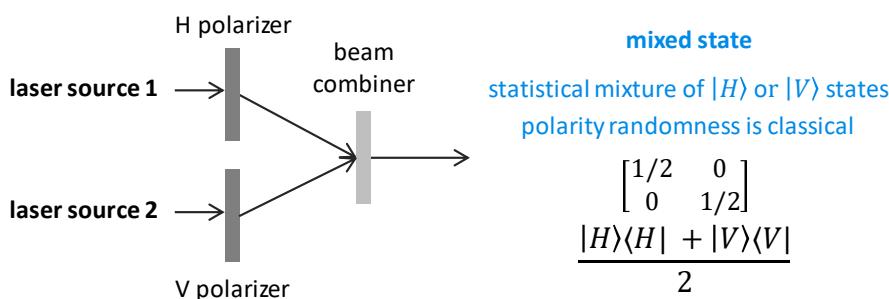
However, a pure state measurement generating random results most of the time, we still also experimentally prepare and measure it on a repeated basis to have an idea of its state probability distribution. In the end, both pure states and mixed states describe the information we can extract from a system after doing repeated experiments and measurements. Their difference lies with the origin of measurement randomness. Its origin is entirely quantum for pure states and both quantum and classical (or “non-quantum”) for mixed states. Got it? If not, we have a couple practical examples below to figure out what it looks like in the real world!

Typically, mixed states provide the available information describing two sorts of systems:

**Random quantum objects** like photons coming from an unpolarized photons source, or, when photons with different polarities are merged like in the below illustration on the right. The photon polarization at this point is a statistical mixture of horizontal and vertical polarization photons. Let's say this is the case where quantum objects that are prepared differently and are then mixed together. The two sources are not “coherently” prepared. In the example in the left, a  $45^\circ$  polarizing beam splitter applied to horizontalized prepared photons produces superposed H and V photons in a pure state. On the right, the polarizing beam splitter creates 50% vertically and 50% horizontally polarized photons that can be merged by a  $45^\circ$  non-polarizing beam splitter. They are statistically merged, but not superposed, thus creating a mixed state.

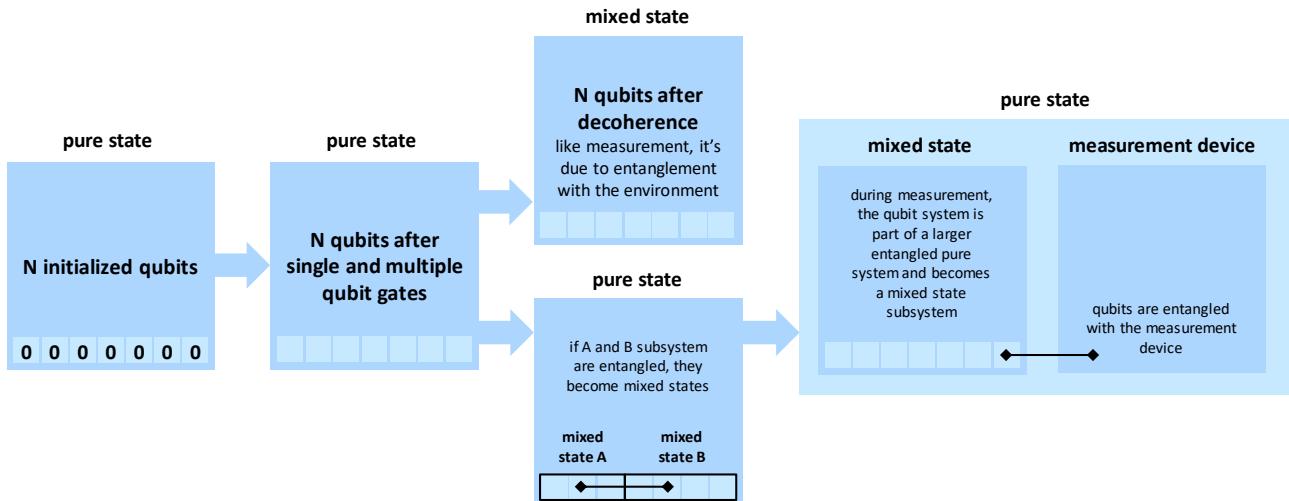


In this other example, two lasers are preparing coherent light that is polarized respectively horizontally and vertically and then merged by a beam combiner. The resulting photons represent a totally mixed state with uncorrelated and incoherent photons. Their statistical distribution is entirely classical with a density matrix void of any off-diagonal values.



**Subsystems** of an inseparable entangled system of several quantum objects. It helps understand what we are measuring at the end of computing when the resulting qubits are still entangled. One particular case is a set of qubits affected by decoherence coming from interactions with the environment. It helps understand the effect of decoherence on the state of a qubits register during computing and how error correction codes are mitigating it. Decoherence comes from the entanglement between a system and its environment, thus, the observed system is not yet isolated and becomes a subsystem of a larger entangled system. Thus, it becomes a mixed state. Want to grasp it clearly? You need to toy with density matrices representations of these pure and mixed states.

Note that these concepts are applicable to both a single qubit and a register of N qubits.



## Density matrices

Density matrices, also named density operators, were introduced in 1927 by **John von Neumann** and **Lev Landau** and later expanded by **Felix Bloch**. Von Neumann created this formalism to develop his theory of quantum measurements.

A density matrix is a mathematical tool used to describe quantum systems in pure or mixed states. Compared to the state vector that we saw earlier, a density matrix is the only way to mathematically describe a mixed state. It consolidates all the physically significant information that could be retrieved from a set of quantum objects given what we know about them. Quantum and classical probabilities are boiled in the density matrix.

Usually represented by the sign  $\rho$  (rho), a density matrix is a square matrix of complex numbers used to describe a quantum system, like a register of several qubits. Its size is  $2^N \times 2^N$  where  $N$  is the number of qubits in the register.

The density matrix of a quantum register in **pure state** is the outer product of its computational basis state vector  $|\Psi\rangle\langle\Psi|$  as described below, with an example using a Bell pair of two qubits. There is no more information in the density matrix than in the basis state vector at this stage.

A density matrix for a **mixed state** adds several pure states matrices with real probability coefficients  $p_i$ . The  $|\Psi_i\rangle$  pure states that are combined to form a mixed state can be themselves states from the computational basis (combination of 0s and 1s) but not necessarily. They can be any vector in the  $2^N$  Hilbert space, and made of (normalized) linear superpositions of these basis states. Mathematically speaking, a pure state density matrix is a special case of mixed state density matrix where only one  $p_i$  is not zero.

We'll repeat here what was said with pure and mixed states: a mixed state density matrix consolidates both **quantum uncertainties** (that persists even when the system state is well known) and **classical uncertainties** (due to a lack of knowledge of individual quantum sources and preparation conditions) when a pure state density matrix contains only information pertaining to **quantum uncertainties**.

pure state vector

$$|\Psi\rangle = \sum_i \alpha_i |i\rangle$$

 $n = 2^N$  for N qubits

pure state outer product

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} [\alpha_1^* \ \cdots \ \alpha_N^*]$$

pure state density matrix

$$\begin{bmatrix} |\alpha_1|^2 & \cdots & \alpha_i \alpha_j^* \\ \vdots & \ddots & \vdots \\ \alpha_i^* \alpha_j & \cdots & |\alpha_n|^2 \end{bmatrix}$$

$|\psi\rangle$  pure state vector example with a **Bell pair** assembling linearly two computational basis state vectors  $|00\rangle$  et  $|11\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(1,0,0,1)^T$$

state vector in a  $n=2^2$  dimensions Hilbert space

the **Bell pair** density matrix is the outer product of the state vector  $|\psi\rangle$

$$|\psi\rangle\langle\psi| = \frac{1}{\sqrt{2}}(1,0,0,1)^T \frac{1}{\sqrt{2}}(1,0,0,1) = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix}$$

transpose vector      correlations between  $|00\rangle$  and  $|11\rangle$

the diagonal contains the computational basis vector  $|\psi\rangle$

(cc) Olivier Ezratty, 2021

A density matrix has several mathematical properties as described *below* and detailed afterwards with some differences between pure and mixed states density matrices.

density matrix characteristics	pure states	mixed states		a density matrix or density operator is the most generic way to represent mixed and pure states, it's a linear combination of pure states outer products multiplied by their positive real number classical probability. For a N qubits register, it's a $2^N$ rows and columns square matrix.
its eigenvalues are all 0 and a 1	$\rho =  \Psi\rangle\langle\Psi $	$\rho = \sum_i p_i  \Psi_i\rangle\langle\Psi_i $	diagonal contains positive real values	
normalization	$\text{tr}(\rho) = 1$			
positivity	$\rho \geq 0$	$ \rho_{ij} ^2 \leq \rho_{ii}\rho_{jj}$		
hermicity	$\rho = \rho^\dagger$		diagonalizable with positive eigenvalues	
projector	$\rho = \rho^2$			
state purity	$\text{tr}(\rho^2) = 1$	$\frac{1}{N} \leq \text{tr}(\rho^2) < 1$		
		completely mixed state maximum entropy*		* : Von Neumann entropy level of uncertainty with the state of qubits or subsystem of qubits
			pure state minimum entropy*	$S(\rho) = -\text{tr}(\rho \log \rho)$

(cc) Olivier Ezratty, May 2021

**Hermicity**. A density matrix is Hermitian, meaning that it's equal to its transconjugate matrix. As a consequence, the density matrix can be diagonalized in a different basis, with positive real number eigenvalues.

Hermicity comes from the density matrix construction: it's real number linear sum of Hermitian matrices resulting from the Hermitian inner product of pure states vectors. One consequence is that it removes any global phase from the quantum system it describes. You can easily understand it by evaluating on your own a density matrix of a given qubit and its global phase.

**Positivity**. A density matrix  $M$  is positive semi-definite, meaning that  $\langle x|M|x\rangle \geq 0$  for all  $x$  vectors. It's also defined as a symmetric matrix with non-negative eigenvalues (meaning... positive or zero). These eigenvalues being the values in the diagonal after matrix diagonalization. But even before diagonalization, all density matrices diagonal values are positive due to hermicity and the way they are constructed as positive probabilities combinations of outer products of pure states whose diagonal are always containing positive values.

**Normalization.** A density matrix trace equals 1 for both pure and mixed states. A density operator is said to be “*normalized to unit trace*”. That’s the sum of its diagonal values which are all positive real numbers. It comes from two rules: Born’s rule applied to a pure state ( $\sum_i \alpha_i^2 = 1$ ) and classical probabilities rules applied to the mixed state ( $\sum_i p_i = 1$ ). As a result, a density matrix diagonal value at position  $j = \sum_i p_i \alpha_{ij}^2$ ,  $\alpha_{ij}$  being the weight  $\alpha_j$  from the pure state  $i$  composing the mixed state. The diagonal is also referred to as a statistical mixture or as a population.

There are some differences between pure and mixed states density matrices.

**Projector.** A pure state density matrix is a projector, i.e. equal to its square and the trace of its square density matrix  $\rho^2$  is equal to 1. Being a projector means that its eigenvalues are all zeros except a single one that is 1. The eigenvector associated with the eigenvalue one is the state vector of the system. Being a projector means the density matrix can be used as the way to measure a quantum state using this vector as a basis reference. In a single qubit system and the Bloch sphere, it would be any vector in the sphere and the related measurement observable, a geometrical projection of the evaluated qubit on this vector. In the case of a mixed state, the density matrix trace is inferior to 1 and its minimum is  $1/N$ , when the state is maximally mixed with equal probabilities for all basis values. The average value obtained with applying an observable  $A$  to a pure state quantum system state vector  $\psi$  is evaluated with the formula  $\langle \psi | A | \psi \rangle$ , also named an expectation value. In other words, it’s the dot vector product of  $\psi$  and the vector obtained by applying matrix  $A$  to vector  $\psi$ . The expectation value of a mixed state represented by a density matrix  $\rho$  is  $tr(\rho A)$ , a trace of the density matrix multiplied by the observable  $A$  matrix.

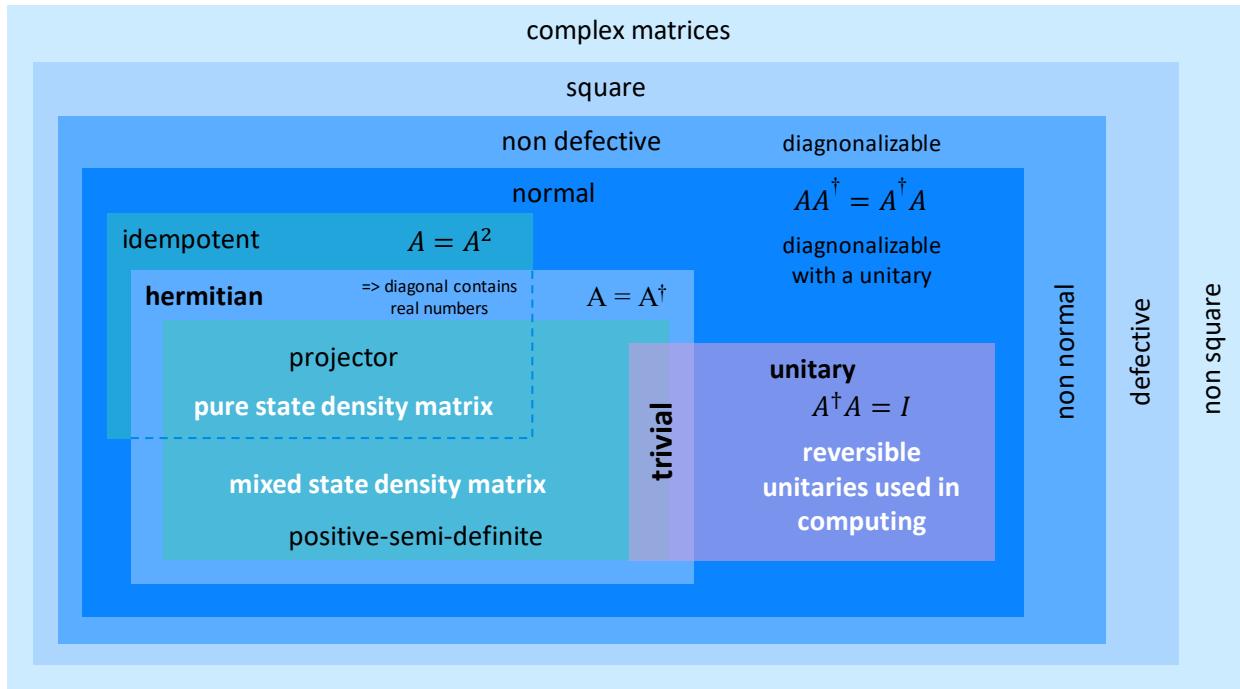
**Off-diagonal elements** can have a time-dependent phase that will describe the evolution of coherent superpositions. These elements are also named “coherences”. As decoherence starts due to interactions with the environment, any pure state will progressively turn into a mixed state and the off-diagonal values will be affected. This evolution follows the Liouville–von Neumann equation.

$$\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{|+\rangle\langle +| + |-\rangle\langle -|}{2} = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} = \frac{1}{2} \mathbb{I}$$

**Combinations.** A mixed state can be the result of an infinite number of combinations of pure states, the most common example being, for two qubits, the half-identity mixed state being an equally mixed state of both  $|0\rangle$  and  $|1\rangle$  or  $|+\rangle$  and  $|-\rangle$  as described *above*. Given a density matrix, you can’t compute the pure states that were combined to create it. Said otherwise, quantum states with the same density matrix can’t be distinguished operationally (i.e. by a set of measurements). Also, when a unitary operation  $U$  (defined later, sorry) is applied to a mixed state defined by its density matrix  $\rho$ , the resulting state density matrix is  $U\rho U^\dagger$ .

For the fun of a better understanding, I’ve added *below* a graphical segmentation of all the various matrices types we’ve been mentioning in the previous pages and how they are related with each other.

We forgot to define a **non-defective matrix**, which is a diagonalizable matrix. And a normal matrix  $A$  verifies  $AA^\dagger = A^\dagger A$ . A **trivial** matrix is both Hermitian and unitary and have orthonormal eigenvectors with eigenvalues being +1 or -1.



(cc) Olivier Ezratty, August 2021

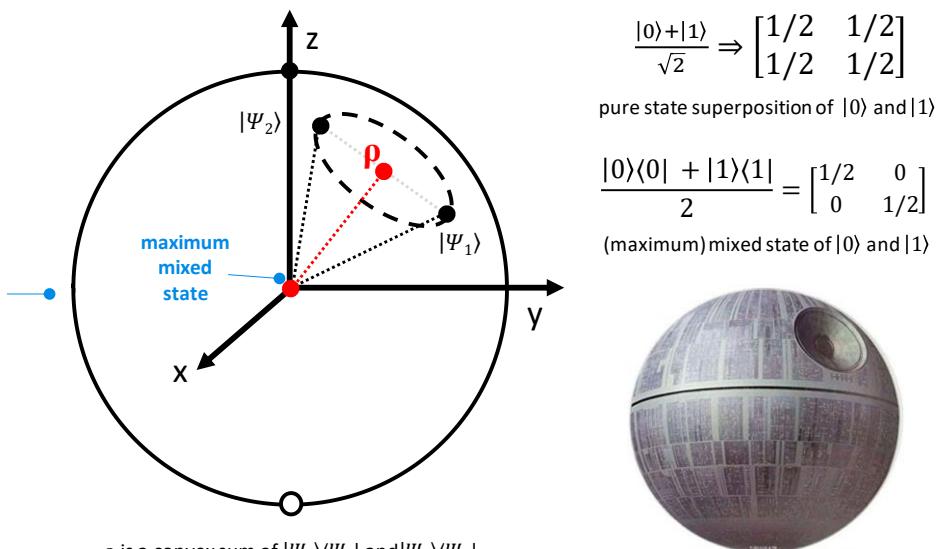
**Single qubit mixed states** can be represented by a point inside the Bloch sphere as shown below in a “Death Star” representation, with a statistical mixture of two pure qubit states. The mixed state is a convex sum of pure states inner products, ‘convex’ meaning it’s a sum using positive real coefficients that sum up to 1. The geometric representation is a good way to figure out why a given mixed state can result from an infinite number of combinations of two pure states. We can combine more than two pure states to create a mixed state. By the way, the Bloch sphere becomes a Bloch ball.

a single qubit mixed state can be represented by points inside the Bloch sphere with 3 degrees of freedom: its two usual angles and the vector length.

a **maximum mixed state** is at the center of the Bloch sphere with equiprobability of  $|0\rangle$  and  $|1\rangle$ .

a mixed state can result from an infinite number of **combinations** of various pure states as shown in the sphere.

the **state purity** is measured by its proximity to the Bloch sphere surface.



(cc) Olivier Ezratty, 2021

$p$  is a convex sum of  $|\Psi_1\rangle\langle\Psi_1|$  and  $|\Psi_2\rangle\langle\Psi_2|$

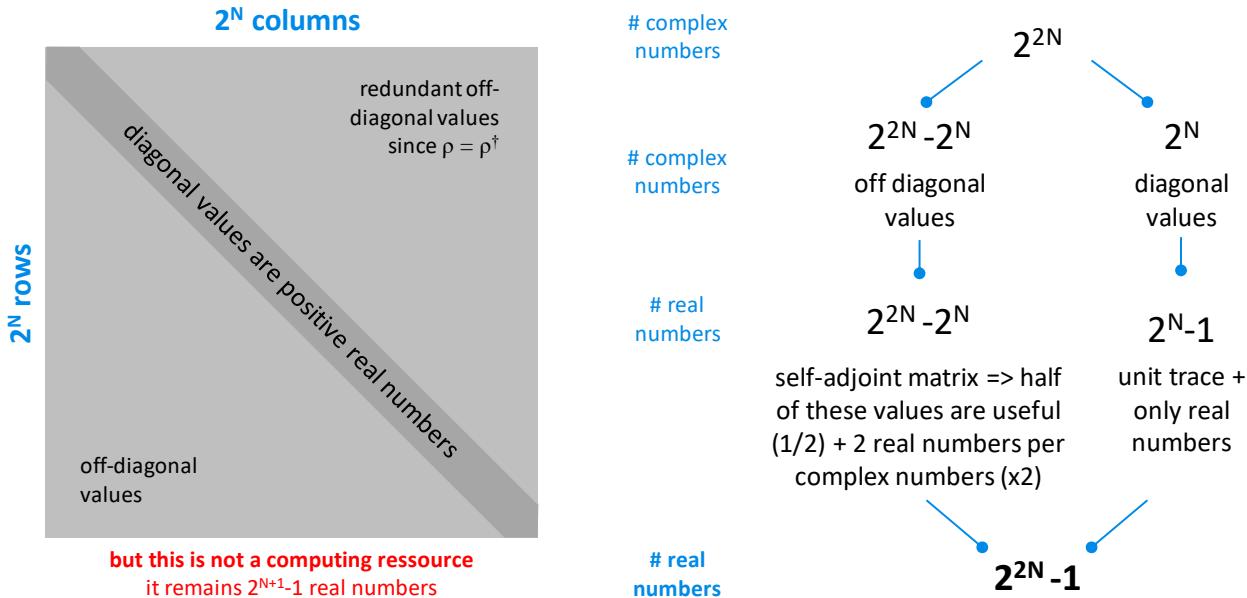


**Density matrix dimensionality.** Although it contains  $2^{2N}$  complex values, due to normalization, the dimensionality of a density matrix is  $2^{2N}-1$  real numbers. The explanation is reconstructed below. For a starter, we have  $2^{2N}$  complex values which is the square or  $2^N$ , the number of lines and columns in the density matrix. We separate the matrix diagonal from the off-diagonal values. The diagonal values are real numbers because they are the positive probability sums of the diagonal values of pure states density matrices, themselves being positive as  $|\alpha_i|^2$ .

The matrix trace equals 1, removing another useful dimension. The off-diagonal values are redundant since the matrix is equal to its transadjoint. So we divide by two their dimensionality. Since

these are complex numbers, we multiply it by two to get a number of real numbers. When summing this up, we find  $2^{2N}-1$  different real numbers.

This dimensionality is usually presented as  $2^{2N-1}$  complex numbers or  $2^{2N}$  real numbers, avoiding the minus 1 which is quickly negligible as N grows.



However, this dimensionality does not correspond to some useful computing resource in standard gate-based programming models although some work has been done to exploit it, but with no additional computing acceleration<sup>197</sup>. A theoretical perfect gate-based quantum computer is using qubits registers that are in a pure state until measurement, representing thus a dimensionality of  $2^{N+1}-1$  real numbers, the -1 standing for the normalization constraint of the computational basis vector<sup>198</sup>. So why do we care about these density matrices for mixed states? These are mostly used to understand the effects of decoherence and measurement and with qubits registers tomography which helps determine their fidelities.

The sequence of quantum gates in a quantum circuits can also be represented by a large unitary matrix of dimension  $2^N * 2^N = 2^{2N}$  complex numbers. So, with a dimensionality close to a density matrix. But this is not an actual computing resource. It deals more with the extensive computing resources required to emulate in-memory an entire unitary algorithm in a classical computer instead of just executing gates one by one on the computational state vector.

There are many other subtleties with density matrices that we can't detail in the ebook. For example:

**Diagonalization** is possible for any mixed state density matrix. It will decompose the state into classical probabilistic combination of pure states eigenvectors forming an orthonormal basis.

**Reduced density matrices** are the density matrices of subsystems of composite systems. The reduced density matrix for an entangled pure state is a mixed state or mixed ensemble.

<sup>197</sup> See [Quantum Circuits with Mixed States](#) by Dorit Aharonov, Alexis Kitaev and Noam Nissam, 1998 (20 pages). It describes a model using not only unitary matrix operator-based quantum gates. It enables the usage of subroutines in programming. But this programming model doesn't seem adopted so far except for quantum error correction codes which implement measurement during computing. Mixed states based programming is implemented in the qGCL extension of the language pGCL as described in [Quantum programming with mixed states](#) by Paolo Zuliani, 2005 (14 pages).

<sup>198</sup> Thus, wrong is the statement that "A calculation using n number of qubits on a quantum computer would need  $2^n$  classical bits on a standard computer" as seen in [Simulating subatomic physics on a quantum computer](#) by Sarah Charley, October 2020. Why? Because one of the  $2^N$  quantum amplitudes in a N qubit register cannot be stored or emulated on a single bit!

**Mixed state purification** consists, inversely, in integrating a mixed state in a larger system to create or reconstruct a pure state. It is used in some error-correcting codes.

**Bipartite pure states** are tensor products of two systems that are not entangled. A pure state system is entangled if and only if some of its reduced states are mixed rather than pure. If all were pure, it would mean that the pure state density matrix  $\rho$  would be separable into several pure states, one for each qubit in the case of a qubits register.

**Schmidt decompositions** are used to decompose bipartite systems and evaluate their level of entanglement. This level of entanglement can be determined with the Schmidt coefficients coming from the Schmidt decomposition.

**Matrix rank.** A matrix rank is the number of non-zero values in its diagonalized version. The rank of a density matrix gives an indication of the purity of the state it represents. A pure state density matrix has a rank 1, since it can be diagonalized into a matrix where only one value in the diagonal is non-zero. A maximally mixed state has a rank of  $2^N$ , i.e. the number of lines and columns in the density matrix representing N qubits.

**Schmidt rank** is an indication of the level of entanglement in a density matrix. Not to be confused with the matrix rank which deals with its purity level.

**Quantum Channels** are transformations of a quantum state resulting from any kind of interaction with a quantum environment. They are modelized with an operator, called a superoperator, transforming a density matrix into another density matrix. Technically speaking, a superoperator is a completely positive (we've defined that already) and trace-preserving operator (self-explainable), or CPTP. Its form is a linear map from one Hilbert space to another Hilbert space. Its dimension is a square matrix with  $2^{2N}$  columns and as many rows, so with  $2^{4N}$  (or  $16^N$ ) complex numbers, before normalization, N being the number of qubits. It is useful to modelize quantum subsystems (which are in mixed state), decoherence, quantum error correction and qubits noise<sup>199</sup>. It is even possible to build a tomography with a superoperator, aka a quantum process tomography (QPT). One for example can build a QPT of a quantum gate to detect its imperfections. A QPT can also be done for a more complex operation, or unitary applied to a set of qubits, like a Quantum Fourier Transform<sup>200</sup>.

## Grad, curls and divs

In the equations of Maxwell, Schrödinger, Dirac and others that we have seen are used notations good to remember here around the symbol nabla :  $\nabla$ , sometimes used with an arrow  $\vec{\nabla}$ .

Nabla generally designates the gradient of a scalar or vector function, i.e. its first derivative. A scalar function applies to a vector, often of three dimensions x, y and z of a Euclidean space. It returns a number. A vector function returns a vector! This leads to the notions of **gradient** and **Laplacian** which apply to a scalar function and correspond to first and second derivatives in space, and to divergence and rotational (or curl) which apply to a vector function. A Laplacian can also be applied to a vector function. We won't go far in this ebook with respect to these functions.

$\nabla = \left( \frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z} \right)$	$\nabla f = \left( \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z} \right)$	$\nabla \cdot \vec{G} = \left( \frac{\partial G_x}{\partial x}, \frac{\partial G_y}{\partial y}, \frac{\partial G_z}{\partial z} \right)$	$\nabla \times \vec{G} = \left( \frac{\partial G_z}{\partial y} - \frac{\partial G_y}{\partial z}, \frac{\partial G_x}{\partial z} - \frac{\partial G_z}{\partial x}, \frac{\partial G_y}{\partial x} - \frac{\partial G_x}{\partial y} \right)$
del or nabla operator, first space derivative of a vector	scalar function gradient, scalar field vector of space variations	vector function divergence, showing its local evolution	rotational or curl of a vector function G transforming a vector field in a vector field describing the field variation in space

<sup>199</sup> See [Quantum Channels](#) by Stéphane Attal (65 pages).

<sup>200</sup> See [Quantum Process Tomography of the Quantum Fourier Transform](#) by Yaakov S. Weinstein, Seth Lloyd et al, 2004 (45 pages).

$$\nabla^2 f = \nabla \cdot \nabla f = \left( \frac{\partial^2 f}{\partial x^2}, \frac{\partial^2 f}{\partial y^2}, \frac{\partial^2 f}{\partial z^2} \right)$$

scalar function laplacian

$$\nabla^2 \vec{G} = \left( \frac{\partial^2 G_x}{\partial x^2} + \frac{\partial^2 G_x}{\partial y^2} + \frac{\partial^2 G_x}{\partial z^2}, \frac{\partial^2 G_y}{\partial x^2} + \frac{\partial^2 G_y}{\partial y^2} + \frac{\partial^2 G_y}{\partial z^2}, \frac{\partial^2 G_z}{\partial x^2} + \frac{\partial^2 G_z}{\partial y^2} + \frac{\partial^2 G_z}{\partial z^2} \right)$$

vector function laplacian

## Permanent and determinant

This inventory would not be complete without describing an even stranger mathematical object: the **permanent** of a square **matrix**  $n \times n$ , invented by Louis Cauchy in 1812.

$$\text{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n a_{i,\sigma(i)}$$

The *above* formula describes its content. The  $\Pi$  denotes a multiplication of values from the index matrix  $i$  and  $\sigma(i)$ .  $\sigma$  is a permutation function of integers between 1 and  $n$ , the dimension of the matrix (number of columns and rows). The sigma relates to the set of  $\sigma$  functions of the permutation group  $S_n$  (also called symmetrical group) which has a size of  $n!$  (factorial of  $n$ ). The values  $a_{i,\sigma(i)}$  are the cells of the coordinate matrix  $i$  and  $\sigma(i)$ .

Here is what it gives with  $n=2$  and  $n=3$  knowing that beyond that, it becomes less readable:

$$\text{perm} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad + bc \quad \text{perm} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh + ceg + bdi + afh$$

The permanent is therefore a real number resulting from  $n!$  (factorial of  $n$ ) additions of multiplications of  $n$  values of the matrix. The permanents are notably used to evaluate matrices that represent graphs.

They are also used in the classical numerical simulation of boson sampling that we will describe in the section dedicated to [photon qubits](#), page 332<sup>201</sup>. Contrary to the calculation of the determinant, *below*, which can be simplified, that of the permanent remains a classical intractable problem.

The **determinant of a matrix** is a variant of its permanent (*opposite*).  $\text{sgn}(\sigma)$  is the sign of permutations, which is +1 if the number of permutations needed to create the permutation is even and -1 if it is odd. Olé!

$$\det(A) = \sum_{\sigma \in S_n} \left( \text{sgn}(\sigma) \prod_{i=1}^n a_{i,\sigma(i)} \right)$$

And this is what it gives for  $n=3$ . Note that the group of permutations includes the permutation that does not change the order of the elements.

$$\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh - ceg - bdi - afh$$

Determinants have particular properties such as  $\det(AB)=\det(A).\det(B)=\det(B).\det(A)=\det(BA)$  which can facilitate the calculation of the determinant of a matrix if it can be factorized into several matrices. Also, the determinant of a matrix is the product of its eigenvalues.

So much for the definition of the basics of the linear algebra of quantum computing. I've skipped a lot of other definitions and rules of computation. It was a question of clarifying certain notions that are frequently used in the scientific literature on quantum computing and in many of the reference works cited in this ebook. What we have just seen may be useful for you to compare some of the scientific literature on quantum computing.

---

<sup>201</sup> The calculation time of a permanent increases faster than an exponential of a fixed value ( $Mn$ ) as soon as  $n$  becomes very large compared to  $M$ . So, for example, with  $M=2$ ,  $2n$  is much smaller than  $n!$  as soon as  $n$  is greater than 4. As the numerical simulation of the boson requires a determinant that depends on the size of the simulation, it is even more cumbersome to compute than an exponential problem.

If you like maths, linear algebra and complexity, you can have some fun exploring type III factors algebra that describes the observables in relativistic quantum fields theory<sup>202</sup>! Classical quantum physics and computing is based on a simplistic type I factors algebra. Simpler, but still complicated.

## Fourier transforms

Since quantum physics deals a lot with wave-particle duality and particularly with waves, waves signals decomposition is a key mathematical tool. That's the role of a Fourier transform that we mentioned already when dealing with Heisenberg's indeterminacy principle.

The Fourier Transform implements a mathematical decomposition of a function  $f(x)$  into a function  $\hat{f}(\xi)$  returning a complex number containing an amplitude and phase for single frequencies  $\xi$ . It's a more generic version of Fourier series which work with periodic signals. Fourier transform are Fourier series where the signal period can approach infinite. It can be used for example to decompose a wavepacket pulse signal that is concentrated in time.

Usually, a Fourier transform operates in the time domain and  $x$  is a time in second while  $\xi$  is a frequency in Hertz.

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx$$

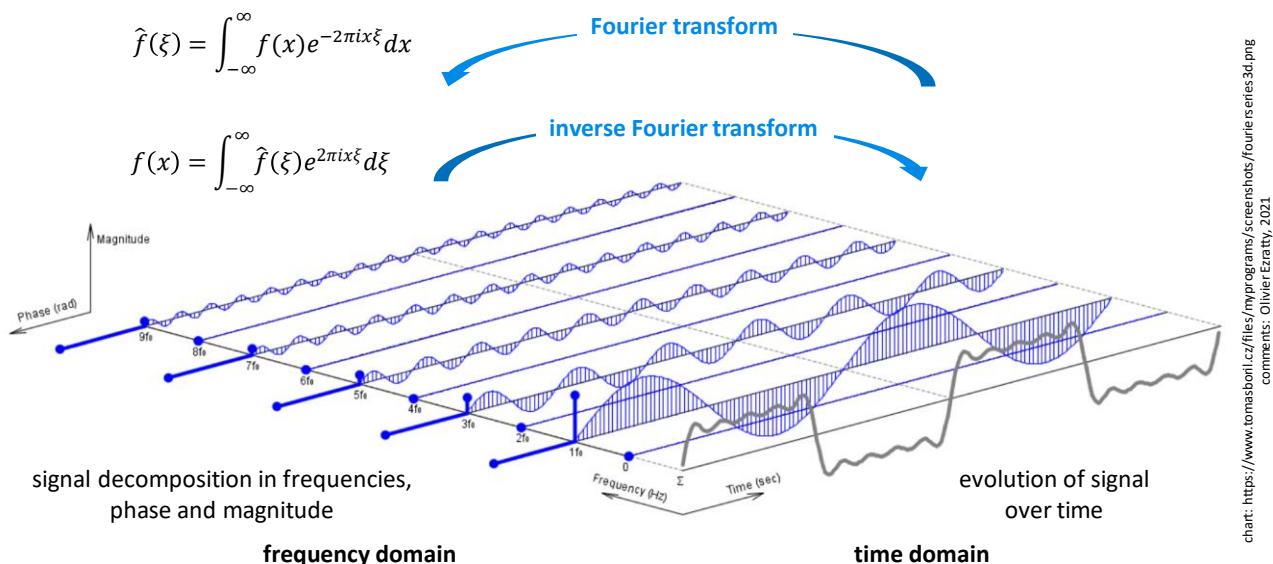
It can be decomposed using Euler's formula in its real and complex parts separating the amplitude and phase of the Fourier transformed signal:

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) \cos(2\pi x \xi) dx - i \int_{-\infty}^{\infty} f(x) \sin(2\pi x \xi) dx$$

The inverse Fourier transforms that frequency decomposition function  $\hat{f}(\xi)$  back into its original compound time domain signal  $f(x)$ .

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi) e^{2\pi i x \xi} d\xi$$

All of this is easier to understand with examples like in the schema below decomposing a time domain signal into five frequencies constituents with their respective magnitude and (equal) phases.



Computing Fourier series and transforms is done in many ways:

<sup>202</sup> See [The Role of Type III Factors in Quantum Field Theory](#) by Jakob Yngvason, 2004 (15 pages).

**Discrete-time Fourier Transform** (DTFT) is a form of Fourier analysis that is applicable to a sequence of values. It is often used to analyze samples of a continuous function. The term discrete-time refers to the fact that the transform operates on discrete data, often samples whose interval has some units of time.

**Discrete Fourier Transform** (DFT) converts a finite sequence of equally-spaced samples of the function into a same-length sequence of equally-spaced samples of the Discrete-Time Fourier transform (DTFT). The samples are complex numbers coming from a DTFT.

**Fast Fourier Transform** (FFT) computes the discrete Fourier transform (DFT) of a sequence, or its inverse (IDFT). It's an efficient variation of the DFT.

**Quantum Fourier Transform** (QFT) is a linear transformation applied on qubits. It is the quantum analogue of the DFT and reverse DFT. A QFT is a Discrete Fourier Transform applied to the data stored in the  $2^n$  computational basis states of a  $n$  qubits register. The Quantum Fourier Transform, implements a DFT on the complex amplitudes of a quantum state. We cover it [later](#).

Fourier series were created by **Joseph Fourier** (1768-1830, French) as part of his work in the book “The Analytical Theory of Heat” published in 1822. Beforehand, he accompanied Napoleon Bonaparte in his 1798-1801 Egyptian expedition as a scientific advisor.

He then became a Prefect for the Isère department, based in Grenoble. Afterwards, he also drove the young Jean-François Champollion to get interested in deciphering the Rosetta Stone.

## Qubits

Qubits are the basic elements of data manipulation in quantum computers. They are the quantum equivalents of classical computing bits. With them, we move from a deterministic to a probabilistic world but with the capability to handle more information during computing.

In conventional computing, bits used in processing units like microprocessors correspond to circulating electrical charges that reflect the passage or absence of an electrical current. A classical bit has a value of 1 if the current is flowing or 0 if the current is not flowing. The logic is transistors based. A bit readout gives 1 or 0 and deterministically, i.e. if the read operation is repeated several times, or the read operation is repeated after a re-edition of the calculation, it will yield the same result. This is true for data storage of information, for its transport and processing. This is valid modulo the errors that can occur during this journey. These most often occur in storage and memory and are corrected via error correction systems using some data redundancy, usually with some parity bits for each stored byte, so with a rather low data overhead. In data storage, complicated redundancy systems are used like RAID disks organization mixing and matching several disks and parity error codes to take into account the physical errors coming from storage.

In a qubit, everything is different! While qubits are usually initialized at  $|0\rangle$ , operations on them called quantum gates create a mathematical linear superposition between states  $|0\rangle$  and  $|1\rangle$ . These two states correspond to two different discrete possible values of a physical property of a quantum object like an electron spin (up or down in a given direction), a photon polarization or an atom energy level. Qubits are represented mathematically by a vector in a two-dimension Hilbert space which describes its amplitude and phase, reminding us of the “wave” nature of quantum objects.

We'll see later how we use the Bloch sphere geometrical representation to understand how amplitude and phase are visualized. And it gets more complicated when we conditionally connect qubits together using multi-qubits quantum gates implementing quantum entanglement.

At the end of computing, we read the value of a qubit. Like all quantum object measurement, it results in a wavepacket collapse onto one of the two qubit basis states. So, we get a  $|0\rangle$  or a  $|1\rangle$  and the result is probabilistic, not deterministic. The wealth of information handled by a qubit during computing is lost at the end of calculation.

The role of a quantum algorithm is to leverage this wealth of information during computing so that a simple result is generated at the end. We turn this probabilistic outcome in a deterministic one with executing the algorithm a great number of times, up to thousands times, and averaging the obtained results. It's also dependent on the structure of quantum algorithms which are designed to generate a result with qubits being as close as possible to their so-called "computational basis states", namely,  $|0\rangle$  and  $|1\rangle$ .

		bits: 0 or 1		qubits: 0 and 1
states	mathematical bit	2 possible exclusive states, 0 or 1	mathematical qubit	linear combination of $ 0\rangle$ and $ 1\rangle$
initialization		0 or 1		$ 0\rangle$ basis state
dimensionality		1 binary digit => two possible values		2 real numbers => one point on Bloch sphere
modifications		logic decision tables, irreversible		reversible unitary transformations
readout		0 ou 1, deterministic		0 or 1, probabilistic
errors		no error, perfect mathematical object		no error, perfect mathematical object
physical implementation	physical bit	current/no current in a logic electronic circuit and two states memory device bit	physical qubit	quantum object with two exclusive states for one property
computing vs memory		separate devices and parts of processors		all done in qubits and with quantum gates
computing operations		transistors based logic		amplitude and phase change + entanglement
errors sources		cosmic rays, transistors leakage		decoherence, thermal, electromagnetic, radioactivity...
error levels		$2.5 \times 10^{-11}$ bit per hour error rate		usually $\gg 0.1\%$ with qubit gates and readout
information redundancy	logical bit	parity bits	logical qubit	large number of physical per logical qubits, $10^2$ to $10^6$
error correction		ECC (memory), MCA (CPU), RAID (storage)		quantum error correction codes
error level after correction		negligible		under an acceptable threshold for fault tolerance

(cc) Olivier Ezratty, September 2021

To sort things out, it's still useful to differentiate three levels of 'qubit objects' used in computing as described in the *above* table:

**Mathematically.** Bits and qubits are idealized mathematical objects that implement a pure mathematical formalism with no errors. What is named a "qubit" is above all a mathematical object. Its dimensionality is different than with a bit. It's represented by two complex numbers, the amplitudes  $\alpha$  and  $\beta$  from the qubit quantum state description  $\alpha|0\rangle + \beta|1\rangle$ . Due to normalization ( $\alpha^2 + \beta^2 = 1$ ) and getting rid of the qubit global phase, its dimensionality becomes two real numbers, usually represented by two angles in the Bloch sphere. Bits and qubit measurement are both mathematical and physical operations. With qubits, it's mathematically based on a projective measurement on the computational basis comprised of  $|0\rangle$  and  $|1\rangle$ , using a Hermitian matrix. Physically, it's using a measurement apparatus operating on the qubit quantum object.

**Physically.** Bits and qubits are implemented with different sorts of physical devices. With bits, we use to say they correspond to currents circulating or not circulating in transistor-based devices. While this is true with processing, this is different with memory and storage<sup>203</sup>. Qubits are implemented with quantum systems comprised of a single quantum object (atom, electron, photon) or several quantum objects (particularly with superconducting qubits and topological matter qubits like Majorana fermions). The  $|0\rangle$  or a  $|1\rangle$  states correspond to two exclusive states for one given property of a quantum object or system, that is clearly separable at measurement, like a photon polarization that is detected with a polarizer and a photon detector or an electron spin that can be detected with some magnetic sensor and a technique called electron spin resonance (ESR). These are also called two-level systems (TLS).

<sup>203</sup> These rely on electronic systems storing information like some magnetic encoding in hard disks drives or with two states transistor-based objects in SRAM (used in processors), DRAM (used around processors) or Flash memory (used in SSD and your usual USB memory key).

Physical qubits processing is using physical operations: **amplitude and phase changes** implemented by single-qubit gates and provoking **superposition** and **entanglement** which conditionally connects qubits together with two or more qubits gates, **interferences** resulting from the previous operations and are at the core of most quantum algorithms, and **quantum measurement** yielding  $|0\rangle$  or  $|1\rangle$  for each qubit when computing has ended or when executing quantum error correction codes. Both bits and qubit physical objects are prone to physical errors. While error rates are very small with classical bits, it's currently quite high with qubits. One simple operation like a two qubits quantum gate can generate over 0,4% error rates, which is unacceptable for most algorithms.

Qubits errors, namely decoherence, come from the various interactions between the qubit quantum objects and their environment like thermal noise, electro-magnetic noise, cosmic rays and gravity<sup>204</sup>. These errors require quantum error correction codes, which, as we'll later see, require a significant overhead of physical qubits.

**Logically.** Error correction is thus required to create usable computing devices. In classical computing and telecommunications, “bits” are corrected with different techniques including using parity bits<sup>205</sup>. Bits are processed, stored and transmitted with a very low-level of errors.

Qubits must be assembled in groups called logical qubits, which are physical assemblies of a much great number of physical qubits, up to 10 000's<sup>206</sup>. Redundancy overhead becomes much bigger than with parity bits used in classical computing. In logical qubits, physical qubits are processed with quantum error correcting codes. The number of physical qubits assembled into logical qubits depends on their physical error rate and on the logical qubit error rate that is expected to enable practical quantum computing. For example, the famous integer factoring Shor algorithm is very demanding since using very precise small angles phase rotation gates.

While qubits are everywhere in quantum computing, these are not the only quantum objects available to manage quantum information.

Quantum computers can also theoretically be built with **qutrits** (with three possible quantum states), **ququarts** (with four possible states) and more generically, with **qudits** ( $d$  being the number of possible quantum states of the qubit underlying quantum system)<sup>207</sup>.

It can deliver some computing power with a smaller number of quantum objects than with qubits. These are still mostly research labs tools. For example, researchers at Berkeley are investigating superconducting qudits with more than two levels<sup>208</sup>. The most common qudits are implemented with photons by managing several of their properties.

Using qudits would have an impact on quantum algorithms design and programming. Most of quantum algorithms are designed for quantum computers using qubit-based gates. However, compilers could probably automatically transform classical quantum gates into qudits-based gates.

---

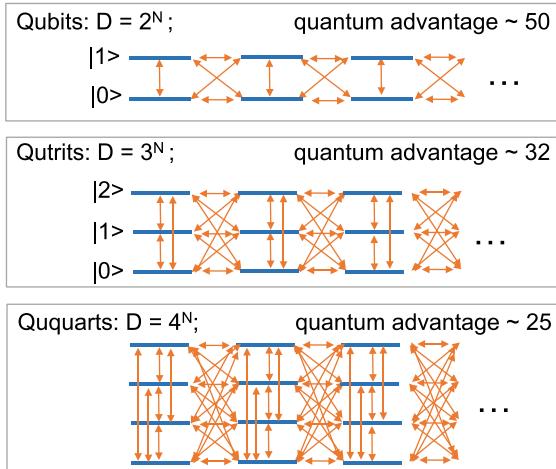
<sup>204</sup> It explains why many qubit types requires some sort of isolation: vacuum and low temperature to avoid thermal and electro-magnetic noise and multi-layered shielding to avoid other sources of electromagnetic noise. But we'll see later that for superconducting and electron spin qubits, the required low temperature is also linked to the microwaves used to control qubits.

<sup>205</sup> ECC (error correcting codes) are used in memories. Some systems are used in processors like the Intel MCA (Machine Check Architecture) which detects and reports errors in microprocessor. Other systems correct errors in storage like RAID redundancy for hard-disk drives and SSDs. We also have error correction codes used in classical telecoms.

<sup>206</sup> As of 2021, there are no commercial computers using real logical qubits. The reason is simple: the number of available physical qubits, topping at 65 with IBM's last generation of superconducting qubits, is still *under* the number of physical qubits required to build just one logical qubit!

<sup>207</sup> See for example [Ultracold polar molecules as qudits](#) by JM Hutson et al, 2020 which deals with qudits using fluorine-calcium and rubidium-cesium diatomic molecules allowing four quantum levels per molecule. This reduces the number of necessary qubits of  $\log_2(d)$ ,  $d$  being the number of state levels of the qubits.

<sup>208</sup> See [Quantum Simulations with Superconducting Qubits](#) by Irfan Siddiqi, 2019 (66 slides) which is the source of the illustration.



The record so far is about creating quvigint, qudits with 20 different exclusive values for photons, that are efficiently measured with state tomography<sup>209</sup>.

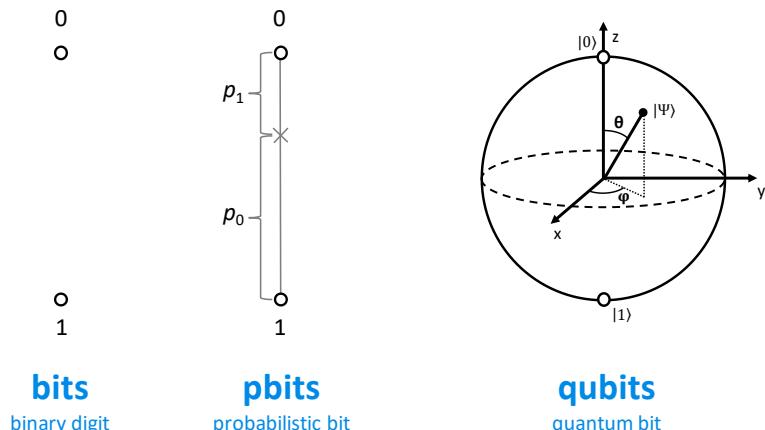
## Bloch sphere

Let's first dig into the mathematical models of qubit representation. These models do not depend on the qubits underlying quantum object types. Physical qubit types have an impact on their error level and types as well as on the low-level quantum gates operations available to control qubits.

In a classical probabilistic model, a probabilistic pbit would have a probability  $p$  of having the value 0 and  $1-p$  of having the value 1<sup>210</sup>. It would be a linear probabilistic model. We cover the niche market of probabilistic computers in a [dedicated section](#), page 436.

Well, with qubits, these probabilistic laws are quite different!

A qubit vector state is defined by two complex numbers  $\alpha$  and  $\beta$  according to the formula describing the qubit quantum object state  $|\Psi\rangle$  as  $\alpha|0\rangle + \beta|1\rangle$ . Quantumly speaking,  $|\Psi\rangle$  is a linear superposition of basis states  $|0\rangle$  and  $|1\rangle$  with coefficients  $\alpha$  and  $\beta$ , aka amplitudes.  $\alpha$  is a complex number whose square describes the probability of having the state  $|0\rangle$  and  $\beta$  is a complex number whose square describes the probability of having the state  $|1\rangle$ .



The sum of the probabilities of the two basis states must give 1. It is indeed not  $\alpha+\beta$  but  $\alpha^2+\beta^2$  that give 1. It comes from the generic probabilistic model developed by **Max Born** in 1926 and from one of the postulates of quantum physics. It gives to the square of the modulus of the wave function of a quantum the meaning of a probability density of the presence of an elementary particle in space (mostly, for electrons).

<sup>209</sup> See [Finding quvigint in a quantum treasure map](#) by University of Queensland, March 2021 and [Robust and Efficient High-Dimensional Quantum State Tomography](#) by Markus Rambach et al, March 2021 (6 pages).

<sup>210</sup> Linear probabilistic models are used in the probabilistic processors discussed in a small [dedicated chapter of this ebook](#).

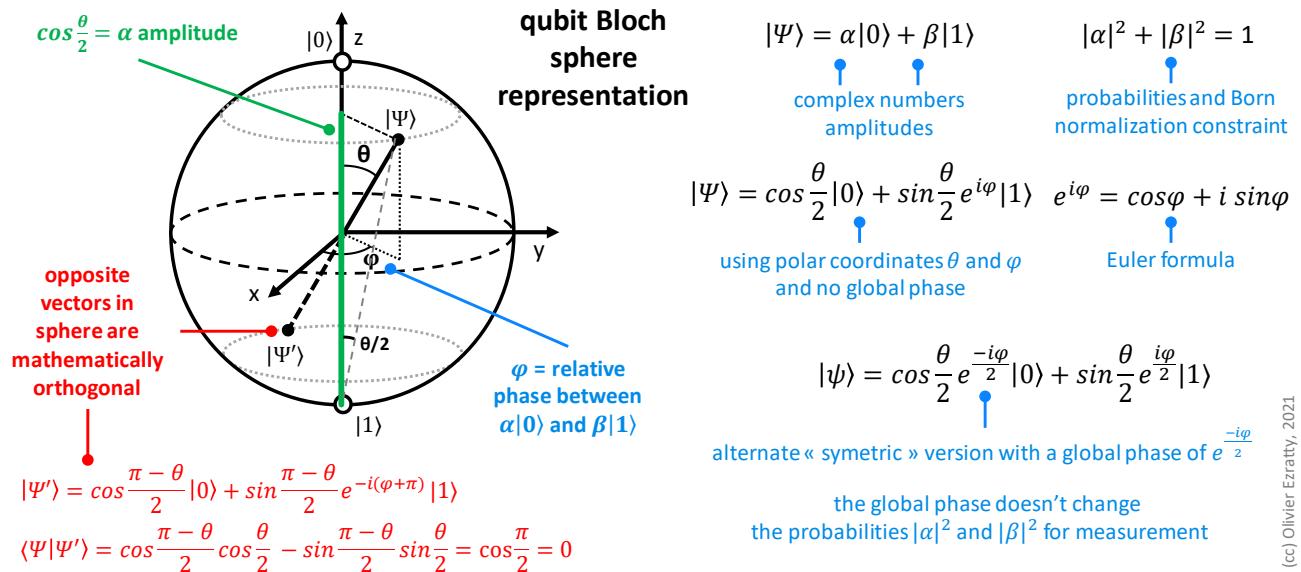
The mathematical representation model of the state of a qubit is based on complex numbers and on the geometrical metaphor of the famous **Bloch sphere**. This model is linked to the representation of the state of a qubit or any two-state quantum by a two-dimensional vector whose length, called "norm", is always 1.

**Angles.** The qubit state  $|0\rangle$  is a length 1 vector going from the center of the sphere to the North pole of the sphere and the state  $|1\rangle$  is a vector going from the center of the sphere to its South pole. An arbitrary qubit state  $|\Psi\rangle$  is represented by a vector with an angle  $\theta$  (0 to  $\pi$ , latitude) with respect to the vertical z-axis and an angle  $\varphi$  (0 to  $2\pi$ , longitude) with respect to the x-axis located from the center of the sphere to its equator and around the z-axis.  $\theta$  corresponds to the qubit amplitude and  $\varphi$  to its phase.

**Orthogonality.** The basis states  $|0\rangle$  and  $|1\rangle$  are opposite in the Bloch sphere and are mathematically orthogonal. This is highly counter-intuitive and linked to the angle  $\theta$  that is divided by two in the formulae. When  $\theta$  equals  $\pi$ , corresponding to a half turn in the sphere, moving from  $|0\rangle$  to  $|1\rangle$ ,  $\cos(\theta/2) = \cos(90^\circ) = 0$  illustrating the fact that  $|0\rangle$  and  $|1\rangle$  are indeed mathematically orthogonal states. This is true for any opposing states within the sphere as with the  $|\Psi\rangle$  and  $|\Psi'\rangle$  examples below. These opposite states are antiparallel or antipodal, meaning parallel but in opposite directions. It explains why angle  $\theta$  is halved in the equations describing a quantum state in Bloch sphere in the sine and cosine calculations of the formulas giving  $\alpha$  and  $\beta$ <sup>211</sup>!

So, we divide  $\theta$  by 2 to link the geometric representation in the sphere with the mathematical representation of the qubit state, and above all, to allow a spreading of all the states of a qubit over the whole sphere. The whole sphere occupation of qubits representations makes it easier to describe how single qubit gates work as we'll show later in a graphical way.

By the way,  $\sin(\theta)$  is a marker of the qubit coherence or level of superposition. It's easy to grasp since the sinus will be equal to zero when the qubit is in the  $|0\rangle$  and  $|1\rangle$  states. It will be maximal, at 1, when the qubit vector will sit on the equator in the Bloch sphere with an even superposition of  $|0\rangle$  and  $|1\rangle$ .

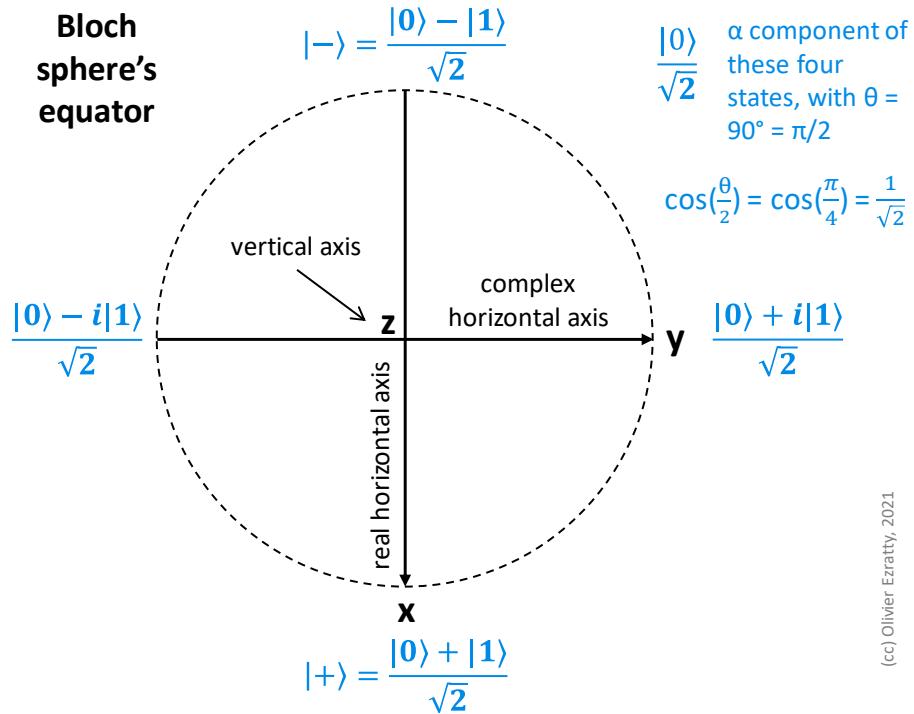


<sup>211</sup> This is deciphered in [Ian Glendinning's The Bloch Sphere](#), 2005 (33 slides) which explains this by the mathematical orthogonality of the two states  $|0\rangle$  and  $|1\rangle$  which are nevertheless opposed in the Bloch sphere. It is even better explained in [Why is theta/2 used for a Bloch sphere instead of theta?](#) which definitely clears up this mystery.

**Global phase.** A qubit representation is usually independent of its global phase. It can be removed from the equation to turn  $\alpha$  into a real number. Still, a qubit is sometimes represented with a global phase of  $\frac{-i\varphi}{2}$  as shown above. When removing the global phase from  $\alpha$ , the complex part of  $\beta$  integrates the phase difference between the amplitudes  $\alpha$  and  $\beta$ . In that case,  $\beta$  is a complex number when the qubit is not in the plane crossing the x-axis ( $\theta = 0$ ) and the z-axis ( $\varphi = 0$ ) of the Bloch sphere, meaning it has a non-zero phase. This complex number associates a real part for the direction z and a complex part for the dimensions x and y which are orthogonal to z. Applying a rotation around the z-axis will generally reintroduce a complex number in the  $\alpha$  of the transformed qubit, which we do not necessarily factorize to remove the global phase of the qubit when doing hand calculations.

**Information.** The paradox to be understood is the following: since there is an infinite number of positions in Bloch's sphere, a single qubit could theoretically store a large amount of information, at least much more than a bit. Let's say it could be two floating point numbers, like the two angles  $\theta$  and  $\varphi$  in the Bloch sphere. Unfortunately, we can only obtain a classical 0 or 1 after measurement because of that damn Holevo theorem<sup>212</sup>! We could theoretically retrieve some floating point number with averaging the results of a large number of runs of the algorithm. Their precision will depend on several factors: the number of runs or "shots", the qubit error rates and the efficiency of quantum error correction codes. Given the overhead of all of this, forget about using qubits as a high-precision floating point number storage device!

When the state vector of the qubit is horizontal in the Bloch sphere, i.e. it sits in its equator, and we have an even superposition of  $|0\rangle$  and  $|1\rangle$ , but with a variable relative phase between the  $|0\rangle$  and  $|1\rangle$  amplitudes which is related to the horizontal angle of the vector  $\varphi$  with respect to the z axis as in the diagram on the right. Two usually superposed states are  $|+\rangle$  and  $|-\rangle$ .



<sup>212</sup> To learn more and with a better scientific accuracy, you can consult the Wikipedia sheet of the [wave function](#) and [amplitude probability](#). Other explanations can be found in the example of the electron orbit levels in the hydrogen atom in [Quantum Mechanics and the hydrogen atom](#) (19 slides). The physical interpretation of Max Born's statistical rule remains in any case open, as explained in Arkady Bolotin's June 2018 paper, [Quantum probabilities and the Born rule in the intuitionistic interpretation of quantum mechanics](#) (14 pages).

These are orthogonal states. These equatorial states share the same  $\alpha$  component of  $1/\sqrt{2}$  but opposite  $\beta$  values. This qubit-rich information is then modified by phase rotation quantum gates.

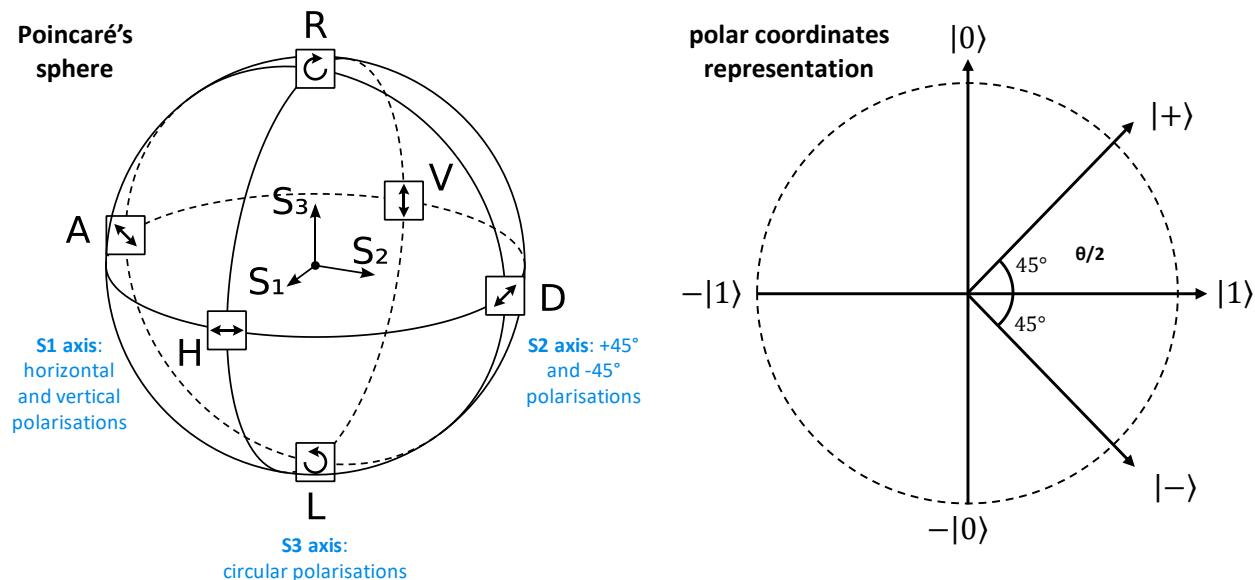
If all qubits in the equator share the same 50%/50% amplitude probabilities, they have a different phase. A significant part of the quantum computing power comes with playing with the qubit phase that generates interferences between qubits. We'll see that later with algorithms such as phase amplitude and phase kickback.

As a general rule, most quantum gates do not generate all vector positions in the Bloch sphere. They are often half or quarter turns. The points of the sphere most often used are the cardinal points: the  $|0\rangle$ ,  $|1\rangle$ , then the four points corresponding to the superposition of  $|0\rangle$  and  $|1\rangle$  on the equator.

To obtain all the quantum computing power, we need to make smaller turns than quarter turns, with the variable-phase R gates, usually composed with T gates, which we will see later and is outside the so-called Clifford gates group. Only these gates are supposed to enable some exponential speedup with gate-based quantum computing. Another way to look at this is that quantum advantage comes from using the full power of "analog" qubits.

**Origins.** We owe this Bloch sphere to three scientists: **Erwin Schrödinger** for his wave function of 1926, **Max Born** for his associated probabilistic model, created the same year, and to **Felix Bloch** (1903-1983, Switzerland) who represented the state of a two-level quantum on the sphere in 1946.

Bloch's sphere is frequently assimilated to **Poincaré's sphere**, named after **Henri Poincaré** (1854-1912, France) and created in 1892<sup>213</sup>. It is used to describe the polarization of light. The sphere polar coordinates represent the various types of light polarization : linear polarization (on the sphere equator), left elliptical polarization (upper hemisphere), right elliptical polarization (lower hemisphere) then left and right circular polarization (North and South poles). The vertical axis (circular polarization) and one of the horizontal axis (linear polarization) represent two observables for a photon. All other states can be described as linear superpositions of these couples of basis states. And contrarily to massive particle-based quantum objects whose quantum probabilities are described by Schrödinger's equation, light equations used here are just Maxwell's electro-magnetic waves equations.



(cc) Olivier Ezratty, 2021

<sup>213</sup> Here are some sources of information associated with this section: [Lectures on Quantum Computing](#) by Dan C. Marinescu and Gabriela M. Marinescu, 2003 (274 pages), [The Bloch Sphere](#) by Ian Glendinning, 2005 (33 slides), [The statistical interpretation of quantum mechanics](#), Max Born's 1954 Nobel Prize acceptance speech in physics (12 pages) and the excellent book [The mathematics of quantum mechanics](#) by Martin Laforest, 2015 (111 pages), which describes the mathematical basics of quantum computing with complex numbers, vectors, matrices and everything.

The Bloch sphere representation is also used for representing an electron spin measured along three orthogonal axis (X, Y, Z), showing how superposition works with spins.

Sometimes, a system of polar coordinates is used on one circle, positioning the computational basis states of  $|0\rangle$  and  $|1\rangle$  as geometrically orthogonal vectors. It somewhat duplicates values since of  $-|0\rangle$  and  $-|1\rangle$  are similar to  $|0\rangle$  and  $|1\rangle$ , with just a different global phase. Only the right half of the circle is useful.

Many other fancy qubits representations have been created with projection of the Bloch sphere onto a plane, representations of several qubit states with many Bloch spheres, even some representation of quantum entanglement with three Bloch spheres for two qubits<sup>214</sup> or with tetrahedrons<sup>215</sup>. None of these have been standardized and have a practical value for most quantum developers.

## Registers

In a quantum computer, qubits are organized in registers: a bit like the 32- or 64-bit registers of today's classical processors. One key difference is for now, a quantum computer has only one register and not many as with current classical microprocessors.

The main difference between an n-qubit register and a traditional n-bit register is the amount of information that can be manipulated simultaneously. In conventional computers, 32- or 64-bit registers store integers or floating-point numbers on which elementary mathematical operations are performed.

A register of n qubits is a vector in a  $2^n$  dimensional space of complex numbers. Its dimensionality is exponentially larger than a n-bits register. Let's take for instance a register of 3 bits and 3 qubits. The first one will store one value at a time as 101 (5 in base 2) while the register of three qubits will contain complex numbers attached to each of the possible values of this register, 2 to the power of 3, i.e. 8, aka computational state basis. These complex numbers are the amplitude of each computational state. The total of their squares equals 1 since these are probabilities.

n bits register	n qubits register	
<b>101</b> → 2 <sup>n</sup> possible states once at a time	n=3 example evaluable	000 001 010
independent copies	2 <sup>n</sup> possible states simultaneously	011 100
individually erasable	partially evaluable	101 110
non destructive readout	no copy	111
deterministic	non individually erasable	
	value changed after readout	
	probabilistic	aka register pure states

However, these  $2^n$  states amplitudes do not really constitute some information storage capacity. Quantum algorithm's main goal is to amplify the computational basis state amplitude that is the sought result, while reducing all the other amplitudes to near zero. Logically, it is like testing many hypotheses in parallel to bring out the best one.

<sup>214</sup> See [Two-Qubit Bloch Sphere](#) by Chu-Ryang Wie, 2020 (14 pages).

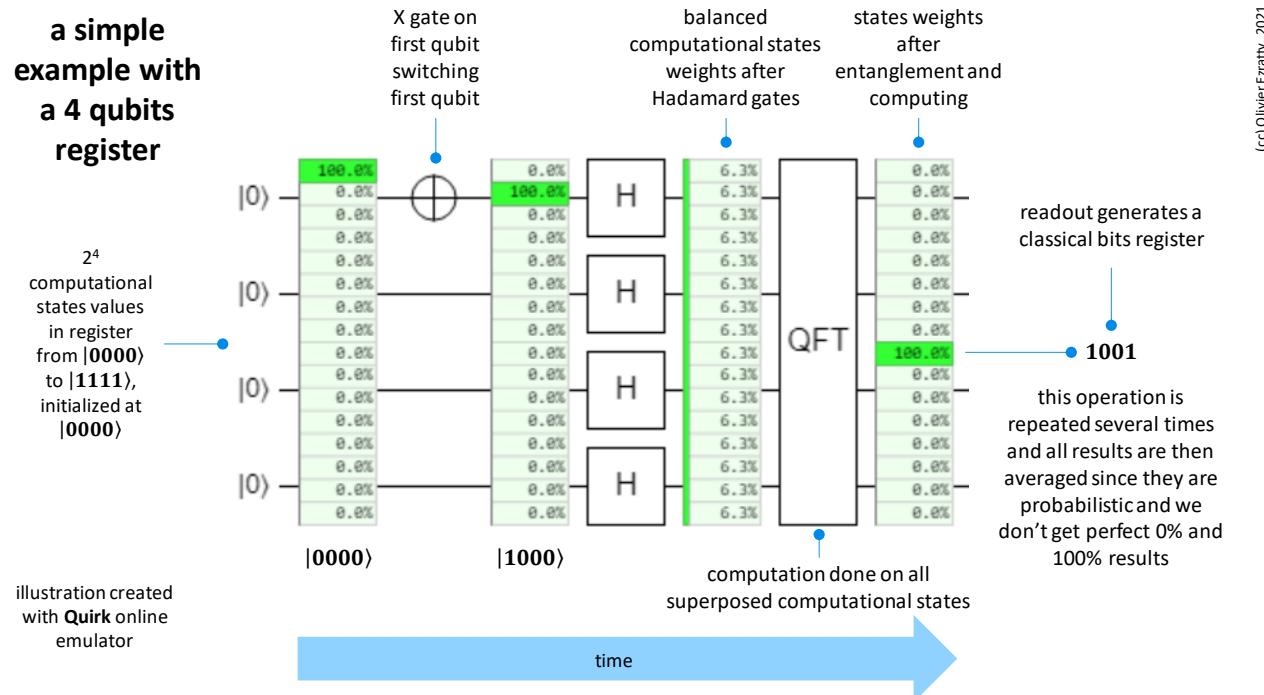
<sup>215</sup> See [Geometry of Qubits - A picture book](#) by Yosi Avron and Oded Kenneth, 2018 (20 slides).

The output information is a set of n classical bits. The  $2^n$  amplitudes handled during computation are not some useful information that we exploit outside the register. We'll always end with one computational state and its related classical bits. So, in the end, you don't really process "big data" with quantum computing or at least, you don't output any big data. You may still use some sort of big data to prepare the state of the register before or during calculation<sup>216</sup>.

But it's not to the advantage of quantum computing since feeding a quantum register with classical data is quite slow<sup>217</sup>.

The graphic representation *below* of the principle mentioned was built using the Quirk open-source simulator. It's a sample of a quantum Fourier transform algorithm run on 4 qubits. The column numbers vector is showing the computational base probabilities. In the beginning we have a 100%  $|0000\rangle$ .

After applying an X gate on the first qubit, we get a 100% amplitude for a  $|1000\rangle$ . After applying Hadamard gates to all qubits, we get even amplitudes of 6,3% for all computational basis states. Then the QFT finds out the result,  $|1001\rangle$  which shows up on the last column<sup>218</sup>.

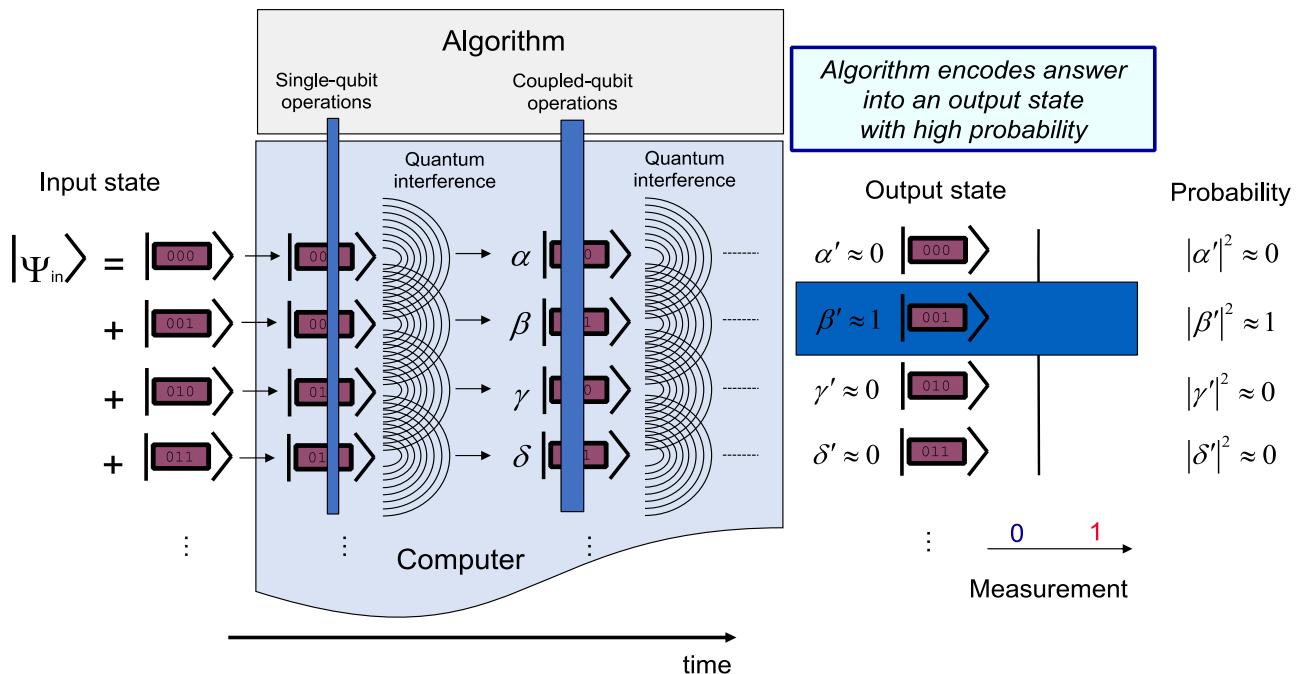


<sup>216</sup> However, exceptions are beginning to appear with hybrid methods for accelerating database access combining traditional computer-based and quantum algorithms. See [Quantum computers tackle big data with machine learning](#) by Sarah Olson, Purdue University, October 2018.

<sup>217</sup> It's well explained in the excellent overview [Quantum Computing: Progress and Prospects](#) from the US Academy of Sciences, 2019 (272 pages) : "Large data inputs cannot be loaded into a QC efficiently. While a quantum computer can use a small number of qubits to represent an exponentially larger amount of data, there is not currently a method to rapidly convert a large amount of classical data to a quantum state (this does not apply if the data can be generated algorithmically). For problems that require large inputs, the amount of time needed to create the input quantum state would typically dominate the computation time, and greatly reduce the quantum advantage."

<sup>218</sup> In [A quantum computer only needs one universe](#) by Andrew Steane, 2003 (10 pages), the latter insists on the key role of entanglement. He considers that entanglement does not so much explain the gain in quantum computing power.

Another way of presenting things is a little simpler and more graphical: all the register states are on the left, the calculation generates interference between these states to make one of the states on the right come out which is the answer to the problem posed<sup>219</sup>. The example is based on the use of only two qubits that give four different "binary" states of the qubits.



So we do not recover  $2^n$  values in practice, but  $n$  bits. The operation can be repeated several times to obtain an average in the form of floating numbers. But it depends on the algorithms. For the majority of them, a binary output is sufficient, as for Peter Shor's integer factorization algorithm.

We are anyway constrained by **Holevo's theorem** of 1973 which proves that with  $n$  qubits, we cannot recover more than  $n$  bits of information after a quantum calculation ([source](#))!

At the current stage of qubit development, one and two qubits gates error rate is between 0,1% and 0.5% and ideally it should be less than 0.0001%. This error rate can be evaluated for each isolated qubit.

By the way, don't believe the nonsense that is the comparison of the exponential size of the qubit registers computational basis state with the number of particles in the Universe. These are not equivalent data. A number of objects combination is not homothetic with a number of objects! With a given number of objects, the combinatorics of these objects will always represent a number that is much higher than the number of objects taken as a reference.

On the other hand, besides this exponential combination sizing, qubits have a lot of drawbacks in total opposition with classical bits. One can neither copy classically nor erase the value of qubits individually. Their measurement modifies their values. These are probabilistic objects that are difficult to manipulate.

<sup>219</sup> See [Introduction to Quantum Computing](#) by William Oliver from MIT, December 2019 (21 slides).

**Ancilla qubits.** Universal gate quantum computing uses ancilla qubits or control qubits that can be combined with the computing qubits. The value of these qubits is not read at the end of the processing. It is a kind of trash can of qubits used during computations. They are used in various algorithms as well as to implement the error correction codes (QEC) explained later. We still always use a single qubit register. It can be just logically partitioned between computation qubits and ancilla qubits, these last playing more or less the role of classical registers in a microprocessor. Their content may be scrapped at the end of some parts of computing. It's sometimes done using the "uncompute trick" which reverses part of the processing affecting these ancilla without erasing the other qubits containing the intermediate computing result.

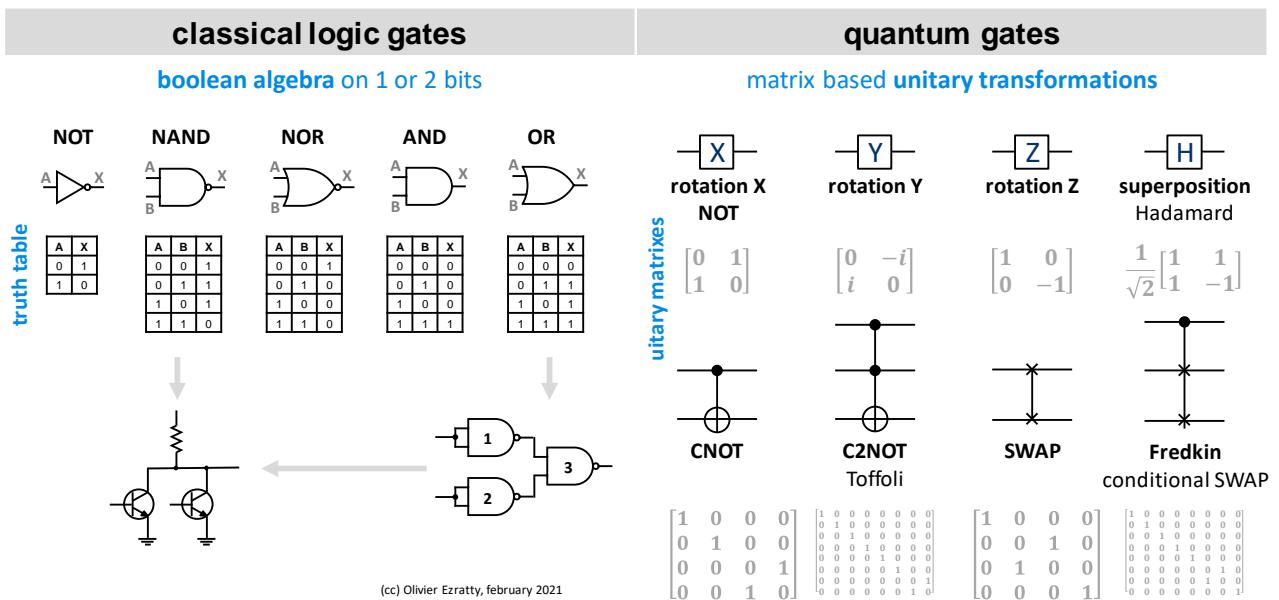
## Gates

In classical computing, logic gates execute Boolean algebra using bit-dependent decision tables as an input. Several types of logic gates with one and two inputs are used, including the NAND gate which is interesting because it is universal and uses only two transistors. The other one- and two-bit Boolean gates can theoretically be created with NAND gates. In general, however, logic gates are mixed in the circuits.

An Intel Core i5/7 processor with over 10 billion transistors contains several billion logic gates. A processor is obviously very complex, with gates managing access to a cache memory and registers, and instruction pipeline executing the code defining the gates to be used in calculations. These operations are generated at the processor's clock frequency, most often expressed in GHz. The classic two-bit logic gates (NAND, NOR, XOR, AND, OR) are irreversible because they destroy information during their execution.

Qubits undergo operations via quantum gates that can be applied to one or more qubits. Single-qubit gates apply linear algebra operations in the form of  $2 \times 2$  unitary matrices of real and complex numbers as shown below. These unitaries are applied to the qubit state vector containing the famous  $\alpha$  and  $\beta$  complex amplitudes. These generate a rotation of the qubit vector in the Bloch sphere. The norm of the vector remains stable at 1 at least, before any decoherence happens. And quantum gates modify qubits information without reading it.

Quantum gates operating on two qubits are applying  $4 \times 4$  unitary matrices applicable to the computational basis state vector containing 4 entries ( $2^2$ ). Then, on three qubits, the gate unitary is an  $8 \times 8$  matrix, applicable to a state vector containing  $2^3$  entries.



Here are the main quantum gates used by quantum developers<sup>220</sup>:

- **X** gate (or NOT) performs an inversion or bit flip. A  $|0\rangle$  becomes  $|1\rangle$  and vice-versa. Mathematically, it inverts the  $\alpha$  and the  $\beta$  of the two-component vector that represents qubit state. It generates a  $180^\circ$  rotation in the Bloch sphere around the X axis.

This gate is often used to initialize to  $|1\rangle$  the state of a qubit at the beginning of a process which is by default initialized at  $|0\rangle$ .

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- **Y** gate performs a  $180^\circ$  rotation around the Y-axis in the Bloch sphere. It also turns a  $|0\rangle$  into  $|1\rangle$ .

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

- **Z** gate applies a sign change to the  $\beta$  component of the qubit vector (phase flip), i.e. a phase inversion and a  $180^\circ$  rotation with respect to the Z axis. The X, Y and Z gates are called **Pauli gates**.

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Their unitary matrices are usually noted  $\sigma_x$ ,  $\sigma_y$  and  $\sigma_z$ . Any single qubit unitary transformation can be written as a linear combination of Pauli gates with real number coefficients, plus the identity I.

- **S** gate generates a phase change, or a quarter turn rotation around the Z-axis (vertical). This is the equivalent of a half Z-gate. It is also called a "phase gate".

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

- **T** gate equivalent to a half S, which generates a phase change of one eighth of a turn. With two of these gates, an S gate is generated. This gate that is not part of Clifford's group (defined ... later) has the particularity of allowing by approximation the creation of any rotation in Bloch's sphere.

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

It's the key to universal gate-based quantum computing. It is indispensable to run a quantum Fourier transform and all derived algorithms like Shor integer factoring, HHL (linear algebra) and most quantum machine learning algorithms.

- **R** phase shift gates are variations of Pauli gates, with rotations different from the half or quarter turns in the Bloch sphere, using an arbitrary angle. The  $R_z$  gate rotates around the z axis,  $R_x$  around the x axis and  $R_y$  around the y axis<sup>221</sup>. A  $R_z(\text{angle})$  gate is also called a P(angle) gate (P for phase).

$$R_m = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^m}} \end{bmatrix}$$

When the x, y and z axes are not specified, it is z, the vertical axis of the Bloch sphere, as in the matrix *above*. When x, y and z are specified without an angle or m, it is  $90^\circ$  or  $\pi/2$ . The rotation is carried out on a complete round divided by m. The  $R_z$  gates modify the phase of a qubit and not its amplitude. Thus, the measurement of its state  $|0\rangle$  or  $|1\rangle$  is not affected by this gate. It will return both  $|0\rangle$  or  $|1\rangle$  with the same proportions, before and after the use of an  $R_z$  gate. Only two points of a sphere do not move during a rotation around an axis connecting them.

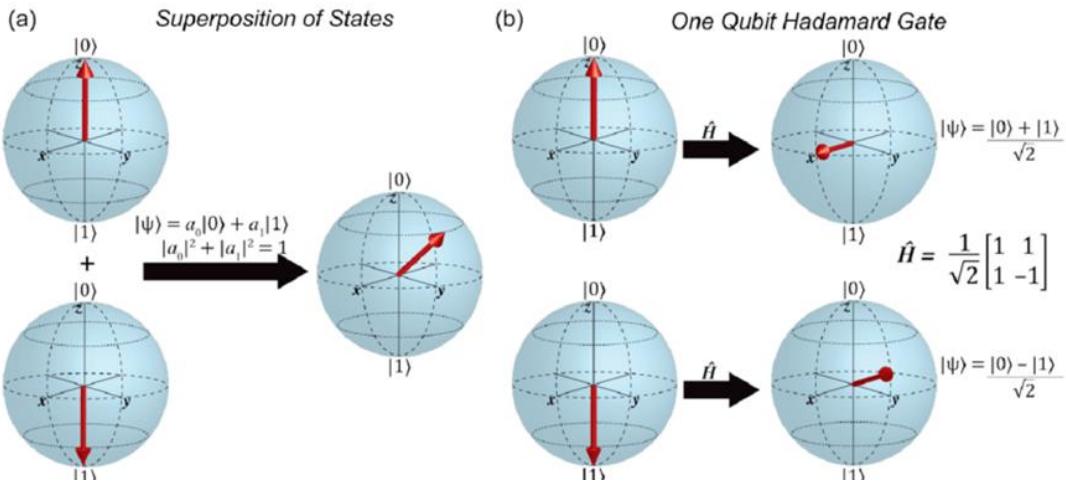
- **H** gate aka Hadamard-Walsh: puts a qubit at  $|0\rangle$  or  $|1\rangle$  in a superposed state " $|0\rangle$  and  $|1\rangle$ ". It is fundamental to generate this superposition in the registers.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

---

<sup>220</sup> Single qubit gates can be classified in XY and Z gates. XY gates are rotations around an axis in Bloch's sphere equator and can be viewed as amplitude change gates while Z gates are rotations around the Z axis and can be described as phase change gates.

<sup>221</sup> This is well explained in [The Prelude](#), Microsoft, 2017.



It is often used to initialize a quantum register before executing an oracle-based algorithm like Grover or Simon algorithms. Here is a representation of the effect of this gate on a qubit initialized at  $|0\rangle$  or  $|1\rangle$  ([source](#)). If we apply two Hadamard gates to a qubit, we return to the starting point. In other words:  $HH = I$  ( $I$  = identity operator)<sup>222</sup>.

- **I or ID** gate is the identity gate. It may be used as a pause. In the real physical world, a real I gate is not an exact identity due to decoherence! If you “run” 20 identity gates on a  $|1\rangle$  qubit, you’ll end up having some phase flipping error transforming progressively the qubit into a  $|0\rangle$ .

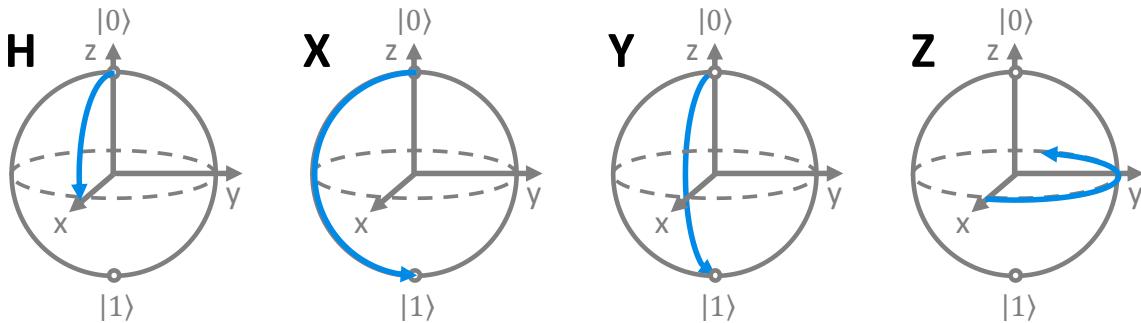
$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- $|0\rangle$  reset gate is sometimes indicated at the beginning of an algorithm to indicate that we start with initialized qubits. It’s obviously irreversible.

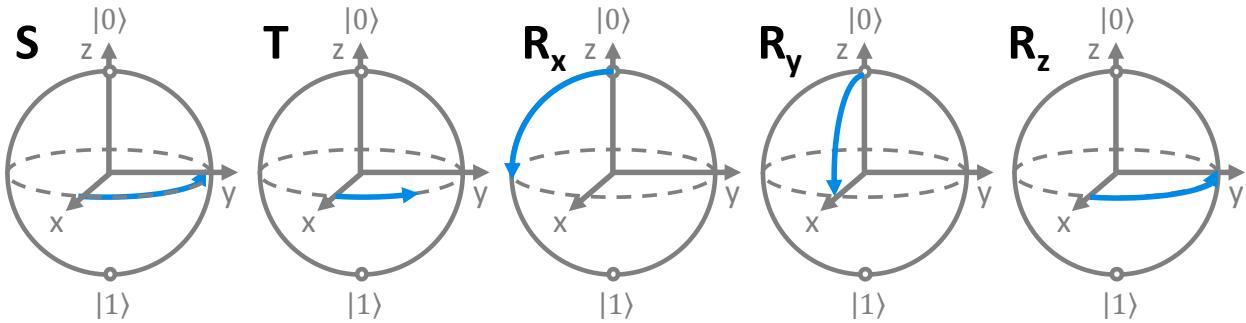
$$|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

The mathematical formalism applied to a single qubit simply illustrates this. But this works only in theory, only if the gate error rate is zero. Since it is not zero, you don’t ever have a perfect  $|0\rangle$  or  $|1\rangle$ . A qubit reset operation may also be used to clean up ancilla qubits after their usage, when we are not using the uncompute trick, which is a way to cleanly reset ancilla qubits.

Below are representations of the effect of these unary gates on qubits initialized in  $|0\rangle$  for the gates H, X, Y, R<sub>x</sub> and R<sub>y</sub> and with  $|+\rangle$  for the phase change gates S, T, Z and R<sub>z</sub>. Indeed, phase shift gates have no effect on  $|0\rangle$  as well as on  $|1\rangle$ . For  $|1\rangle$ , it may just change the qubit global phase, and not its relative phase between the qubit amplitudes  $\alpha$  and  $\beta$ , with no material impact on most algorithms. In the examples, the R gates use an angle of 90° or  $\pi/2$ .



<sup>222</sup> This is also valid with X, Y and Z gates. In the usual notation, an H gate applied to  $|0\rangle$  gives a state  $|+\rangle$  and an H gate applied to  $|1\rangle$  gives a state  $|-\rangle$ .



Then we have two or three qubit gates. Apart from the SWAP gate and its derivatives, these gates are conditional gates that apply a transformation of the state of one or two target qubits according to the state of one control qubit. These conditional gates implement the principle of state entanglement of the qubits that are in play. The dependency relationship between the qubits involved remains valid after the execution of these gates.

- **CNOT gate** is an inversion of the value of a qubit conditioned by the  $|1\rangle$  value of another qubit. It is a quantum equivalent of the XOR gate in classical computing. Formerly called Feynman gate (C).
- **C2NOT or Toffoli gate** is an inversion of the value of a qubit conditioned by the  $|1\rangle$  value of two other qubits.
- **CZ gate**, or Control-Z, is a conditional phase change Z gate.
- **CS gate**, or Control-S, allows a phase change of a qubit controlled by the state of a qubit.
- **SWAP gate** inverts the quantum values of two qubits. It can be generated from the chaining of three consecutive CNOT gates. The SWAP gate is the only two-qubit gate that is not creating a new entanglement between the two qubits. If they were separable before the gate, they will still be separable afterwards.

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The key role of SWAP gates is to connect qubits that are physically distant in the register physical layout. A SWAP gate may also displace some entanglement. For example, if qubits A and B are entangled, but C is not entangled with A and B, a SWAP between B and C will displace entanglement to A and C and leave B unentangled with A and C.

SWAP is usually a costly gate. It is not used a lot when the qubit topology enables all to all qubits direct connections like with some trapped ions qubits.

two qubits quantum  
gate unitary matrix \*      2 qubits  
register state      resulting state  
 SWAP on  $|01\rangle = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$

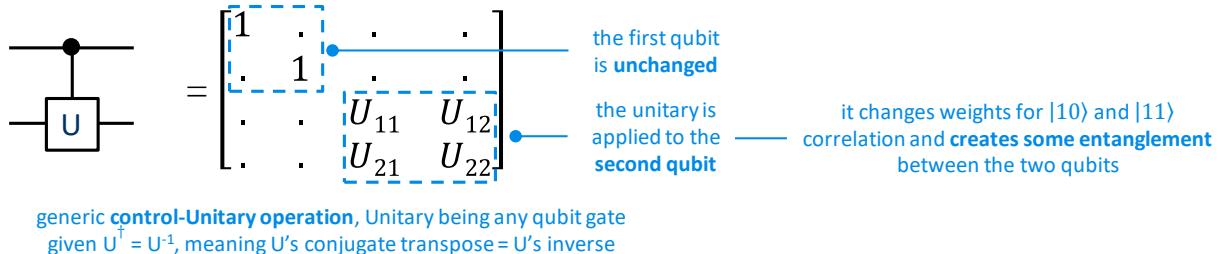
complex number values  
 $\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$  weight of  $|00\rangle$   
 weight of  $|01\rangle$   
 weight of  $|10\rangle$   
 weight of  $|11\rangle$

the 2 qubits gate unitary matrix for SWAP  
 is multiplied by the 2 qubits register state

a 2 qubit register state is a vector containing  
 the weight of each combination of  $|0\rangle$  and  $|1\rangle$

- **Fredkin gate** is a SWAP gate between two qubits that is conditioned by the state of a third qubit. So it has three inputs.

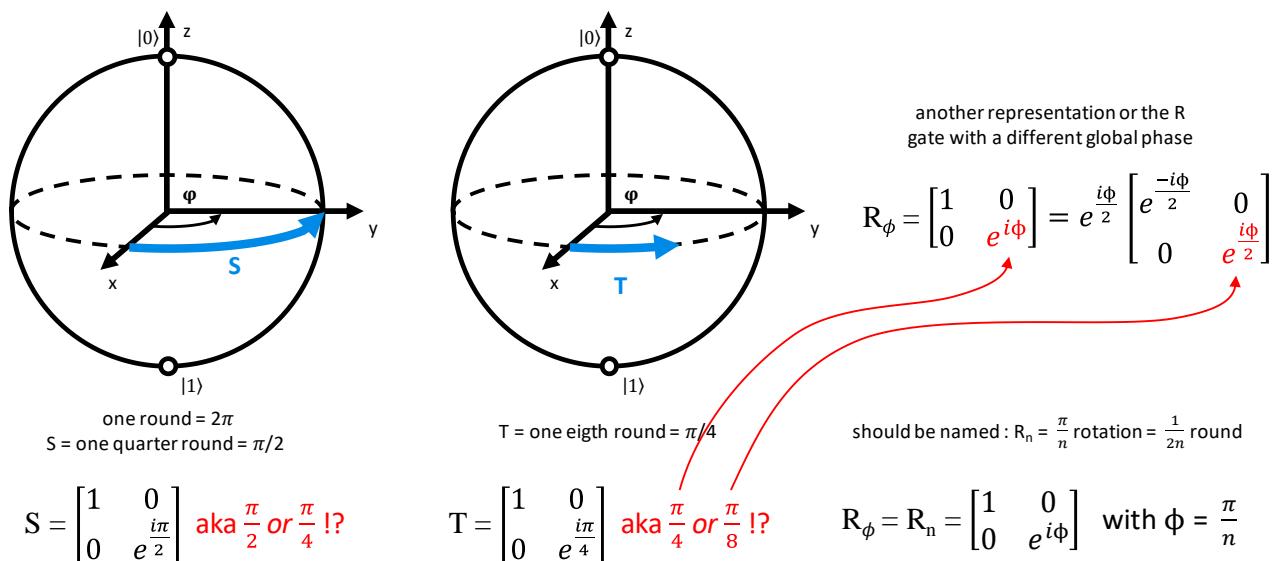
- **Generic Control-U gate** is a two qubits gate applying a generic one qubit unitary to a qubit based on the state of a control qubit.



- **Phase-controlled R gates** are the equivalent of single-qubit phase-change R gates, conditioned by the state of a control qubit. If the algorithm, like a quantum Fourier transform, requires m to be large, it is not easy to ensure the reliability of the gate because the required precision becomes very large compared to the phase errors generated by the quantum system. However, phase errors are difficult to correct!

A precision record of such a gate seems to have been reached by Honeywell with its ion trapped qubits presented in 2020 which have a rotation precision of 1/500 turn. This reminds us that during operations, quantum computing is analog. It is digital only at the level of commands and measured results, which become classical bits again<sup>223</sup>.

There are some reasons to get confused with S, T and R phase gates angles. For example, a S gate is sometimes branded as a  $\pi/2$  and sometimes as a  $\pi/4$ . The same is applied to a T gate that is sometimes a  $\pi/4$  and sometimes a  $\pi/8$ . The explanation is in the chart below and is related to the way a global phase is applied to the gate unitary operator. We can split hairs with using a “rotation” for the large one and a “round” for the small one.



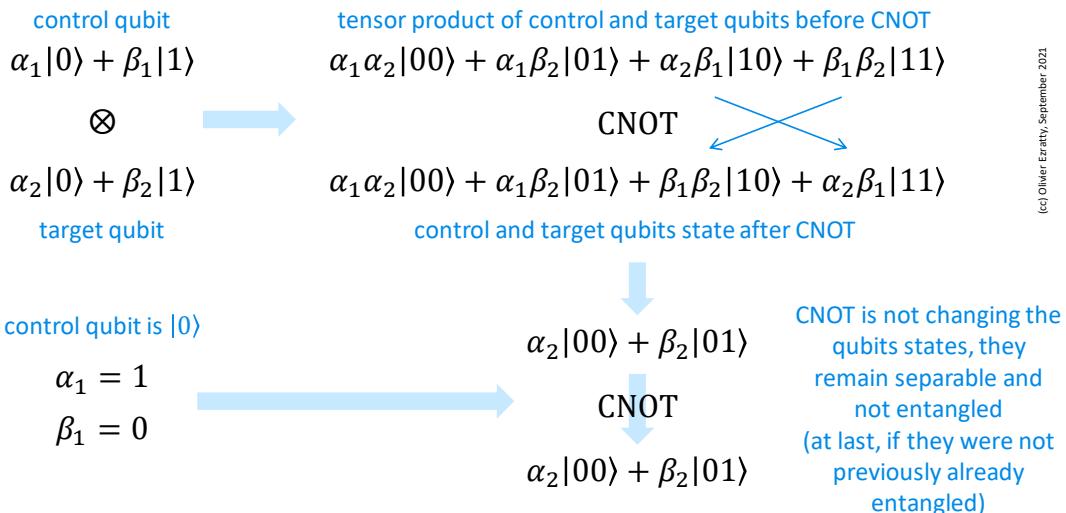
The effect of two-qubit gates is mostly always presented with using  $|0\rangle$ s and  $|1\rangle$ s as starting points in the control qubit, like with “*a CNOT inverts the state of a target qubit when the control qubit is  $|1\rangle$* ”. But the CNOT will always have an effect on the target qubit when the control qubit is not exactly in the  $|0\rangle$  state.

<sup>223</sup> Here are a few sources of information on the subject of quantum gates: [Gates, States, and Circuits](#) by Gavin E. Crooks, July 2021 (82 pages), [Universality of Quantum Gates](#) by Markus Schmassmann, 2007 (22 slides), [An introduction to Quantum Algorithms](#) by Emma Strubell, 2011 (35 pages), [Equivalent Quantum Circuits](#) by Juan Carlos Garcia-Escartin and Pedro Chamorro-Posada, 2011 (12 pages), [The Future of Computing Depends on Making It Reversible](#) by Michael P. Frank, 2017.

You just need to have a non-null  $\beta$  complex amplitude component in the first qubit. So, the only case a CNOT will do nothing on the target qubit is when the control qubit is exactly a  $|0\rangle$ .

To fully understand the effect of these gates on any qubit state and computational basis vectors for several qubits, you have to look at the unitary matrices implementing these gates and their linear effects on the qubits and/or register computational basis vectors.

In other words, and as demonstrated *below*, unless the control qubit is  $|0\rangle$ , a CNOT gate will create some new entanglement between the control and target qubit. But one could argue two things: first, after a couple of operations, we never have a perfect  $|0\rangle$  and are rapidly off-bounds, creating tiny entanglements with CNOT gates in that case, and second, most CNOT gates are run after a Hadamard gate was applied on the control qubit, getting off the  $|0\rangle$  state!



(cc) Olivier Ezratty, September 2021

Let's add a number of two-qubit gates which play a particular role. These are physical gates implemented at the lowest control level depending on the qubit type. They are not necessarily directly useful for developers but are the basis of some specific universal gates sets with some qubit types.

- **$\sqrt{\text{SWAP}}$  gate**, or square root SWAP, stops halfway through a SWAP. It is a physical level gate used to entangle electron spin qubits.
- **iSWAP gate** is a two-qubit gate that is implemented in superconducting qubits like those from IBM.
- **XY gate** is a generic two-qubits gate implementing a rotation by some angles  $\beta$  and  $\theta$  between the states  $|01\rangle$  and  $|10\rangle$  and  $i\text{SWAP}=\text{XY}(0,\pi)$ . It's a physical gate proposed by Rigetti that can be implemented on superconducting qubits to reduce the number of two-qubits gates required to run many algorithms<sup>224</sup>.
- **ZZ coupling** is a technique that can be used with qubit couplers to connect two superconducting qubits and implement a CZ gate<sup>225</sup>.

$$\sqrt{\text{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\text{XY}(\beta, \theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\frac{\theta}{2}) & i \sin(\frac{\theta}{2}) e^{i\beta} & 0 \\ 0 & i \sin(\frac{\theta}{2}) e^{-i\beta} & \cos(\frac{\theta}{2}) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

<sup>224</sup> See [Implementation of the XY interaction family with calibration of a single pulse](#) by Deanna M. Abrams et al, 2019 (13 pages).

<sup>225</sup> See [Implementation of Conditional Phase Gates Based on Tunable ZZ Interactions](#) by Michele C. Collodo, Andreas Wallraff et al, PRL, May 2020 (10 pages).

- **Mølmer-Sørensen gate, Cirac-Zoller gate (C-NOT), AC Stark shift gate and Bermudez gate** are various two-qubit gates implemented at the physical level with trapped ions qubits. The Mølmer-Sørensen gate is a “mixed-species” entangling gate that can couple different breeds of ions. It is also less sensitive to motion temperature. It’s the main entangling gate for IonQ trapped ion computers.

	atoms		electrons & spins				photons
qubit type	trapped ions	cold atoms	super-conducting	silicium	NV centers	Majorana fermions	photons
single qubit gates	rotations	$U_{xyz}(\theta, \psi, \mu)$	$R_x(\pm\pi/2), R_z(\lambda)$ (IBM, Rigetti)	$R_x, R_y$	$R_x, R_y$	T, H	X, Z, H X, Z, R, CZ (Xanadu)
two qubit gates	XX Mølmer-Sørensen	C-Z $C-U_{xy}(\theta, \psi)$	CNOT, iSWAP (IBM) C-Z (Rigetti)	$\sqrt{SWAP}$	CNOT	CNOT	CNOT

[cc] Olivier May, July 2021

**Logical reversibility.** Quantum gates have the particularity of being logically reversible. It can easily be visualized for a single qubit gate, which is a simple rotation in the Bloch's sphere and therefore, reversible with the inverse rotation. A multi-qubit gate is a rotation in a wider dimensional space, with  $2^N$  dimensions, N being the number of qubits. Likewise, it's logically reversible with an inverse rotation, but harder to visualize.

We can rewind some parts of algorithms by applying in reverse order the quantum gates that have just been applied to a set of qubits<sup>226</sup>. One benefit of this process is the so-called uncompute trick used in some oracle-based algorithms. It enables resetting the ancilla qubits used in computation without doing any reading. It avoids damaging the useful qubits that we need to use for the rest of the algorithm.

That being said, qubits can undergo other operations. They could be stored, meaning transferred, in or from quantum memory.

They can also be used to encode two bits instead of one, in what is called "superdense coding", which is mainly used in quantum telecommunications<sup>227</sup>.

**Gates classes.** The science of quantum gates has led to the creation of many concepts, theorems about groups of quantum gates. They are associated with the notion of **universal gate sets**, capable of generating all other quantum gates.

Below is a custom diagram summarizing these classes of quantum gates. In short,  $SU(2^n)$  is the space of unitary transformations applicable on n qubits. It covers all the quantum computations that can be performed on n qubits.  $SU(2)$  includes all the unitary transformations that can be performed on one qubit (with  $n=1!$ ). Clifford's group includes gates with one and discrete qubits quarter-turn rotation plus conditional gates. T (eighth-turn) and R as Control-R gates with different angles from  $\pi$  and  $\pi/2$  are not in Clifford's group. They are needed to cover  $SU(2)$  and  $SU(2^n)$  well. In practice, the addition of the T gate is enough to create a universal gate set with using approximations.

The classification of the gates begins with the **Pauli gates** that apply half-turn rotations around the X, Y and Z axes of the Bloch sphere of representation of the qubits.

---

<sup>226</sup> See [Synthesis and Optimization of Reversible Circuits - A Survey](#) by Mehdi Saeedi and Igor Markov, 2011 (34 pages), which reviews the algorithmic impact of reversibility in both classical and quantum computing.

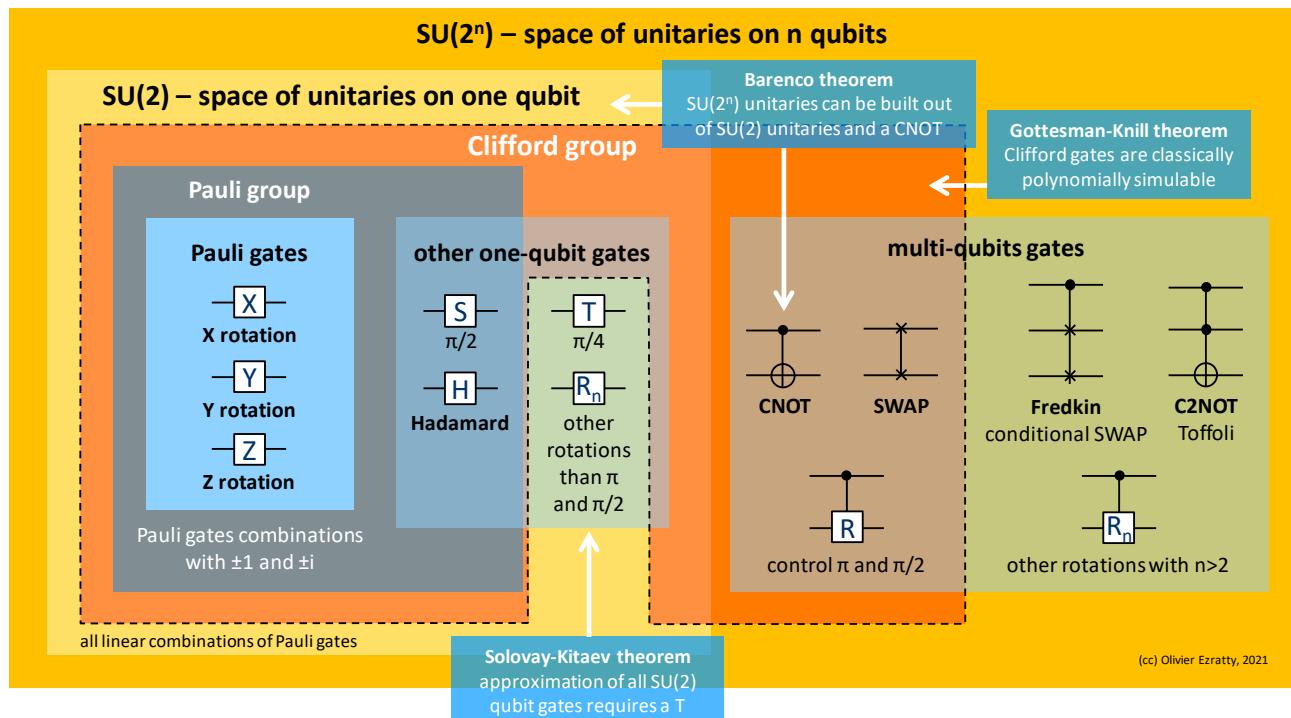
<sup>227</sup> See [From Classical to Quantum Shannon Theory](#), 2019 (774 pages) which describes the application of Shannong's information theory to quantum computing. As well as [On superdense coding](#), August 2018, by Fred Bellaiche, an Econocom engineer who publishes very interesting and popularized scientific articles on quantum.

**Pauli group** includes the gates resulting from the combination of these three Pauli gates and the sign inversion operations on the  $\alpha$  or the  $\beta$  of the qubits ( $\pm 1$  and  $\pm i$ ). On one qubit, the Pauli group includes the gates  $\pm I$ ,  $\pm iI$ ,  $\pm X$ ,  $\pm iX$ ,  $\pm Y$ ,  $\pm iY$ ,  $\pm Z$ , and  $\pm iZ$  (where  $I$  is the identity).

**Clifford group** includes single and multiple qubit gates that standardize the Pauli group applicable to  $n$  qubits, i.e. the  $U$  gates of this group combined with the Pauli group gates  $\sigma$  with  $U\sigma U^*$  generate Pauli group gates. A Clifford gate is a quantum gate that can be decomposed into Clifford group gates. These include Pauli gates ( $X$ ,  $Y$ ,  $Z$ ) and  $H$ ,  $S$  ( $90^\circ$  rotation) and CNOT (also called CX for *control-X*) gates. The Clifford group is very large as soon as  $n > 1$ . Its size is respectively 24, 11,520 and 92,897,280 elements for  $n=1$ , 2 and  $3^{228}$ . It is usually said that Clifford group gates are digital quantum gates while non-Clifford gates are analog.

**Gottesman-Knill's theorem** demonstrates that algorithms using gates in the Clifford group can be simulated in polynomial time on classical computers. It means that they are insufficient to provide an exponential speedup compared to classical computing<sup>229</sup>.

So, how can we obtain an exponential acceleration? It is necessary to use gates with more than two qubits implementing entanglement to obtain this acceleration like the Toffoli gate<sup>230</sup>. This can also be achieved with using phase-controlled R gates that are not part of Clifford's group, which can be approximated with adding a T gate. These non-Clifford gates have a particularity: they are difficult to correct with quantum error correction codes and to be implemented in a fault-tolerant manner. We'll see that [later](#).



<sup>228</sup> Source: [Clifford group](#) by Maris Ozols, 2008 (4 pages). Clifford is the name of an English mathematician, William Kingdon Clifford (1845-1879) who is not related to the group that bears his name.

<sup>229</sup> [Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient](#) by A. Mari and J. Eisert, December 2021 (7 pages) generalizes the Gottesman-Knill theorem to quantum systems that preserve the positivity of the Wigner function (aka, do not use non-Gaussian photon states). It creates additional constraints on how to obtain exponential speedups with photon based quantum computers.

<sup>230</sup> See [On the role of entanglement in quantum computational speed-up](#) by Richard Jozsa et Noah Linden, 2002 (22 pages).

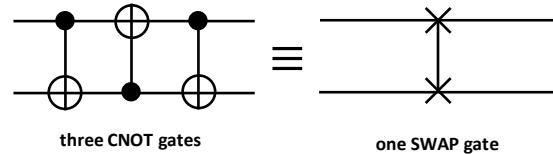
**Continuous gates** make it possible to generate rotations of any angle in the Bloch sphere. The latter allow to generate all the phase-controlled R gates we have just seen and which are indispensable for QFT (Quantum Fourier Transform) based algorithms. Only a few qubits technologies can generate these gates at the hardware level, and usually with a poor precision.

**Discrete gates** are sets of (Hadamard, Z, S, CNOT) that make at best only half and quarter turns in the Bloch sphere.

**Universal gate set** is a group of gates that has the property of allowing the creation of all unitary operations on a set of qubits. From a practical point of view, also it allows to create all known quantum gates for one, two and three qubits. Such a gate-set must be able to create superpositions, entanglement and it must have at least one gate with no-real parameters (i.e. complex numbers instead of real numbers).

Here are some known sets of universal gates:

- CNOT + all single qubit unitaries can enable the creation of any unitary transformation on any number of qubits. This is demonstrated in the **Barenco theorem** according to which  $SU(2^n)$  unitaries can be built out of  $SU(2)$  unitaries and a CNOT two qubit gate<sup>231</sup>. It also demonstrates that any unitary transformation  $SU(2^n)$  on n qubits can be built with a maximum of  $4^n$  elementary quantum gates.
- CNOT + T (eighth of turn) + Hadamard, using approximations, linked to the **Solovay-Kitaev's theorem**. It proves that a dense and finite set of quantum gates in  $SU(2)$  space allows can be used to reconstruct any gate in this space with a maximum error rate  $\epsilon$ .



a set of universal gates can be combined to create all sorts of quantum gates. it requires at least one two-qubit gates like a CNOT.

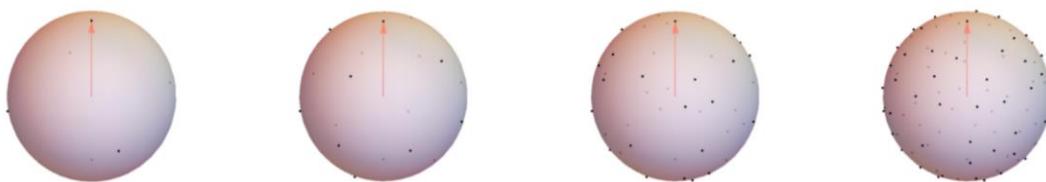
The number of gates to be chained is a polynomial order of magnitude of  $\log(1/\epsilon)$ . The  $SU(2)$  space is the Special Unitary group of dimension two.

It includes unit matrices (from determinant 1) with complex coefficients and dimension 2.

$$SU(2) = \left\{ \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}$$

This search for a set of discrete quantum gates allowing by approximation to generate a set of continuous gates of arbitrary rotations is important for some algorithms that we will see later, notably the discrete Fourier transform that is exploited in Shor's algorithm.

Here is *below* the effect of the sequence of T and H gates which, according to the combinations, allow to cover the different positions of Bloch's sphere, validating **Solovay-Kitaev's theorem**<sup>232</sup>.



<sup>231</sup> See [Elementary gates for quantum computation](#) by Adriano Barenco, Charles Bennett, David DiVicenzo, Peter Shor and al, 1995 (31 pages).

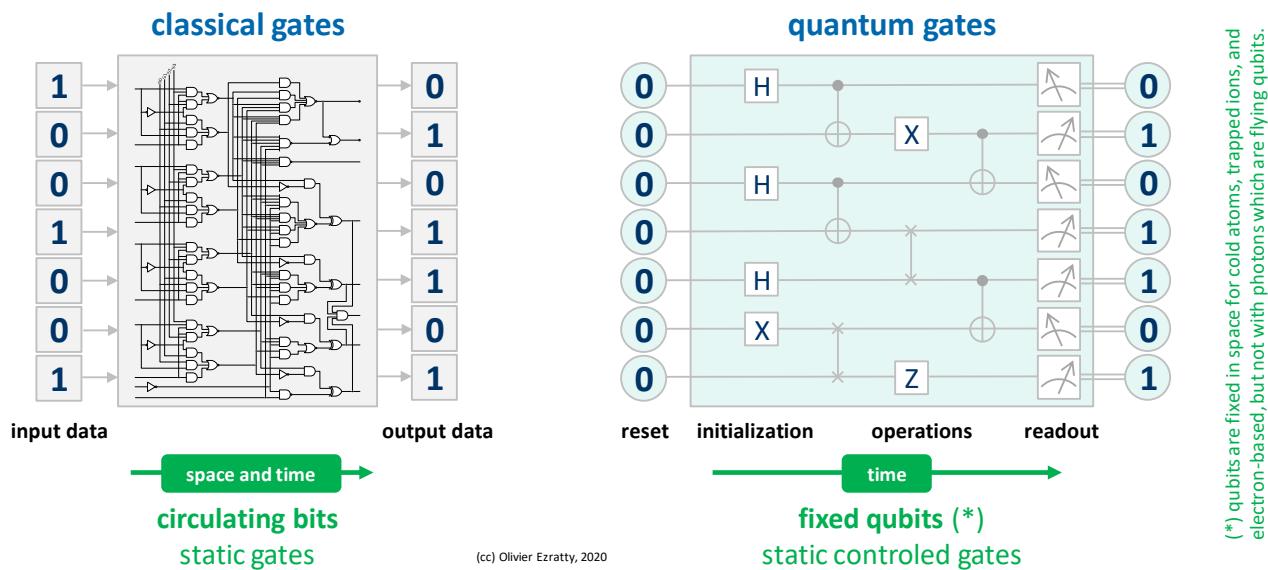
<sup>232</sup> See [Non-Clifford Gates, Universal Quantum Gate Sets & the T-Operator](#) by Francisca Vasconcelos, 2017 (5 pages and 12 [slides](#)).

# Inputs and outputs

Traditional microprocessors are composed of fixed logic gates, etched into the silicon, and 'moving' bits, which are electrical pulses that propagate through the circuit through the various gates. All this at a certain frequency, often in GHz, set by a quartz clock.

In a quantum computer, the first stage of processing consists of resetting the quantum register into an initial state. This is called "preparing the system". The various registers are first physically configured in the  $|0\rangle$  state. The following initialization consists in using different operators such as the Hadamard transformation to create  $|0\rangle+|1\rangle$  superposition or the X gate to change this value  $|0\rangle$  to  $|1\rangle$ . Sometimes, more preparation is required to prepare a denser register state, like with quantum machine learning algorithms.

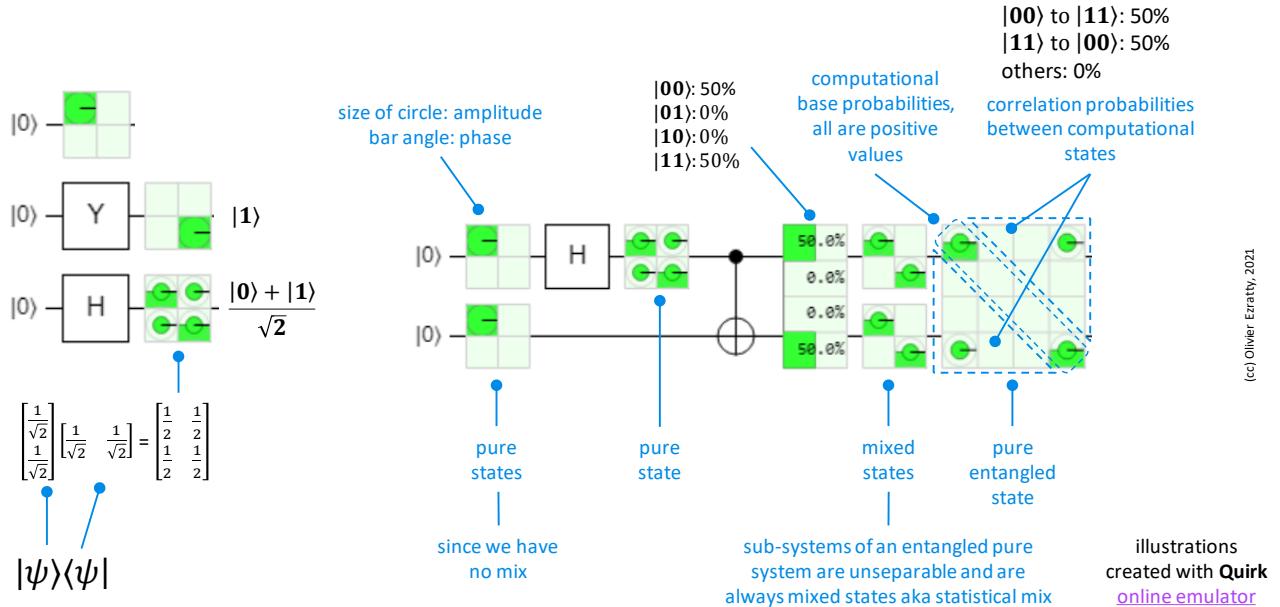
Once this initialization is done, computing gates operations are sequentially applied to the qubits according to the algorithm to be executed. They always include some multi-qubits gates implementing entanglement between qubits. Finally, qubits are measured at the end of the processing, which has the effect of modifying their quantum state.



Quantum algorithms diagrams for universal gates computers (*below right*) are most often time diagrams, whereas for classical logic gates it is also a physical diagram. In the right part describing a quantum algorithm, there are no physical wires connecting the qubits between an input and an output, the gates being in their path. It is a time-based schema !

A quantum algorithm is the description of a quantum circuit made of a series of sequenced timely quantum gates operating on 1, 2 and sometimes 3 qubits. It's the way to create a large unitary transformation on the initialized qubits.

Now, let's toy a little bit with qubits and gates with Quirk, particularly to identify pure and mixed states with single or two qubits. It also shows the role of off-diagonal values in density matrices.



Here, we describe a mixed state generated on two qubits after one of them is entangled with a third qubit.

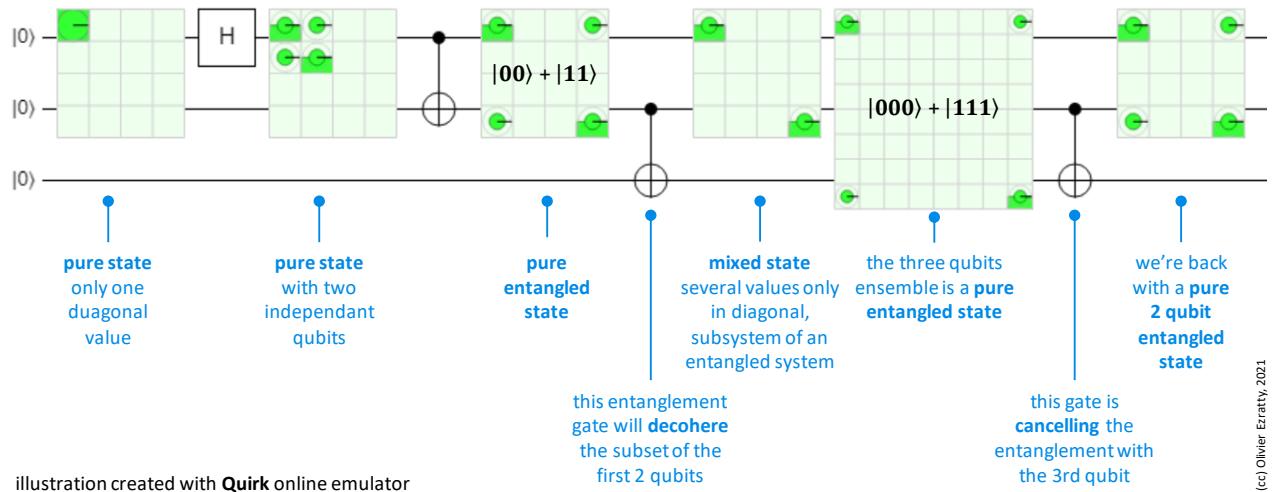
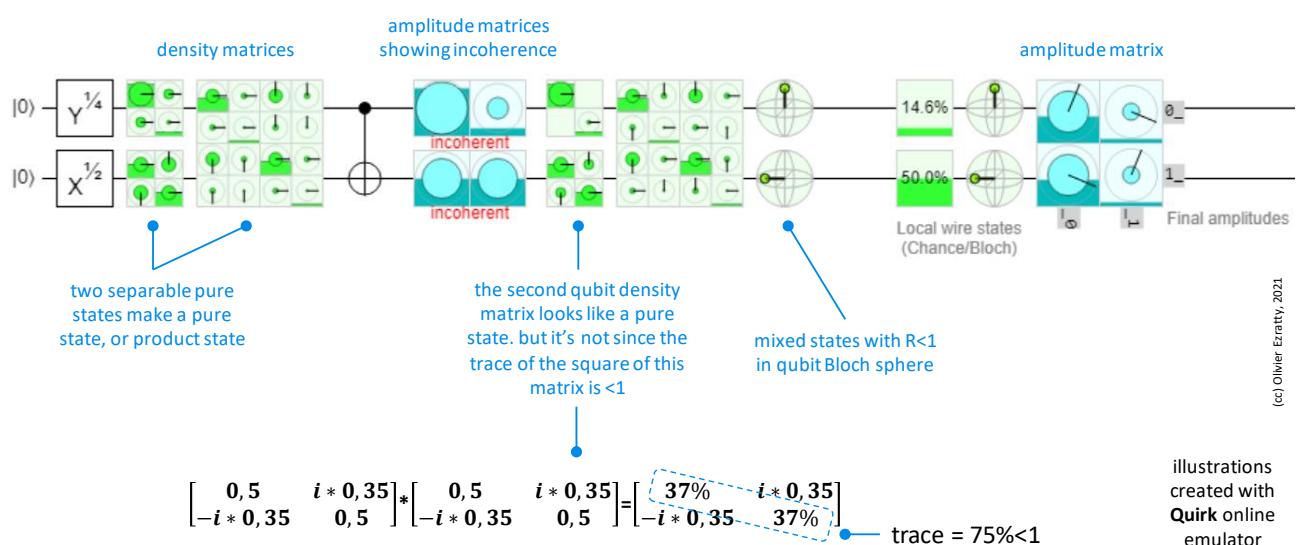


illustration created with **Quirk** online emulator  
<https://algassert.com/post/1716>



# Qubit lifecycle

One way to understand how a universal gates quantum computer works is to track the life of a qubit during processing:

**Initialization.** A qubit is always initialized at  $|0\rangle$ , corresponding to the base state, usually at rest, of the qubit. This initialization consumes some energy with all known types of qubits.

**Preparation.** It is then programmatically prepared with quantum gates to adjust its values that are vectors in the Bloch sphere. The Hadamard gate is one of the most common one and creates a superposed state of  $|0\rangle$  and  $|1\rangle$ . Single qubit gates apply a rotation of the qubit vector in the Bloch sphere. These rotations are based on unitaries,  $2 \times 2$  complex numbers matrix operations applied to the qubit vector  $[\alpha, \beta]$ . These unitaries have a trace of 1, maintaining the vector length of 1. For most quantum algorithms, qubit preparation is usually simple with a set of X gates to set them and H gates to create superposed states. In some cases like with quantum machine learning, qubit states preparation can be more complex, requiring a lot of gates.

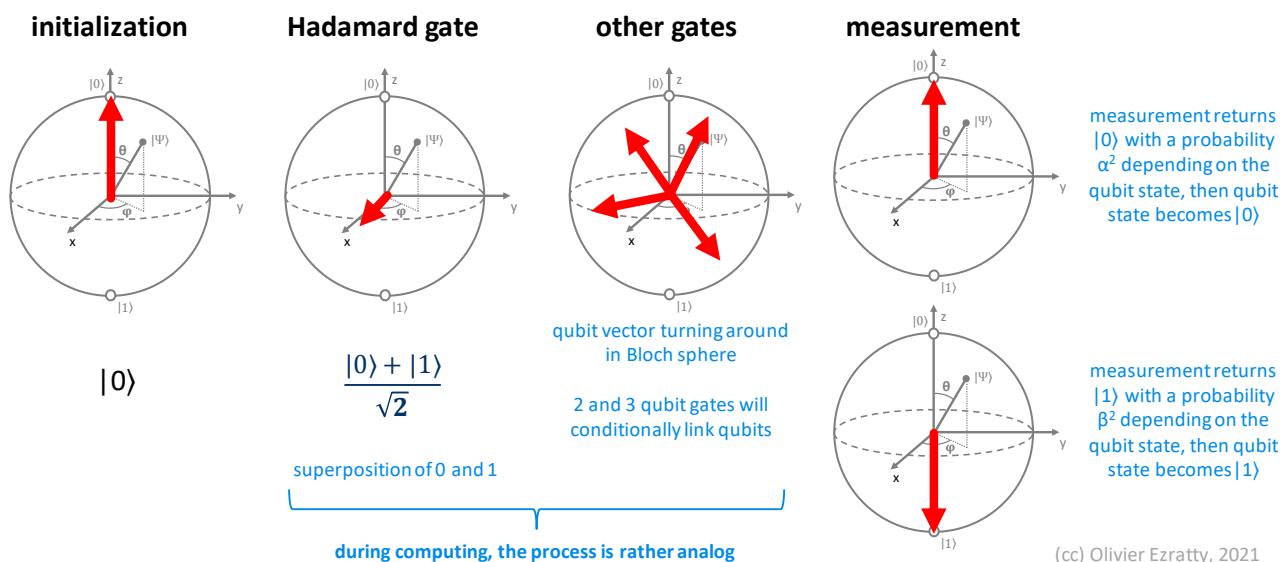
**Multiple-qubit gates** then conditionally link qubits together. Without these quantum gates, little could be done with qubits.

**Data manipulation.** The qubits information that is manipulated during computing is "rich" with a dimension of two real numbers, the angles  $\theta$  and  $\phi$ , or the vector  $[\alpha, \beta]$  for each qubit. But a set of  $N$  qubits holds  $2^N$  complex numbers values, representing the proportion of each of the computational basis states made of the various combinations of  $N$  0s and 1s. It creates a dimensionality of  $2^{N+1}-1$  real numbers, to take into account the normalization constraint for the computational basis states amplitudes. As these gates are operated on the qubits, quantum computing works in an analog way<sup>233</sup>.

**Measurement.** When we measure the value of a qubit, we obtain a classical binary 0 or 1 with a probabilistic return depending on the qubit state. So, for each qubit, we have a 0 as input, a 0 or a 1 as output, and an infinite number of states in between during calculations.

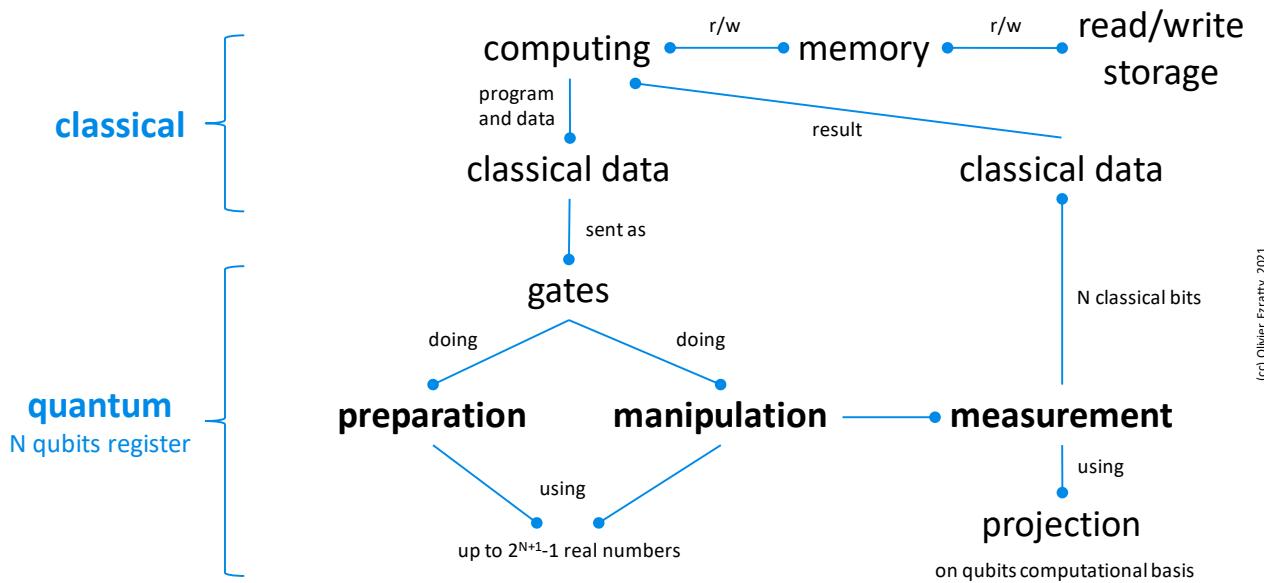
All this to say that the mathematical richness of qubit-based quantum computing happens only during processing.

This is the life cycle of the qubit illustrated in the diagram *below*:



<sup>233</sup> This is the position stated in [Harnessing the Power of the Second Quantum Revolution](#) by Ivan H. Deutsch, November 2020 (13 pages). Or more precisely, the author states that gate-based quantum computers are both digital and analog.

Here's another schematic view of how classical and quantum computing are intertwined and the format of data that is handled. What is specific to quantum computing is that the same instructions handle data and computing, i.e. quantum gates. The wealth of data in registers exists only during computing but not at the end, after measurement, where it is back in classical mode, turning the computational basis state vector of dimension  $2^{N+1}-1$  real numbers to a meager N classical bits.



## Measurement

We'll now look into quantum measurement, a much broader topic than you may think. We have already explained that quantum measurement is assimilated to a wave function collapse onto basis states, in the case of qubits,  $|0\rangle$  or  $|1\rangle$ . We've also seen that quantum computing is highly probabilistic, requiring executing several times your calculation and making an average of the obtained results.

But quantum measurement is way more subtle than that. We'll see here what can be measured in qubits and when, what is a projective measurement, what is a POVM, a CPTP map, what are gentle and weak measurements, non-selective and selective measurement, state tomography and the likes. Some of these techniques are related to quantum computing, including error corrections and some hardware benchmarking tasks and others with quantum telecommunications.

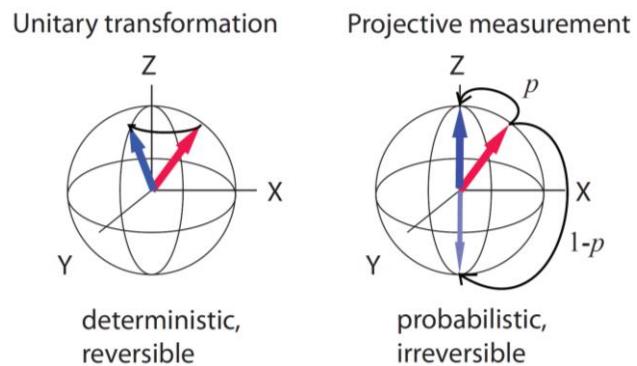
### Projective measurement

A projective measurement is the most generic form of measurement used in quantum computing. We'll first describe it geometrically and then with some mathematical formalism. Projective measurement is also named a von Neumann measurement since **John Von Neumann** elaborated its formalism in 1932.

It's easy to intuitively understand what it looks like with using the Bloch sphere for a qubit. A projective measurement consists in doing a geometrical vector projection of your qubit pure state on any axis in the Bloch sphere.

The simplest case of all is a projection on the z axis containing the  $|0\rangle$  and  $|1\rangle$  orthogonal vectors. It's about doing a measurement in the qubit computational basis. It could also be, theoretically, a projection on any other axis, like the  $|+\rangle$  and  $|-\rangle$  states that sit on the Bloch sphere equator along the x axis. We'll see later how to achieve this feat.

While quantum gates are reversible operations based on unitary operators, reading the state of the qubits is an irreversible operation. It is not a rotation in Bloch's sphere but a projection on an axis, which will yield a binary result with a probability depending on the qubit state<sup>234</sup>. The projection is using a self-adjoint matrix operator, meaning that if executed several times, you'll always get the same result. Of course, the measurement of the qubit modifies its state unless it's already a perfect  $|0\rangle$  or  $|1\rangle$ .



After a projective measurement on the Z axis, the qubit will irreversibly collapse in the states  $|0\rangle$  or  $|1\rangle$ . Qubits measurement is reversible only in the case when they are already perfectly in the computational basis states  $|0\rangle$  or  $|1\rangle$ . In that case, the measurement along the Z axis is not changing the qubit value and is therefore reversible since it's an identity operation.

Mathematically, a projective measurement is using Projection-Valued Measures (PVMs) on a closed system. On a given qubit, it uses two orthogonal measurement operators, in the form of  $2 \times 2$  self-adjointed (Hermitian) matrices.

When measuring a qubit along the Z axis, also named the observable Z with eigenvalues +1 and -1 and eigenvectors  $|0\rangle$  and  $|1\rangle$  (the observable Z is the matrix representation of a Z single qubit quantum gate!), these PVMs operators are respectively:

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} [1 \ 0] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} [0 \ 1] = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Given the Z observable operator is  $Z = M_0 - M_1$ , which returns +1 for  $|0\rangle$  and -1 for  $|1\rangle$ .

On a general basis, with a quantum object with several distinct states, a measurement operator is a matrix  $M_m$  and the probability to get the outcome m (with m=0 and 1 in the case of a qubit, or m=0 to N-1 in the case of a N states quantum object) is  $p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$  with the completeness constraint  $\sum_m M_m^\dagger M_m = I$  ( $I$  being the identity matrix).

For m=0, it reads as  $p(0) = [\alpha \ \beta] \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = [\alpha \ \beta] \begin{bmatrix} \alpha \\ 0 \end{bmatrix} = \alpha^2$  ! Since  $\beta^2 = 1 - \alpha^2$  due to the Born normalization rule, only one measurement is required to get both  $\alpha^2$  and  $\beta^2$ , these being not individual measurement results but their respective probabilities.

Any global phase added to  $|\psi\rangle$  will disappear during measurement. If we define  $|\psi'\rangle = e^{i\theta} |\psi\rangle$  and apply a measurement operator  $M_m$  on  $|\psi'\rangle$ :

$$p'(m) = \langle \psi' | M_m^\dagger M_m | \psi' \rangle = \langle \psi' | e^{-i\theta} M_m^\dagger M_m e^{i\theta} | \psi' \rangle = \langle \psi' | M_m^\dagger M_m | \psi' \rangle = p(m)$$

After the measurement with the operator  $M_m$ , the system state  $|\psi\rangle$  becomes the projection of  $|\psi\rangle$  on  $M_m$  divided by the probability of getting state m:

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}} \quad \text{also often written} \quad \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m | \psi \rangle}}$$

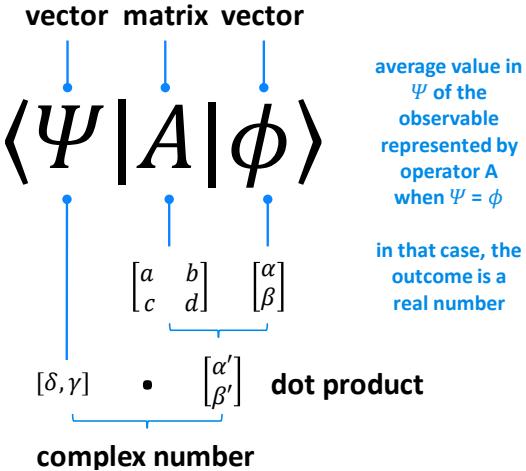
since  $M_m^\dagger = M_m$  (self-adjoint matrix) and  $M_m^\dagger M_m = M_m$  (projector matrix)

<sup>234</sup> Schema source: [A computationally universal phase of quantum matter](#) by Robert Raussendorf (41 slides).

All these measurement equations are part of the measurement postulate (usually the third) from quantum mechanics postulates.

On the right, let's make a pause to understand the  $\langle A | B | C \rangle$  Dirac notation. You usually read it from the right. The ket on the right is a vertical vector that is multiplied by the middle object that is a square matrix. It creates a similar vertical vector. Then, you multiply it with the bra on the left which is an horizontal vector. It is a dot product of an inner scalar product. The result is a complex number and it is a real number when  $\Psi = \phi$ .

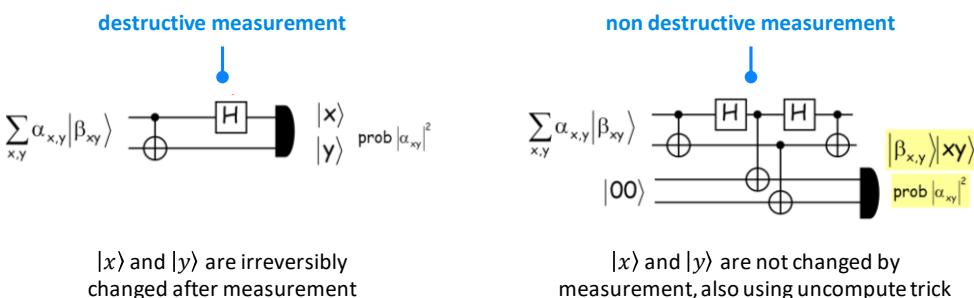
Now, let's be a bit practical.



How can we change the measurement basis with qubits, for implementing a measurement along another axis than Z? At least two options are available:

- It may be possible to *physically* implement a measurement on a different basis than the computational basis. This is, for example, the case with polarization-based photon qubits where the polarizer angle can be dynamically and programmatically modified with some electrically controlled optical settings. It looks more difficult to implement for other types of qubits.
- When the *only* supported measurement is a projective measurement in the computational basis  $|0\rangle$  and  $|1\rangle$ , any another projective measurement can be implemented with first applying a unitary transformation to the qubit that creates a rotation in the Bloch sphere equivalent to moving the measurement axis to the Z axis ( $|0\rangle$  and  $|1\rangle$ ). When we say we do an “X” or “Y measurement”, it means that we first apply a H or  $HS^\dagger$  single gate rotation ( $H$  = Hadamard gate and  $S$  = half a Z gate or quarter phase turn) to handle this axis rotation and then, apply a (computational basis) Z-axis measurement. This is what is regularly done with quantum error correction codes as well as with MBQC (measurement-based quantum computing).

With QECs (quantum error correction codes), this sort of projective measurement is part of the non-destructive measurement technique, applied to ancilla qubits, these additional qubits that detect errors in entangled computing qubits. So, when physicists say they are doing a measurement on a basis of two orthogonal vectors, they mean they are applying first a unitary transformation and then a measurement on the computational basis.



## Qubits register measurement

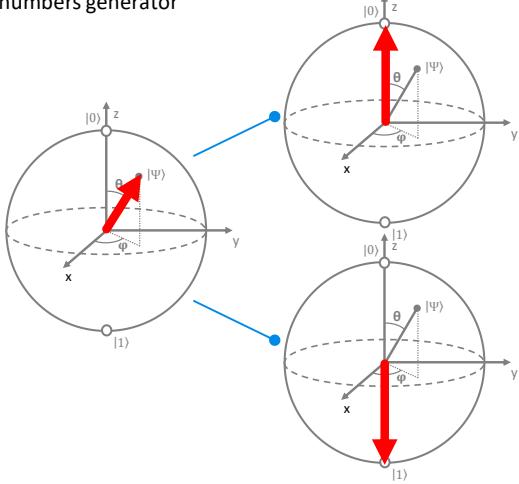
So far, we've just elaborated on measurement mathematical underlying tools and dealt with only one qubit. How about measuring a whole qubits register?

A N qubits register has  $2^N$  possible computational basis states, from  $|00\dots 00\rangle$  to  $|11\dots 11\rangle$ . When measuring once a qubit register, you get one of these states, being a combination of N 0s and 1s.

You could stop there and think, that's my result, fine, done! Well, no! Since the measurement outcome is probabilistic and prone with errors, you need to run your algorithm a certain number of times and count the number of times you'll get each computational basis state. If doing so a great number of times, you'll end up recovering a probability distribution for each computational basis state and reconstruct a full state vector. But to do that, you'll need to execute your algorithm an exponential number of times with regards to the number of qubits, losing any gain coming from quantum computing.

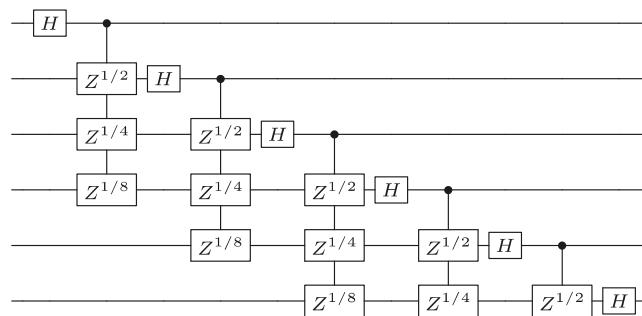
#### a single qubit measurement is probabilistic

i.e.: a qubit register after a Hadamard gate applied to all qubits is a simple random numbers generator



#### on a practical basis:

- the algorithm is executed many times, up to 8000 for IBM Q Experience
- an average of qubits results is computed, producing a real number
- the averaged result is theoretically deterministic
- modulo the error generated by noise and decoherence



x1000 to x8000 shots required in NISC computers

The process you'll implement will depend on what data you want to extract from your prepared qubits register and the run algorithm. Usually, a quantum algorithm is supposed to generate a simple computational basis state (one given combination of 0s and 1s) and not a combination of several states and their respective probabilities.

You can then run several times your algorithm and compute the average values of each qubit, giving a % of 0/1 for each then round up to the nearest 0 and 1. And there you are. What is “several” ? It depends. IBM proposes to run your algorithm a couple thousand times on its cloud Q Experience platform with 5 to 65 qubits and states that this number will grow with the number of qubits, we hope linearly. I have not yet found the rule of thumbs used to define the number of runs, or “shots”.

All in all, you have to remember that one run of our algorithm is non-deterministic and with many runs, you'll converge progressively to a deterministic solution being the average of all runs results.

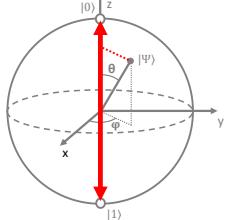
**measurement** is using a collection  $\{M_m\}$  of operators acting on the measured system state space  $|\Psi\rangle$ , with probability of  $m$  being:  $p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$

system state after measurement becomes:

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}} \quad \text{with:} \quad \sum_m M_m^\dagger M_m = I$$

a measurement is **projective** if all measurement operators or projectors  $M_m$  are satisfying  $M_m^2 = M_m$ , aka « idempotency »

a classical projective measurement is a projection of the qubit vector on the z axis



the z basis is qubit's **computational basis**:

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

probabilities  $p(0) = |\alpha|^2 \quad p(1) = |\beta|^2$

state after measurement  $\frac{\alpha}{|\alpha|} |0\rangle = e^{i\phi} |0\rangle \quad \frac{\beta}{|\beta|} |1\rangle = e^{i\phi} |1\rangle$

removed global phase

when **another basis projection** is required like x or y axis in the Bloch sphere, gates are applied to the qubit that change the qubit basis. we then measure qubits using the  $|0\rangle$  and  $|1\rangle$  basis.

for example, if we want to make a qubit measurement on the  $|+\rangle$  and  $|-\rangle$  basis, we first apply a X rotation on the qubit and then do a measurement in the  $|0\rangle$  and  $|1\rangle$  basis.

it enables **non destructive measurement** for the initial qubit and is used in most error correction codes that we'll see later.

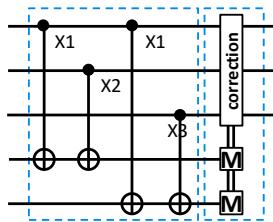
## From computational vector state to full state tomography

What are we measuring? A single computational state, a statistical weight of 0 and 1 or a full vector state? It depends on the algorithm and also on the actual technical need of the undertaken measurement.

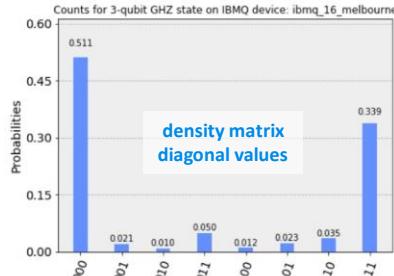
For most algorithms, a series of runs and qubit measurement and their average will output after roundup the found computational basis state.



qubits are measured at the end of computation on each qubit computational basis, several times and averaged: in the general case when the algorithm must generate a pure state.



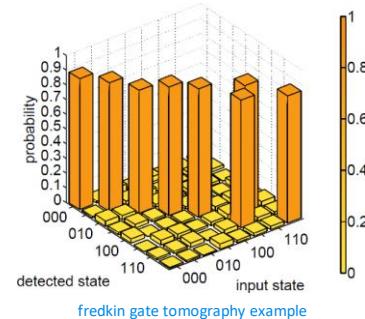
projective measurement on another basis (after X, Y, Z, Rx, Ry or Rz gates): such as with error correcting codes



an histogram with a  $2^N$  probability split of qubits registers computational basis => useful when the algorithm result combines several states, mostly in the middle of an algorithm for debugging purpose.

at the end of computing, we are supposed to have only one bar with a value close to 1, which is easier to measure with a simple measurement method.

this histogram is possible to compute only for a reasonable number of qubits because of its exponential quantum computing cost.

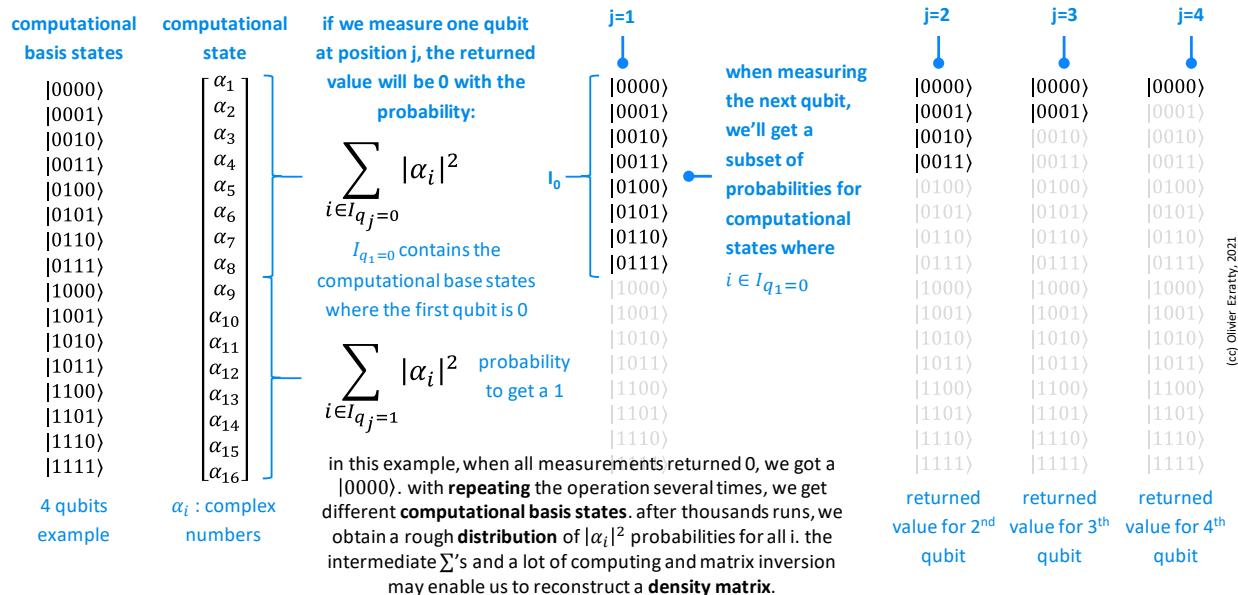


a quantum state tomography is a richer visualization with the full system density matrix => used to assess the quality of qubit gates, entanglement and measurement. more complicated to generate (more repeat projections/measurement). tomography is usually possible for a number of qubits  $\leq 6$ .

For algorithms debugging with a reasonable number of qubits and for characterizing the quality of a small group of qubits, it may be useful to compute either a histogram of the whole computational state vector or even, a so-called quantum state tomography which will reconstitute the density matrix of the quantum register.

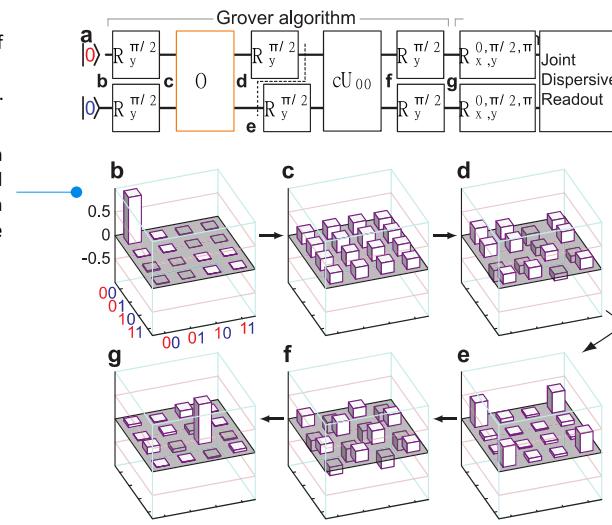
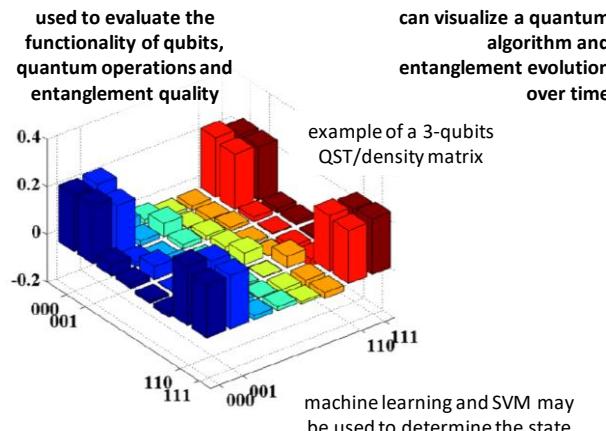
The computational state vector is assembled with a lot of repeat runs and measurements with a number growing exponentially with the number of qubits. It will eventually provide the statistical distribution of each and every computational basis states. Since the number of runs grows exponentially, you understand quickly why it won't make sense to use this technique when we'll exploit a large number of qubits.

Development tools like IBM Q Experience dumps the vector state of your qubits only for helping you learn about how their system work and also understand the impact of noise and decoherence.



Reconstituting the whole system density matrix is a more tedious process. In the most basic technique used, we are keeping track of all intermediate measurements leading to getting the computational state vector and some matrix inversion is required to create it in the end. The process requires even more quantum and classical computation than for reconstituting the computational state vector. This is usually applied with up to 6 qubits, and particularly with 2 qubits to characterize the quality of two qubit gates. A record state tomography of 8 qubits was achieved in 2005 with trapped ions by Rainer Blatt's group in Innsbruck<sup>235</sup>.

**reconstruction of a quantum system density matrix**  
via repeated measurements and statistical analysis of a large number of copies, or done with digital simulation. is using POVM measurement technique and matrix inversion. This is also done at the gate level (GST).



source: Demonstration of Two-Qubit Algorithms with a Superconducting Quantum Processor by L.DiCarlo et al, 2009

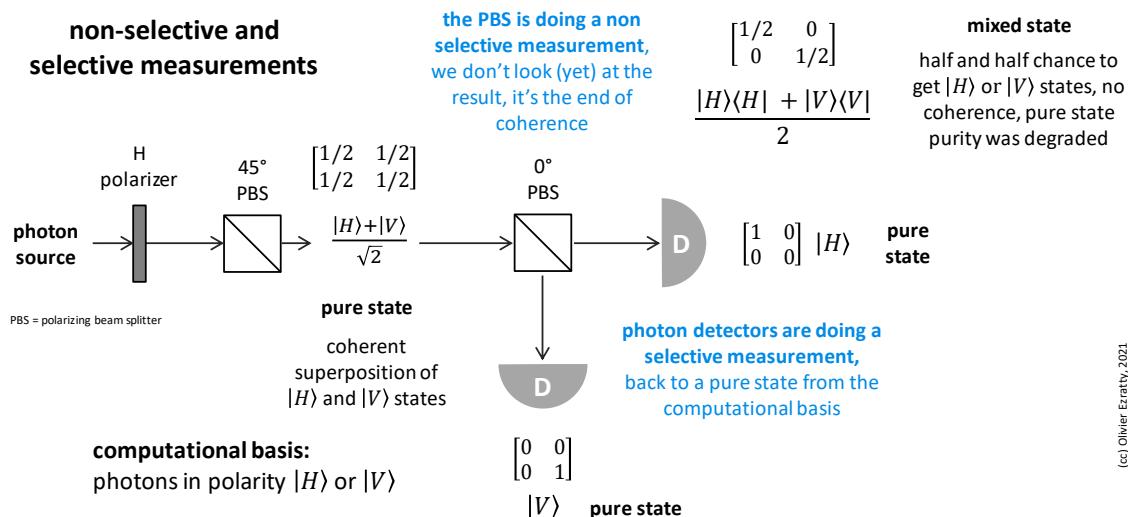
<sup>235</sup> See [Scalable multi-particle entanglement of trapped ions](#) by H. Haffner, Rainer Blatt et al, 2006 (17 pages).

The graphical representation of these density matrices is often used to evaluate the fidelity of two- or three-qubit quantum gates in research publications. The example above illustrates this with comparing the theoretical state of a density matrix for three qubits and two qubits and the result of the measurement<sup>236</sup>. It also helps qualify the quality of qubits entanglement. Various techniques are proposed to speed-up quantum state tomographies and achieve it with a better precision. However, this is a tool for researchers and hardware designers, not for quantum software developers<sup>237</sup>.

The next step is a Quantum Process Tomography which qualifies the quantum channel of a given process, like a series of gates, one gate, or quantum noise and decoherence. It creates an even richer matrix with  $2^{2N}$  columns and rows, representing a linear operator on the system density matrix.

### Non-selective and selective measurements

A non-selective measurement is a measurement that is physically done but not yet read. For any reason, its outcome is not available either because it wasn't yet used or because it's really inaccessible when measurement is done by the environment. How is it different from a real measurement? It deals with the information available about the quantum states we are evaluating. This is explained in the example below using photons polarization and relates with pure states and mixed states.



A single photons source generates photons that traverse first a horizontal polarizing filter and then a 45° polarizing beam splitter (PBS). The PBS create a pure state coherent superposition of  $|H\rangle$  and  $|V\rangle$  states (horizontally and vertically polarized photons). Then, this coherent superposition traverses a 0° PBS. The outcome can be measured in the two PBS exits with single photon detectors. Before being measured, this output is a mixed state of  $|H\rangle$  and  $|V\rangle$ .

There is no more coherent superposition (exit the pure state) and we don't know yet what both detectors will read. But we know that there's a 50% chance that the detector on the PBS horizontally polarized exit will detect a photon and 50% for the other detector. After detection, we'll end up with finding a single photon on one of the detectors, giving a related pure state. And nothing for the other.

<sup>236</sup> Source : [Generation of multiphoton entangled quantum states by means of integrated frequency combs](#), 2016.

<sup>237</sup> See for example [Quantum process tomography via completely positive and trace-preserving projection](#) by George C. Knee et al, UK, 2020 (13 pages). But it requires some background knowledge!

This means that after measurement of a qubit in a given basis, the coherences in its density matrix in the measurement basis are erased. This happens before looking at any measurement outcomes. In other words, a non-selective measurement of a pure state degrades its purity by turning it into a mixed state.

## Positive Operator-Valued Measurement (POVM)

A Positive Operator-Valued Measure (POVM) is a quantum measure generalizing Projection-Valued Measures (PVMs) which is useful when the measurement basis is not made of orthogonal states in their Hilbert space. It is of particular interest when measuring a photon qubit in a telecommunication link with two non-orthogonal polarization basis ( $0^\circ$  and  $45^\circ$  like in the BB84 protocol). Like in PVMs, the measurement operators of a POVM add up to identity matrix. POVMs are also interesting when measuring a subsystem of an open system.

POVMs that are not PVMs are called non-projective measurements. They have many use cases like enhancing quantum states tomography, help detect entanglement and allow unambiguous state discrimination of non-orthogonal states, with applications in quantum cryptography and randomness generation<sup>238</sup>.

## Other Measurements concepts

I'll cover here other measurement-related tools and concepts I have encountered in various courses and scientific papers. You probably don't need to understand this if you are just a quantum software developer. It may be interesting, however, if you are involved in designing quantum systems, error correction systems, measurement systems, quantum firmware and the likes.

**Gentle or Weak Measurement.** It is one type of quantum measurement that retrieves little information of the measured system in average with the benefit of only slightly disturbing it. In a weak measurement, the correlations in the off-diagonal values of the system density matrix are only slightly altered. The system purity and entanglement remain mostly unaltered.

**Postselected Measurement.** It is a measurement where the result is chosen by the user, usually after a weak measurement. Surprising! As all measurements, it also turns a pure state into a mixed state. It refers to the process of conditioning on the outcome of a measurement on some other qubit values. The process consists in throwing away any outcome which does not allow you to do what you want to do. If the outcome you are trying to select has probability  $0 < p < 1$ , you will have to try an expected number  $1/p$  times before you manage to obtain the outcome you are trying to select. If  $p=1/n$  for some large integer  $n$ , you may be waiting a very long time.

This weird technique is noticeably used to better understand quantum physics and phenomenon like measurement non-commutativity<sup>239</sup>.

**CPTP map.** A Completely Positive and Trace Preserving map also referenced as a quantum channel is used to describe non-selective measurements, conditional expectations and quantum filters, as well as feedback networks in quantum control theory. It corresponds to the most generic operation that can be applied to a quantum system. The state of the target system is associated to a trace-one, positive semidefinite density operator and, under the assumption that no initial correlations are present with the environment, its evolution over some specified time interval is described by a completely positive, trace-preserving (CPTP) linear map.

---

<sup>238</sup> See [Understanding the basics of measurements in Quantum Computation](#) by Nimish Mishra, 2019. But what is  $\delta_{mm'}$  in these formulas? It is the Kronecker Delta function which is equal to 0 when  $m \neq m'$  and equal to 1 when  $m = m'$ . Meaning that inner product of all measurement operators is equal to 0 when they are different. This is the definition of orthonormality between a set of operators.

<sup>239</sup> See for example [Quantum advantage in postselected metrology](#) by David R. M. Arvidsson-Shukur, Seth Lloyd et al, Nature Communications, 2020 (9 pages).

For open quantum systems, however, the interaction between the system and environment leads to non-unitary evolution of the system (e.g., dissipation), which requires CPTP maps for full characterization<sup>240</sup>.

In other words, a CPTP map is the mathematical operation that transforms the density matrix  $\rho$  of a quantum system during a measurement on the basis  $|m_k\rangle$  into the density matrix  $\rho'$  as described on the right.

$$\rho' = \sum_k M_k \rho M_k = \sum_k p_k M_k$$

with  $p_k = \langle m_k | \rho | m_k \rangle$

**Quantum Non-Demolition measurement.** It is a type of measurement in which the uncertainty of the measured observable does not increase from its measured value during the subsequent normal evolution of the system. For a qubit measurement, it means that after its measurement, its value won't change anymore in subsequent measurements. QND measurements are the least disturbing type of measurement in quantum mechanics. QND measurements are extremely difficult to implement. Note that the term "non-demolition" does not imply that the wave function fails to collapse<sup>241</sup>. It can be implemented with photons, particularly to measure a photon number (number of photons in a superposed states of similar photon, or a single-mode Fock state), using a secondary probe field interfering with the signal field<sup>242</sup>. It has also been experimented to measure an electron spin with an additional ancilla quantum dot next to an operational quantum dot<sup>243</sup>. It also currently works well with superconducting qubits. What would be a "demolition measurement"? It would be one that, after retrieving the result, would create so significant a back-action on the measured quantum that it would either destroy it (like a classical photon counting device that absorbs the counted photons) or turn it into a state outside the computational basis (such as a different energy level than ground/excited levels for a qubit).

**Quantum Measurement Thermodynamics.** We have already mentioned the theoretical reversible aspect of gates-based quantum computing which relates to the unitary transformations applied with quantum gates. But most of the time, particularly with solid qubits, there is always some energy exchanges between qubits and their control as well as measurement devices. Fundamental research is undertaken to better understand the evolution of the thermodynamic equilibrium of qubit operations particularly during entanglement and also, measurement and error correction. Since measurement is done on a repeated basis due to the implementation of quantum error correction codes, it makes sense to wonder whether this could be optimized. Depending on the qubit state (ground level or excited level, and also in intermediate states), measurement can absorb or release some energy that is quantum and microscopic in nature and it's also powered by entanglement<sup>244</sup>.

<sup>240</sup> Source: [Quantum and classical resources for unitary design of open-system evolutions](#) by Francesco Ticozzi and Lorenza Viola, 2017 (27 pages).

<sup>241</sup> QND was initially introduced in 1975 by VB Braginsky and YI Vorontsov in USSR. Source: [Quantum Nondemolition Measurement](#), Wikipedia. See also [Quantum Non-Demolition Measurement of Photons](#) by Keyu Xia, March 2018. It was demonstrated with the detection of a single photon as described in [Seeing a single photon without destroying it](#) by G. Nogues et al, 1999 (4 pages).

<sup>242</sup> See [Detecting an Itinerant Optical Photon Twice without Destroying It](#) by Emanuele Distante et al, Max Planck Institute, June 2021 (6 pages) which deals with detecting twice a photon with some non demolition quantum measurement. The detectors use a single atom coupled to an optical cavity. Other methods consist in using the cross-Kerr effect where a measured photon traverses an optical medium and changes its refraction index. It provokes a phase shift for a probe photon traversing the same media, its phase being measured with a Mach-Zehnder interferometer. See a description of this old technique in [Quantum non-demolition measurements in optics](#) by Philippe Grangier, Juan Ariel Levenson and Jean-Philippe Poizat, 1998 (7 pages).

<sup>243</sup> See [Quantum non-demolition readout of an electron spin in silicon](#) by J. Yoneda et al, Nature, 2020 (7 pages).

<sup>244</sup> See also [Probing nonclassical light fields with energetic witnesses in waveguide quantum electrodynamics](#) by Maria Maffei, Patrice Camati and Alexia Auffèves, September 2021 (6 pages) which studies the thermodynamics of a qubit coupled to a waveguide, which relates well to superconducting qubit gates and readout operations but also other qubit operations (photons, cold atoms). They demonstrate that the work performed by a coherent pulse on the qubit is always larger than the work that can later be extracted from the qubit, aka its ergotropy. But this classical ergotropy bound is violated if the input field is a resonant single-photon pulse. This opens the door to some energy recovery at the end of computing.

This research field could lead to a better understanding of the whereabouts of the energetic footprints of quantum measurement and entanglement and how it can impact the energy cost of quantum computing, particularly as it scales up<sup>245</sup>.

**Quantum Reservoir Engineering** is a set of qubits management techniques using a quantum bath in order to reduce its energetic footprint, its measurement readout times and enable quantum non-demolition measurement<sup>246</sup>. It's about tightly controlling the qubit coupling with its environment. It is connected to quantum error correction techniques. The approach was initially imagined for NMR qubits, leveraging the Nuclear Overhauser effect. Then it was tested with trapped ions, using some coupling between the qubit harmonic oscillator and a reservoir of oscillator with laser radiations<sup>247</sup>. The technique is also branded "quantum bath", "engineered dissipation", "autonomous feedback" and "coherent feedback". It has since been tested with superconducting qubits and is the basis of the cat-qubits from Inria, Alice&Bob and Amazon<sup>248</sup>.

**Algorithmic Cooling** is a related technique also named heat-bath algorithmic cooling, which consists in balancing the entropy transfers between qubits and with ancilla qubits as part of error correction codes<sup>249</sup>. It is used to improve the purity of a target subset of qubits quantum states in a qubits register.

---

<sup>245</sup> The thermodynamics of quantum measurement is involving a few groups worldwide including the team of Alexia Auffèves from Institut Néel in Grenoble, France, IQOQI and the University of Innsbruck in Austria and Andrew Jordan's team at the University of Rochester, USA. See [A two-qubit engine powered by entanglement and local measurements](#) by Ingrid Fadelli, April 2021 which refers to [Two-Qubit Engine Fueled by Entanglement and Local Measurements](#) by Léa Bresque, Andrew Jordan, Alexia Auffèves et al, March 2021, PRL (5 pages), [Alternative experimental ways to access entropy production](#) by Zheng Tan, Alexia Auffèves, Igor Dotsenko et al, May 2021 (15 pages) and the colloquium [A short story of quantum and information thermodynamics](#) by Alexia Auffèves, March 2021 (14 pages). See also [Stochastic Thermodynamic Cycles of a Mesoscopic Thermoelectric Engine](#) by R David Mayrhofer, Cyril Elouard, Janine Splettstoesser and Andrew Jordan, October 2020 (18 pages) and [Thermodynamics of quantum measurements](#) by Noam Erez, 2018 (3 pages).

<sup>246</sup> Quantum Reservoir Engineering must not be confused with Quantum Reservoir Computing which is an entirely different beast. Introduced by Keisuke Fujii and Kohei Nakajima in 2017, it is the quantum equivalent of a similar technique used in classical deep learning where a low-dimensional data input is projected onto a higher-dimensional dynamical system, the reservoir, generating transient dynamics that facilitates the separation of input states. It is particularly useful to analyze time series of complex data structures. See [Quantum reservoir computing: a reservoir approach toward quantum machine learning on near-term quantum devices](#) by Keisuke Fujii and Kohei Nakajima, November 2020 (13 pages).

<sup>247</sup> See [Quantum Reservoir Engineering](#) by J.F. Poyatos, J.I. Cirac and Peter Zoller, 1996 (14 pages) and the associated presentation [Quantum Reservoir Engineering](#) by Peter Zoller, 2013 (86 slides).

<sup>248</sup> See [Measurement, Dissipation, and Quantum Control with Superconducting Circuits](#) by Patrick Michael Harrington, 2020 (154 pages), [Reservoir engineering using quantum optimal control for qubit reset](#) by Daniel Basilewitsch et al, 2019 (13 pages), [Reservoir \(dissipation\) engineering and autonomous stabilization of quantum systems](#), Quantic team, Inria, 2018 and [Quantum reservoir engineering and single qubit cooling](#) by Mazyar Mirrahimi, Zaki Leghtas and Uri Vool, 2013 (6 pages).

<sup>249</sup> See [Novel Technique for Robust Optimal Algorithmic Cooling](#) by Sadegh Raeisi, Mária Kieferová and Michele Mosca, June 2019 (10 pages).

## Gate-based quantum computing key takeaways

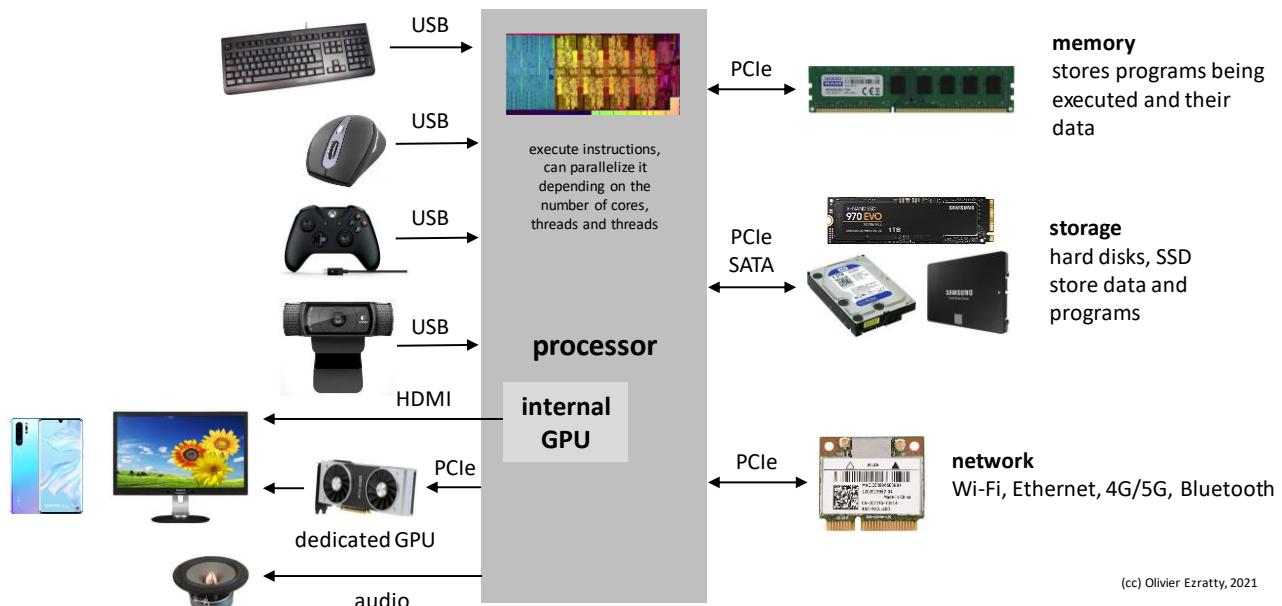
- Gate-based quantum computing is the main quantum computing paradigm. It relies on qubits and finite series of quantum gates acting on individual qubits or two and three qubits. The other paradigms belong to analog quantum computing and include quantum simulators and quantum annealers.
- To understand the effect of qubits and quantum gates, you need to learn a bit of linear algebra. It deals with Hilbert vector spaces made of vectors in highly multidimensional spaces, matrices and complex numbers. The Dirac Bra-Ket notation helps manipulate vectors and matrices in that formalism.
- A qubit is usually represented in a Bloch sphere, reminding us of the wave nature of quantum objects during computation. This wave nature is exploited with qubits phase control and entanglement which provokes interferences between qubits. Qubits entanglement is created by conditional multi-qubit gates like the CNOT.
- A qubits register of N qubits can store a linear superposition of  $2^N$  basis states corresponding to the qubits computational basis, each associated with a complex number.
- While the computational space grows exponentially with the number of qubits, a qubit register measurement at the end of quantum algorithms yields only N classical bits.
- Computation must usually be done a great number of times and its results averaged due to the probabilistic nature of qubits measurement.
- Qubits measurement can be done in various ways, the main one being a classical projective measurement. Other techniques are used that are useful for qubits quality characterization and for quantum error corrections.

# Quantum computing engineering

After reviewing the basic principles of quantum physics and the logical dimension of gate-based quantum computing, let's look at the operational and physical operations of a quantum computer<sup>250</sup>.

Quantum computer architectures depend closely on the characteristics of their qubits. In this section, we will rely on the most common universal quantum gate computer architecture, that of superconducting qubits based on the Josephson effect. It is notably used by IBM, Google, Intel, Rigetti and IQM. However, many of the architectural principles mentioned here are applicable to quantum computers using other types of qubits.

First and as a reminder, here are the main components of a classical computer that you also find in various shapes and forms in smartphones, tablets, personal computers, game consoles and servers. Its key component is its microprocessor. It retrieves data and programs from a storage system and copies them to memory (RAM) entirely or on the fly as needed. The microprocessor then reads the program's instructions from memory in its cache to execute it one after the other and use conditional branching.



Data and programs can be retrieved remotely over a network and from remote servers on the Internet. The whole system is controlled by physical interfaces at input (keyboard, mouse, touchpad, joystick, webcam, microphones, scanners) and generates output (displays, audio, printers, other peripherals). The processor can be complemented by a graphics processor (GPU). It is either external to the microprocessor, for demanding requirements such as in CAD or for video games, or integrated into the microprocessor as is the case for all most laptops and most desktops processors.

Depending on the configuration, the processor is surrounded by a variable number of external components that are soldered in the motherboard.

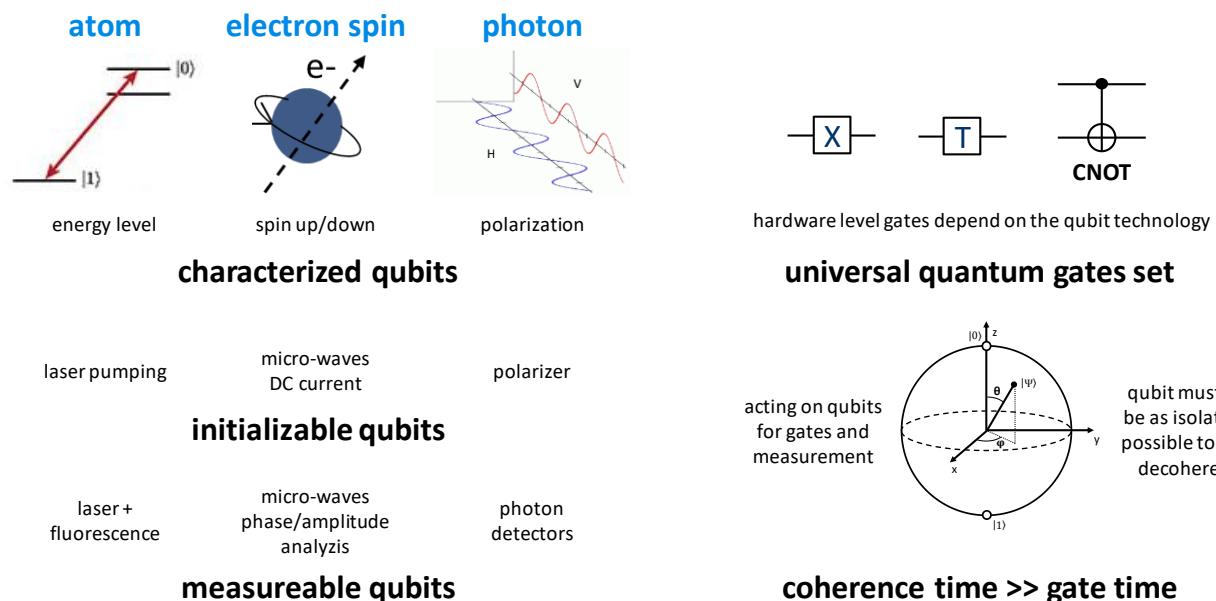
<sup>250</sup> I consulted a very large number of information sources to carry out this part, both on the research side and on the supplier side, such as IBM or D-Wave. Note [Quantum Computing Gentle Introduction](#) from MIT, published in 2011 (386 pages) which describes precisely some mechanisms of quantum computers such as qubit state reading methods. It also describes quite well the mathematical foundations used in quantum computers. You can also enjoy an [8-minute video](#) from Dominic Walliman, who explains the basics of the quantum computer!

This is the case of the Intel chipsets like the Z390, which complements the core processors and manages a large part of the computer's inputs/outputs. Wi-Fi and cellular modems are associated with antennas. Of course, an internal and external power supply and a battery for mobile devices must be added.

On the energy side, it is the processor and GPU that heat up the most and require passive or active cooling depending on their power drain. In embedded systems such as smartphones, this is done with heat conducts and air. In PCs, it is supplemented by one or more fans. In the most extreme cases, liquid cooling uses a water circuit to improve heat dissipation. One of the reasons why heat is generated by classical processing is the non-reversibility of classical computing.

## Key parameters

Let's look at the definition of the key performance indicators of gate-based quantum computers. The best-known set of indicators was created by **David DiVincenzo** in 2000 when he was an IBM researcher. He is now a research professor at the University of Aachen in Germany<sup>251</sup>.



While individual qubits barely existed, he defined the basic technical characteristics of a universal gate-based quantum computer as follows:

**Well-characterized qubits.** Quantum computers use qubits that exploit quantum objects that can have two distinct and measurable states. Their physical characteristics are well known. The architecture is scalable in the sense that it can exploit a large number of physical qubits and then, logical qubits.

**Initializable qubits.** In general, to the value  $|0\rangle$  often called "ground state" for the associated quantum objects, corresponding, for example, to the lowest energy level of an elementary particle or an artificial atom as for superconducting qubits.

**Coherence times.** It must be greater than quantum gates activation times. The time during which the qubits are in a coherent state must be greater than the quantum gates activation time in order to be able to execute an algorithm containing a sufficiently long sequence of quantum gates. Error correction codes using a large number of physical qubits have the benefit of extending this usable computing time.

<sup>251</sup> See [The Physical Implementation of Quantum Computation](#) by David P. DiVincenzo, 2000 (9 pages).

**Universal quantum gates set.** The quantum hardware must allow the creation of a universal gate set. It depends on the qubit technology. It requires a minimum set of single-qubit gates allowing the creation of any rotation in the Bloch sphere, completed by a CNOT two-qubits gate.

**Measurement.** With the ability to measure qubits state at the end of computing, which seems obvious. This measurement should not influence the state of other qubits in the system. Ideally, the measurement error rate should be well below 0.1%.

David DiVincenzo added two other optional criteria that are used instead for quantum communications:

**Flying qubits conversion.** The ability to convert static qubits into flying qubits, who are usually photons, and sometimes electrons.

**Transport these moving qubits.** from one point to another reliably and remotely. This will allow to manage quantum telecommunications, distributed architectures of quantum computers and to set up *blind computing* architectures allowing to distribute treatments while protecting their confidentiality. The technology will quickly become essential to enable the distribution of quantum computations over several quantum processors, a bit like we do with multi-core chipsets or with processing distribution architectures over several CPUs and several servers. Some vendors like IonQ have announced that they will rely on this architecture. This will be useful for qubit architectures that will be limited in the number of qubits, which may only be able to consolidate a few hundred at most. It will thus be necessary to be able to link remote processor qubits and keep them entangled. Different quantum interconnection techniques are possible. The most generic is optical and is not much constrained by distance. At rather short distances, microwave links are possible, particularly to couple superconducting qubits, as well as shuttling electrons<sup>252</sup>.

DiVincenzo's criteria are quite basic. From a practical and operational point of view, quantum computers can also be characterized by another set of parameters as follows:

**Number of qubits.** It will condition the available computing power. As this power theoretically increases exponentially with the number of qubits, it is a key parameter. As of mid-2021, the commercial record was 65 qubits with the largest IBM Q System available in the cloud. The number of qubits should be evaluated in its capacity to scale. Some technologies are easier to miniaturize and scale than others. It is necessary to integrate in this miniaturization both the quantum qubit chipsets and the elements that control them. On top of that, we must ensure that decoherence and noise does not increase as the number of qubits is growing. Today, trapped ions qubits have an excellent fidelity but don't scale well. Superconducting qubits seem to scale-up better but their fidelity is not stable as the number of qubits grows. Cold atom qubits scale a little better but with some practical limits in the number of controllable atoms. Electron spins qubits could scale best in theory.

**Qubits connectivity.** It will condition the quantum algorithms execution speed. The greater this physical connectivity, the faster the code execution will be. With a low connectivity, the compiler of the quantum code will have to add a lot more operations to link the qubits together, particularly relying on SWAP gates. This connectivity varies greatly from one technology to another. In 2D technologies, as with superconducting and silicon qubits, it is limited to neighboring qubits. It seems better with some types of trapped ion qubits.

**Qubit parallel operation.** How qubit gates can be parallelized over different qubit zones without disruption will also condition the speed of execution of quantum algorithms.

---

<sup>252</sup> Princeton University and Konstanz University in Germany are working on optical interconnection between CMOS quantum processors. This is documented in [Quantum Computing Advances With Demo of Spin-Photon Interface in Silicon](#), 2018. The magic consists in transferring the quantum state of an electron spin to a photon at its phase level.

**Qubits fidelities.** When executing quantum gates and reading their state, qubit fidelity conditions the ability to execute long algorithms. It has a direct impact on the supported algorithm depth. It also impacts the capacity to run quantum error correction codes and create logical qubits with an arbitrary fidelity level.

**Execution time.** For both quantum gates and qubit state measurement. The first is obviously important to make the algorithms run as fast as possible. But the second is equally important because it is involved in error correction codes and therefore conditions the execution time of all algorithms.

**Operating temperature.** For the processor and their equipment which is very dependent on the type of qubits. The Holy Grail is of course to operate at room temperature. The currently operational quantum computers based on superconductors operate at a very low temperature of 15 mK (1 mK = 1 milli-kelvin, 0 kelvin = -273.15°C), but some types of qubits still in the research stage are supposed to operate at room temperature, such as those based on photons and NV centers (cavities in nitrogen-doped diamond structures). However, this is not necessarily the case for associated equipment such as photon generators and detectors for photon qubits. Operating at very low temperature is a way to preserve the coherence of the qubits. But the lower the temperature, the smaller the energy that can be radiated by the qubits and their control electronics. Operating qubits at 100 mK or 1K, like with electron spin qubits, creates a much larger available cooling budget to control the qubits than operation at 15 mK.

**Total energy consumption.** We will investigate this and study it in a global manner with incorporating all quantum computer components: the processor itself, all its control electronics as well as the involved cryogenic systems.



**System rackability.** How will quantum computers be deployed in data centers? Does it fit in standard rack systems? It is notably planned by the startup Pasqal, as well as for Quandela's photon generators and LightOn's optical processors, as well as micro-wave external electronics from companies like Zurich Instruments and Qblox. Alpine Quantum Technologies from Austria also announced in 2021 it would fit its trapped ion computing in two standard 19 inches racks. It is associated with issues of weight, space, cooling and power supply. What kind of fluids must be used for cooling, usually cold water, connected to the first stage compressor of cryostats, whatever their size? Quantum computers must also withstand the usual data centers conditions like vibrations, dust and electromagnetic environment, or be separated in special isolated facilities. They could site in the modular building blocks used in the most recent data centers.

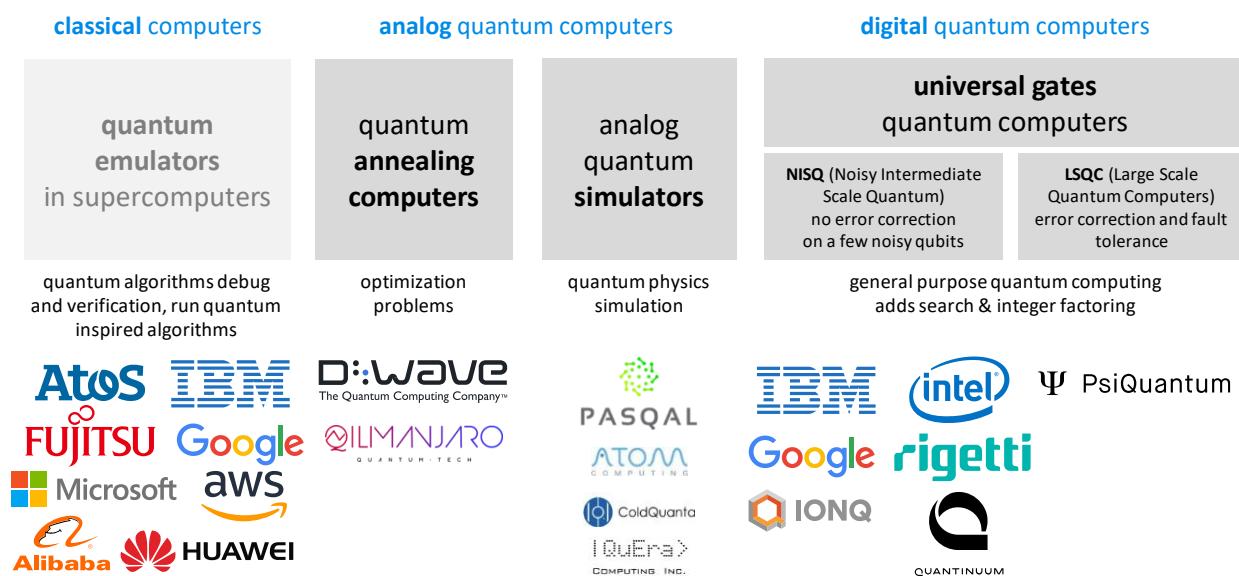
These last three operational parameters play a role when deploying computers or quantum accelerator in data centers. It plays a critical role since, for most applications, quantum computers will be offered through cloud services.

All these considerations to gauge the capabilities of a quantum computer involve the discipline of quantum computers benchmarking! As Kristel Michielsen points out, benchmarks can be used when the number of qubits is below 50 when comparing the rendering of algorithms between quantum computers and their emulation on supercomputers<sup>253</sup>. Beyond that, it will be more difficult.

Benchmarked quantum computers will generally have dissimilar characteristics: different universal quantum gates requiring compilers to assemble different quantum gates to execute the same algorithm, and different error correction codes, adapted to the error rate of the qubits and quantum gates of the compared computers. The dissimilarities will be much greater than between two Intel and AMD processors or two smartphone chipsets!

## Quantum computers segmentation

There is not just one category of quantum computers, but many. We must at least distinguish gate-based quantum computers and analog computers, including quantum annealing computers such as the ones from D-Wave.



(cc) Alexia Aufvèves et Olivier Ezratty, December 2021

But there are at least six categories of quantum computers:

**Quantum emulators.** These are used to execute quantum algorithms on traditional computers ranging from simple laptops to supercomputers, depending on the number of qubits to be emulated. They execute these algorithms, quantum gates and qubits with the processing capabilities of traditional computers, using large vectors and matrices. It is used to test quantum algorithms without quantum computers. Quantum emulators are sometimes called quantum simulators, but this name should be avoided to prevent the confusion with... quantum simulators. These are analog quantum computers simulating quantum physics phenomena, for example magnetism or the tridimensional structure of molecules. Quantum emulators can also reproduce the physical characteristics of various qubits. That's what the Atos QLM emulator do<sup>254</sup>.

<sup>253</sup> In [Benchmarking gate-based quantum computers](#), 2017 (33 pages).

<sup>254</sup> We can make a distinction between an exact digital simulation and approximate digital simulation, emulating a digital error rate that is equal or below NISQ hardware. This can help simulate a greater number of qubits.

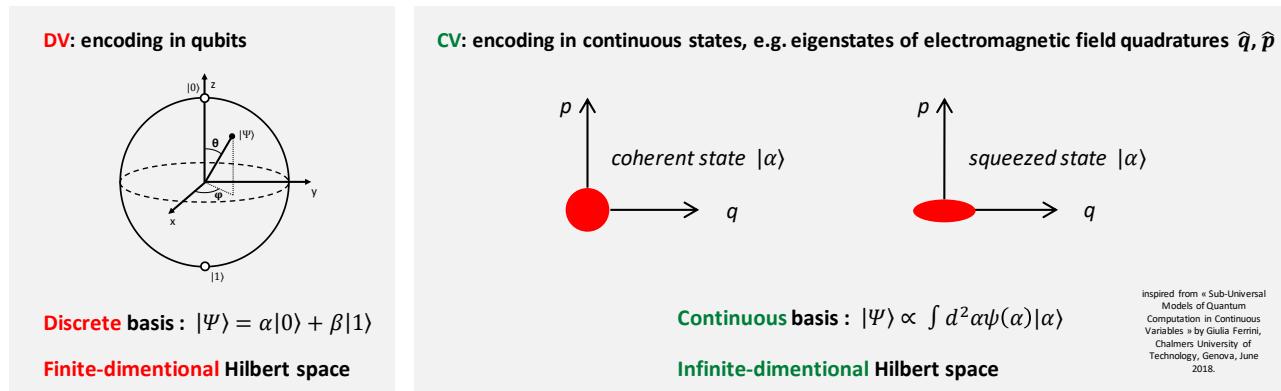
To date, supercomputers can emulate up to the equivalent of 40 to 50 qubits, but records have been broken with more than 100 qubits, with a low number of quantum gates. Emulating quantum computers requires a lot of power both on the memory side, to store  $2^N$  quantum register states for N qubits, if not the full  $2^{2N}$  real numbers of the density matrix, and for the associated processing that relies on floating-point matrix multiplications. Still, records in this field are regularly broken.

**Quantum annealing computers** from D-Wave or Qilimanjaro. They are based on low-quality qubits. The technique is using a slow and controlled evolution of a set of qubits linked together with vertices in qubit "chimera". It is initialized in a state close to the solution and the system converges towards the solution, which is often the result of the search for a minimum of energy, such as for the simulation of atomic interactions in molecules or the optimization of the duration of a complex path. The variables are the weights of the connections between qubits and the unknown to find are the spin of each qubit. Many optimization and quantum simulation algorithms can be translated into quantum annealing algorithms. So far, D-Wave seems to bring some interesting computing time gains but this is highly contested by some specialists.

**Quantum simulators** serve as simulators of quantum phenomena without using gates-based qubit systems. They work in an analog and not digital way, i.e. the parameters linking the qubits together are continuous. For the moment, they are mainly laboratory tools. The most commonly used technique are cold atoms cooled and controlled by lasers, like the ones from Pasqal, ColdQuanta and Atom Computing. Trapped ions and other qubit types could also be used in simulators but no commercial vendor is promoting it when they can also implement gate-based quantum computing which is supposed to be more generic.

**Universal quantum computers** use qubits with quantum gates capable of executing all quantum algorithms and with an optimum speed gain compared to supercomputers as well as to adiabatic quantum computers<sup>255</sup>. They are currently limited to 65 qubits. The quantum noise levels of qubits is detrimental to computing and requires the usage of logical qubits made of many physical qubits and quantum error correction codes (QEC). While waiting for these quantum computers to ramp up with logical qubits, we are using non corrected qubits in the so-called NISQ for "Noisy Intermediate-Scale Quantum", an expression from John Preskill<sup>256</sup>. It describes existing and future general-purpose quantum computers supporting 50 to a few hundred physical qubits. They are supposed at some point to exceed supercomputers computing capacities for specific algorithms. Then, much later, we'll have LSQ (large scale quantum computers), with a very large number of physical qubits and over 50 logical qubits compatible with quantum software requirements.

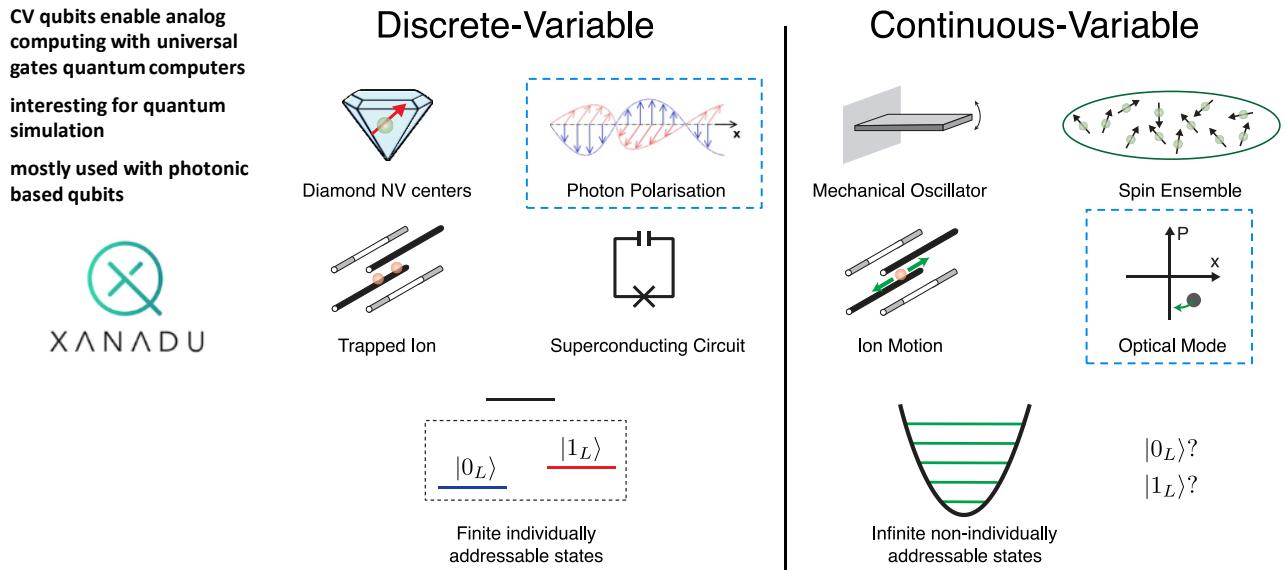
### Direct Variable vs Continuous Variable encoding of quantum information



<sup>255</sup> Here is a quick overview in [Quantum Computing Circuits and Devices](#), April 2018 (18 pages).

<sup>256</sup> In [Quantum Computing in the NISQ era and beyond](#) in 2018.

**Continuous variables quantum computers**, or analog quantum computers with universal gates. They use qubits that store variable quantities between 0 and 1 and can be manipulated with quantum gates, also named ‘qunats’<sup>257</sup>. This category of quantum computing was proposed in 1999 by Seth Lloyd and Samuel Braunstein<sup>258</sup>. They are usually based on continuous variable photons but other qubit types like trapped are used.



**MBQCs**, or Measurement Based Quantum Computers, is an architecture variant of NISQ/LSQ adapted to flying qubits and particularly to photon qubits which can't easily be entangled with two qubits gates. The process consists in entangling all qubits at the beginning of computing. It's followed by qubits readouts in an ordered way, enabling the implementation of traditional gates. MBQC also implements some massive parallelism, adapted to the limited and finite processing depth of flying qubits. The startup PsiQuantum plans to use a variant of this technique named FBQC.

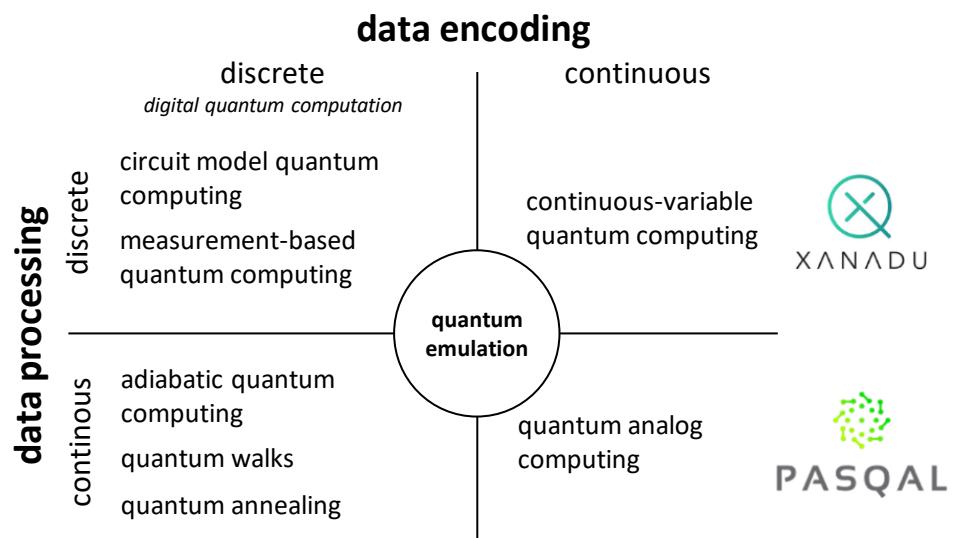
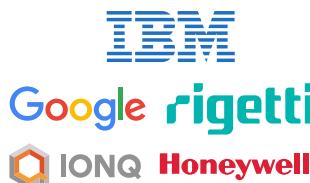
**Topological quantum computing** is based on specific anyon qubits that are self-corrected. The low-level programming model of these qubits is much different from universal quantum computers. This is the path chosen by Microsoft, together with QuTech. Its development seems to be quite sluggish.

Here's another segmentation of these models with two dimensions: discrete or continuous data encoding and discrete or continuous variables computing given the vendor position is rough, some being positioned in various slots (Pasqal also wants to do gate-based computing)<sup>259</sup>:

<sup>257</sup> See [Universal Quantum Computing with Arbitrary Continuous-Variable Encoding](#), 2016 (5 pages, source of one illustration) as well as [Continuous-variable quantum computing in the quantum optical frequency comb](#) by Olivier Pfister, 2019 (16 pages).

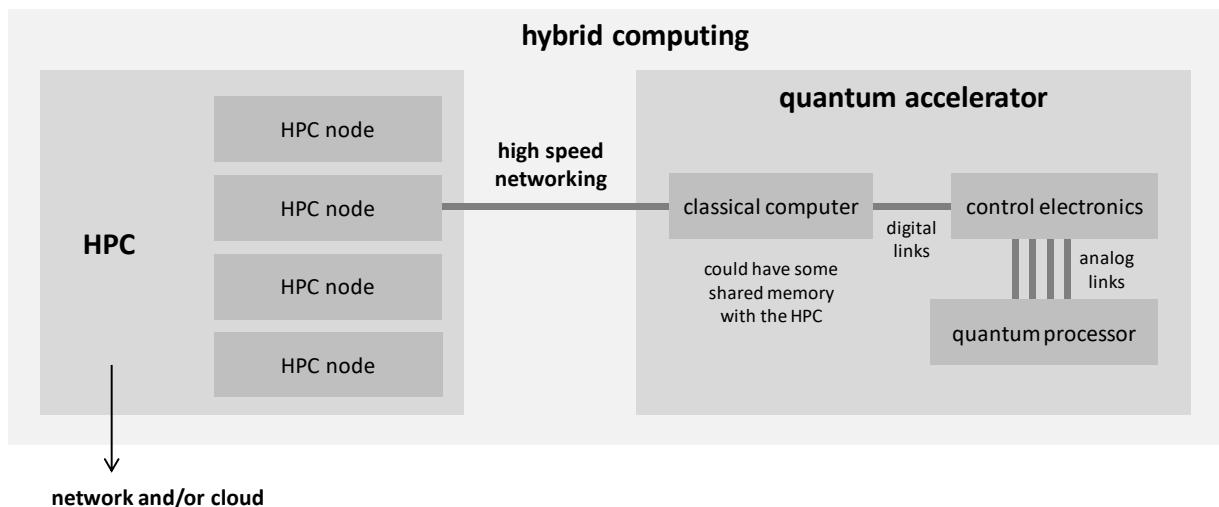
<sup>258</sup> See [Quantum Computation over Continuous Variables](#) by Seth Lloyd and Samuel L. Braunstein, February 1999 (9 pages).

<sup>259</sup> See [Quantum computing using continuous-time evolution](#) by Viv Kendon, 2020 (19 pages) is the source of the chart. I just added some company logos.



based on "Quantum computing using continuous-time evolution" by Viv Kendon, 2020. I just added some company logos.

**Quantum Accelerator.** It is a quantum computer used as a complement to a supercomputer or HPC, usually to run hybrid algorithms like VQE (Variational Quantum Eigensolvers) combining a classical part that prepares the data structure that feeds a quantum accelerator<sup>260</sup>. The QPU serve as an accelerator for the HPC which can be a node or the whole HPC, using CPU and/or GPUs/TPUs. GPUs/TPUs are themselves also accelerators for the CPUs. There are some design issues requiring tight integration between the HPC and the QPU, particularly with regards to batch loading and to the way the quantum algorithm is executed multiple times. A QPU contains itself a classical computer. It converts digital signals (gates) into analog signals (the micro-waves or lasers controlling the qubits and handling their readout). This QPU computer will need to be as close as possible to the HPC computing capacities to improve the turnaround. It may lead to create custom designs integrating an HPC and one or several quantum accelerators<sup>261</sup>. Other quantum accelerator designs contains more or less generic upper software layers with connectors driving various quantum and classical architectures (annealers, gate-based, emulators)<sup>262</sup>.



(cc) Olivier Ezratty, September 2021

<sup>260</sup> See [Quantum Accelerators for High-performance Computing Systems](#) by Keith A. Britt et al, 2017 (7 pages).

<sup>261</sup> See [Quantum Accelerator Stack: A Research Roadmap](#) by K. Bertels et al, 2021 (39 pages) which proposes an detailed architecture for a quantum accelerator.

<sup>262</sup> See for example the proposals in [Quantum Computer Architecture: Towards Full-Stack Quantum Accelerators](#) by Koen Bertels et al, 2019 (20 pages).

This inventory is only an appetizer. We will have the opportunity to detail these architectures.

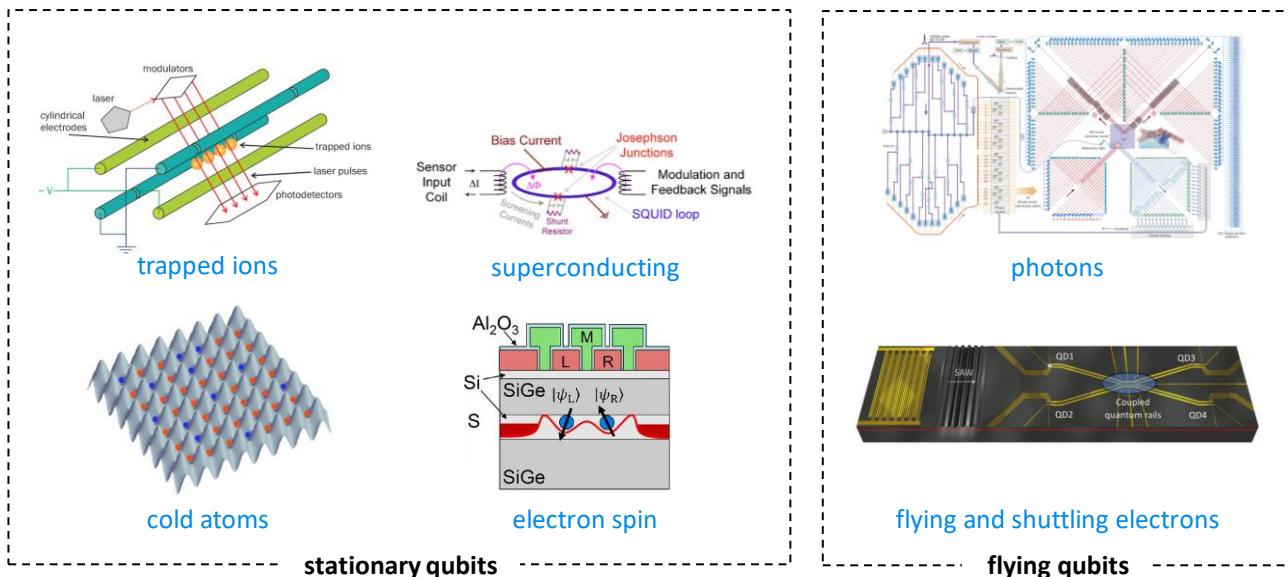
## Qubit types

Quantum computers physical qubits are devices that handle particles or quasiparticles with one physical property or observable that can have two possible mutually exclusive states, that can be initialized, modified with quantum gates and then measured.

They are sometimes unitary elementary particles, as with atoms (trapped ions and cold atoms), electrons (silicon qubits, NV centers, anyons for topological calculations) or photons! And only one at a time! In the case of superconducting qubits, the quantum state is based on a large number of electrons arranged in Cooper pairs that share the same quantum state, the pairs of electrons that are created at superconducting temperature.

Physically, the qubits are of two kinds: stationary or moving (flying). Those based on trapped ions, cold atoms, trapped electrons and superconducting loops are stationary. Flying qubits are based on photons that physically circulate from quantum gate to quantum gate as well as on flying electrons.

In the case of stationary qubits, quantum gates do not move either. They are dynamically activated by electronic circuits or lasers and operate on the qubits.



Here are the main types of qubits that are currently being studied, tested and sometimes commercialized<sup>263</sup>. We'll detail [later](#) all these different options when mentioning the key involved research labs and vendors. Looking at these technologies reminds me of the Wacky Races movie and cartoons vehicles as well as the Tatooine podracers in Star Wars I, with an amazing technology diversity and true believers in their fate. The only difference is we may end up with no single winner but several winners if not some forms of technology hybridization. And Manhattan project? It had only two main uranium and plutonium combustible options and some variations with the explosives.

### Controlled atoms

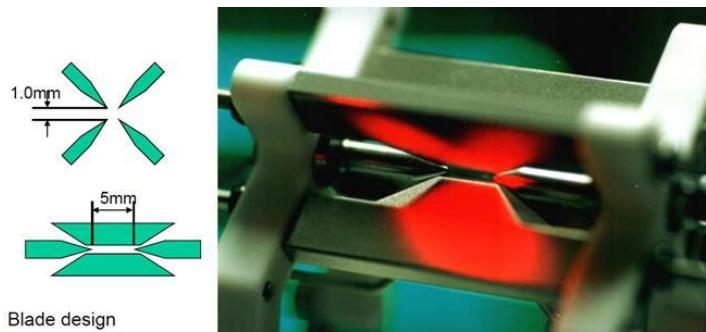
This is one of the oldest types of qubits. It consists in controlling atoms in vacuum with lasers, one qubit per atom. Cold atoms are neutral while trapped ions are ionized atoms.

<sup>263</sup> See [Roadmap on quantum nanotechnologies](#) by Arne Laucht et al, 2021 (49 pages) which reviews some of these qubit types.

One key difference is how these atoms are controlled in space. Ions can be positioned with electrodes and magnetic fields while non-ionized atoms are only controlled by lasers. They both share the measurement technique using laser excitation, fluorescence and visual readout.

**Trapped ions** are atom ions that are kept in a vacuum and suspended by electrostatic suspension. Their initialization is done with laser optical pumping. Lasers are used to cool and stabilize the ions, exploiting the Doppler effect, with different energy transitions than those used to modify the state of the qubits. The most frequently used ions are calcium and strontium.

Single-qubit quantum gates are activated by microwaves, lasers or magnetic dipoles. Lasers or electrodes are used for two-qubit quantum gates. The main vendors in this category are **IonQ**, a spin-off from the University of Maryland, **AQT** (Alpine Quantum Technologies), a spinoff of the University of Innsbruck in Austria and **Honeywell Quantum Systems (Quantinuum)**. While trapped ions are best-in-class for qubits fidelity and connectivity, it seems currently difficult to scale it beyond a hundred ions. And it's very slow.



F. Schmidt-Kaler, et al.,  
Appl. Phys. B 77, 789 (2003).

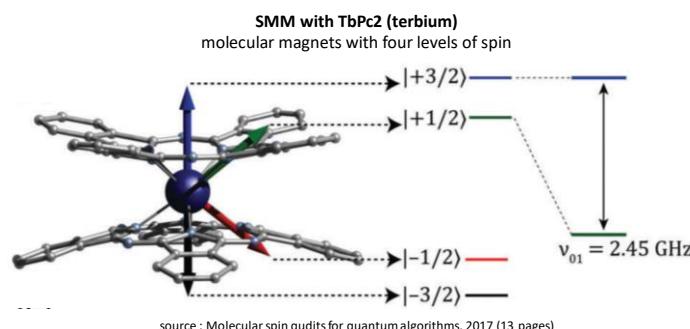
$$\omega_{\text{axial}} \approx 0.7 - 2 \text{ MHz} \quad \omega_{\text{radial}} \approx 5 \text{ MHz}$$

$$\text{trap depth} \approx eV$$

**Cold atoms** are cooled at very low temperatures, also using the Doppler effect. The atoms used are neutral atoms and quite often rubidium, an alkaline metal. The quantum state of these cold atoms is their energy level. Cold atoms are used to create quantum computer qubits with universal quantum gates or analog quantum simulation. Antoine Browayes's team at Institut d'Optique launched initial work in this field starting in 2008. It led to the creation of **Pasqal**. They now control up to 196 atoms. We will examine its activity and technology on page 327. In the USA, **ColdQuanta** is also working on this technology.

**Nuclear magnetic resonance** (NMR) qubits have been tested in the past and nearly completely abandoned because they do not scale at all. It is a good demonstration that the qubits research field has to remain open and cannot be settled too early around one or two technologies. Even now, it's too early to tell which qubit type will really scale to create useful quantum computers.

**Molecular magnets** are being explored, noticeably at the Institut Néel in Grenoble, France. One variant is made with terbium and has four possible spin related quantum levels, creating not qubits but qudits, with  $d=4$ . The small name of these magnets is SMM for Single-Molecule Magnets. The molecule used is TbPc<sub>2</sub> also called bis (phthalocyaninato) terbium(III).



source : Molecular spin qudits for quantum algorithms, 2017 (13 pages)

Their state is measured with a phase-measuring interferometer. Their advantage is their stability. But they are relatively difficult to control<sup>264</sup>.

<sup>264</sup> See [Molecular spin qudits for quantum algorithms](#), 2017 (13 pages). This work was carried out in partnership with the Karlsruhe Institute of Technology in Germany. And also the thesis [Quantum information processing using a molecular magnet single nuclear spin qudit](#) by Clement Godfrin, 2017 (191 pages).

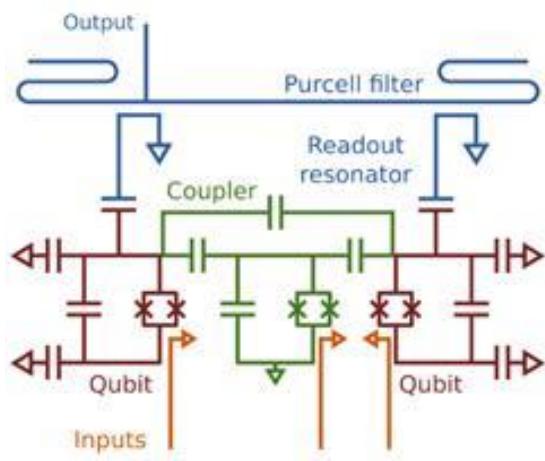
## Controlled electrons

This other category of qubits is about electrons that are controlled most of the time in solid-state circuits instead of vacuum like with cold atoms and trapped ions.

**Superconducting qubits** are based on the state of a superconducting current that crosses a very thin barrier in a loop, usually a metal oxide such as aluminum, using the Josephson effect<sup>265</sup>. There are several types of superconducting qubits: flux, phase and charge.

The most common one is the transmon, a variation of charge superconducting qubits. In all cases, qubit observables are two very distinct states of a high-frequency oscillating current flowing through the Josephson junction.

The oscillation is made possible by the fact that the loop integrates the equivalent of an inductance and a resistance. The current oscillation is activated by the application of microwaves with frequencies between 4 and 8 GHz transmitted by coaxial wires. In transmon qubits, the qubit observable is measured with a resonator integrated in the circuit which receives a microwave and sends it back with some or no phase shift. On the right is a schematic of two superconducting Google Sycamore qubits, themselves connected by a third qubit - in green - which acts as a dynamic coupler between two qubits, to create controlled entanglement.



In some transmons, individual qubits activation frequency is tuned by a direct current flux bias line.

Superconducting qubits are used by **IBM**, **Google**, **Rigetti**, **QCI**, **Intel** and others for universal circuit quantum computing. **Amazon** and **Alice&Bob** are exploring the cat-qubits technique using a cavity with oscillating microwaves, its observable being captured with a transmon qubit.

Superconducting qubits are relatively easy to manufacture because they are based on semiconductor circuit creation techniques even if some of the materials are different, such as niobium and aluminum<sup>266</sup>. They are built on a dielectric substrate, usually with silicium or sapphire. These qubits are operating at 15 mK, requiring dilution refrigeration. This temperature is required for a chain of reasons: qubits being driven by microwaves in the 4-8 GHz range and the current thermal noise being constrained at at least an order of magnitude lower than the temperature corresponding to these microwaves. The 4-8GHz corresponds to off-the-shelf microwave generation equipments and also to the capacitor size in the Josephson junction.

There were many contributors to early superconducting development with Anthony Leggett in the USA, Michel Devoret and Daniel Esteve's team at CEA Saclay and Yasunobu Nakamura in Japan.

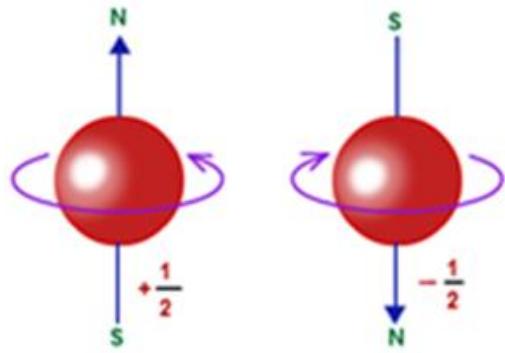
Superconducting qubits have many challenges dealing with scalability. The microwave RF generators are usually located outside the cryogenic enclosure of the quantum processor, which create a lot of wiring with about 3 to 4 cables per qubit. Qubits control frequencies must be different and tuned for adjacent qubits. Their fidelity is not best-in-class and seems to decrease as we grow the number of qubits. But IBM and Google, among others, have plan to build up to one million physical qubits computers, with 100 logical qubits.

<sup>265</sup> See [Digital readout and control of a superconducting qubit](#) by Caleb Jordan Howington, 2019 (127 pages).

<sup>266</sup> See [Practical realization of Quantum Computation Superconducting Qubits](#) (36 slides).

**Electron spin** qubits are developed with scalability in sight. Most of them use two electrons trapped in a quantum well, one containing the qubit and the other one used to measure it.

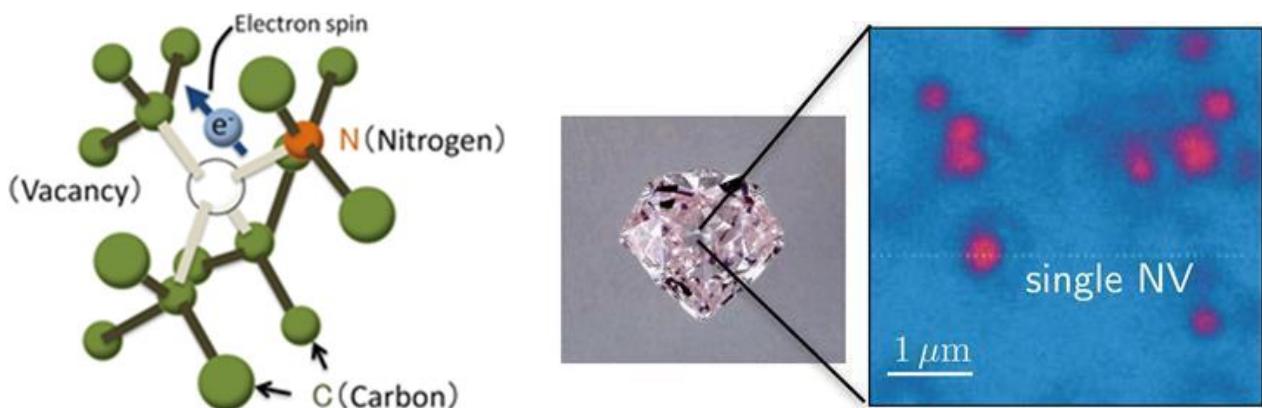
These qubits are usually manufactured using silicon-based CMOS circuits. Silicon is often supplemented with various dopants. They benefit from the reuse of CMOS manufacturing processes that are already well mastered. These qubits are easy to miniaturize down to below 100 nm. They work at temperatures between 100 mK and 1K, higher than superconducting qubits, allowing the use of more electronics around the chipset, to generate the microwaves and other electric signals required to create qubit gates and handle qubit readout.



**Intel** is the largest company invested in electron spin qubits for an obvious reason, being the largest CMOS components manufacturer in the world. You also have **Quantum Motion** (UK), **SQC** (Australia) and the **CEA-Leti** in Grenoble, France.

**NV centers** (Nitrogen Vacancy) are artificial diamond structures in which a carbon atom has been replaced by a nitrogen atom near a carbon atom gap. Qubit states and control rely on a combination of electron, nitrogen and carbon  $^{13}\text{C}$  nucleus spins. Qubit gates are implemented with microwaves, a magnetic field and an electric field. Entanglement is handled with photons, magnetic coupling or with controlling the core spin of neighboring  $^{13}\text{C}$  carbon atoms via the use of microwaves to create a CNOT gate. Qubit readout is using a laser and fluorescence detection.

Defects in diamonds have been studied from 1930 with the examination of infrared absorption. This made it possible to distinguish two categories of diamonds: type I with an absorption band of 8  $\mu\text{m}$  in the infrared and type II without this band. The defects explain the color of diamond gems. It was not until 1959 that these impurities were found to be related to the presence of nitrogen, at 7.8  $\mu\text{m}$  and that nitrogen atoms were well isolated in the diamond crystal. In 1975, it was discovered that some heat treatment could control the diffusion of nitrogen atoms in the diamond. These nitrogen centers explain the diamond color. It has four types: one nitrogen atom isolated in a gap, two nitrogen atoms, three nitrogen atoms surrounding a gap and four nitrogen atoms.

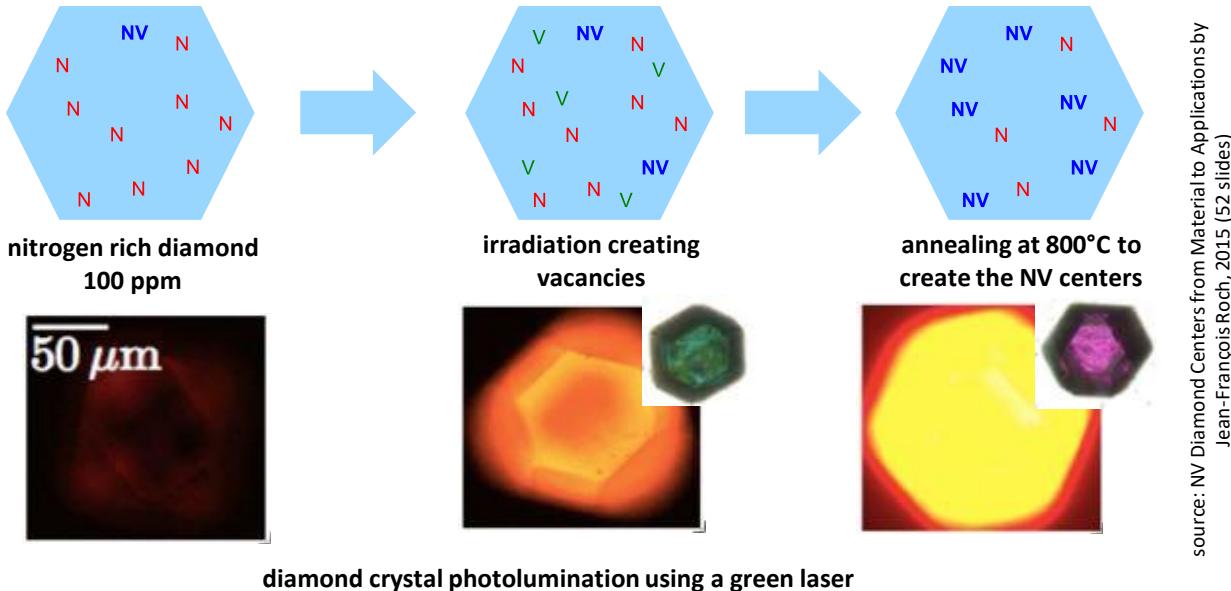


It is the first type that is interesting for both quantum computing and quantum sensing. We can visualize these defects with a confocal microscope (having a very shallow depth of field) by illuminating them with a green laser beam that will generate some red light<sup>267</sup>.

<sup>267</sup> See [Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers](#) by A. Gruber et al, 1997 (4 pages) which is the source of the illustration also seen in the slides by Jean-François Roch.

These NV centers diamonds are slightly pink. These properties make it possible to generate single-photon sources thanks to the isolation of a NV center.

Nitrogen-rich artificial diamonds are used to manufacture these NV centers. Gaps are generated with irradiation. Vacuum annealing at about 800°C-900°C moves the vacancies next to the nitrogen atoms in the crystal structure<sup>268</sup>. This is explained by nitrogen atoms being as large as carbon atoms. The gap creates a small bar of electrons that serve as a virtual magnet via their spin.

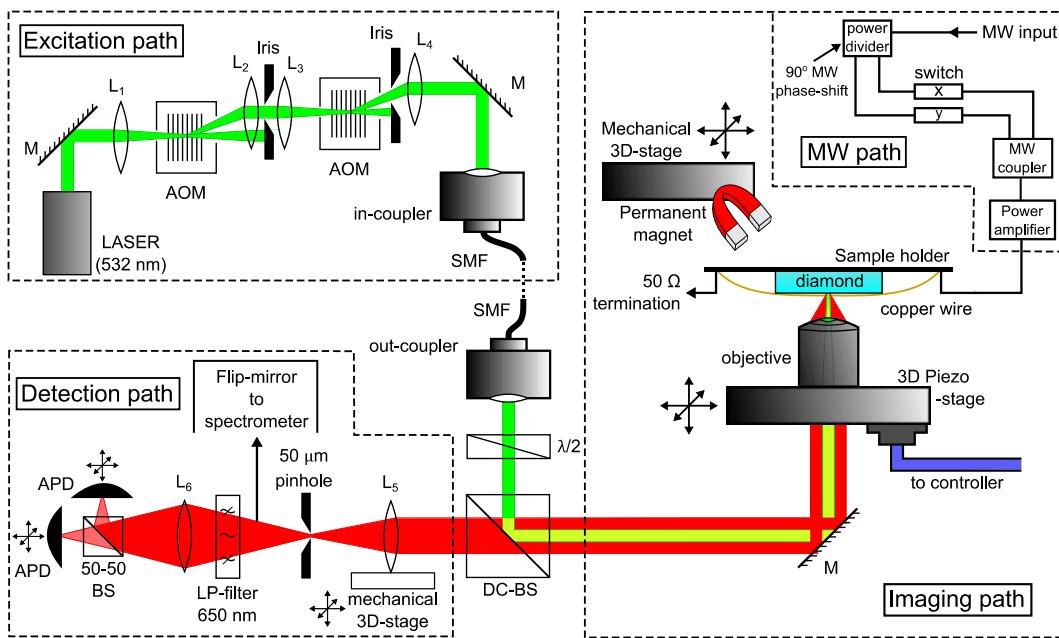


Diamonds can also be produced at NV centers with vacuum deposition of hydrogen and methane (CVD, for Chemical Vapor Deposition) to create a perfect diamond crystal structure and then with ion implantation with nitrogen ion beams.

The carbon structure surrounding a NV center protects the cavity area well. The state of the gap is unstable and quantum. It is excited by lasers and microwaves. The reading of the qubit state is performed by a fluorescence brightness measurement. The American startup QDTI was working commercially on this technique to create qubits. But it has pivoted to focus on the medical uses of diamond-based quantum sensing. **Quantum Brilliance** (2019, Australia) seems to be the only one to be positioned in this niche. They announced early in 2021 to have created a 5-qubit system and plan to scale it quickly.

<sup>268</sup> Source of illustration: [NV Diamond Centers from Material to Applications](#) by Jean-François Roch, 2015 (52 slides). A thesis describes well the different techniques for creating NV centers: [Engineering of NV color centers in diamond for their applications in quantum information and magnetometry](#), Margarita Lesik, 2015 (139 pages).

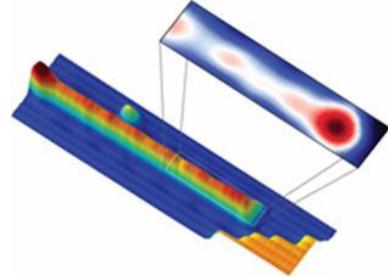
Below is a schematic diagram of the control mechanism for these qubits<sup>269</sup>.



**Figure A.1.:** Schematic representation of the utilized setup for the characterization of NV centers. Experimental setup utilized for optical characterization and coherent spin manipulation of NV centers, comprising of a home-built confocal microscope, a scanning-stage for the imaging of diamond, and external magnet and microwave apparatus. The excitation wavelength is 532 nm. In the figure, mirrors are represented by M, lenses by L<sub>i</sub>, single-mode optical fiber by SMF, beam-splitters by BS, and avalanche photo-diodes by APD.

**Majorana fermions** are anyons or quasi-particles which are particular states of electron clouds. They are electron spins at both ends of superconducting wires.

These qubits use braiding, a special topology that makes it possible to implement error correction at the qubit level. The promise is to enable the creation of scalable fault-tolerant quantum computers. These must also be cooled to a temperature close to absolute zero, around 10mK. This is the path chosen by Microsoft. The existence of the fermions of Majorana is not yet proven. It is one of the most hazardous paths to quantum computing.



Majorana fermions are often discussed but they belong to a broader category named “topological matter” and “many-body systems”.

## Flying qubits

Flying qubits are special because they travel from the place where they originated, traverse physical devices acting on them and terminate their journey on a sensor measuring their observable. They have a limited time available to run any computing, including a finite and small number of quantum gates.

<sup>269</sup> Seen in [Forefront engineering of nitrogen-vacancy centers in diamond for quantum technologies](#) by Felipe Favaro de Oliveira, 2017 (235 pages).

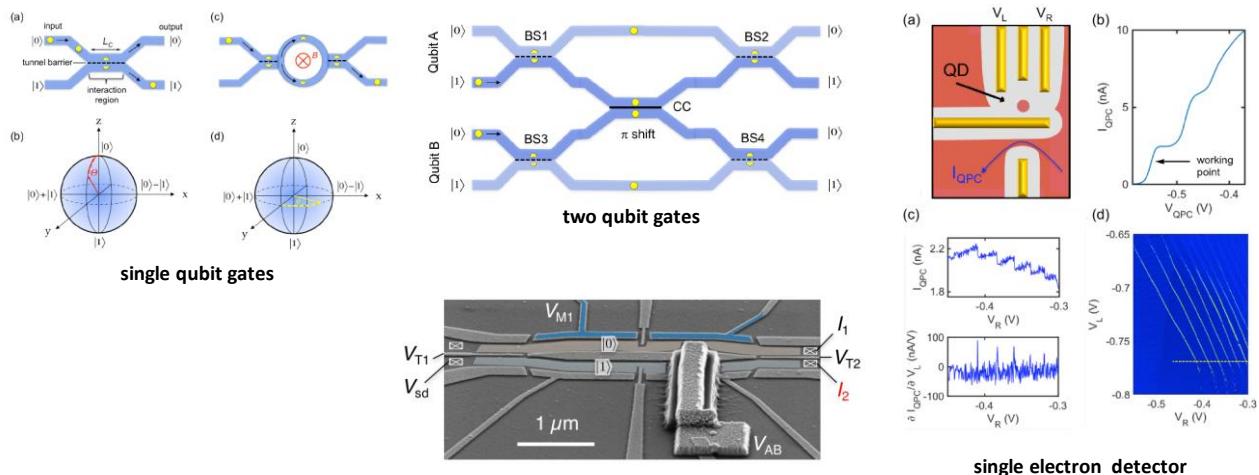
**Photons** are the most common flying qubit but there are many varieties of implementations. One type is based on a horizontal/vertical polarization observable. Others use continuous variables qubits. Boson sampling systems use multi-modes photons.

It is quite difficult to implement two qubit gates with these photon qubits, thus the alternative of the MBQC architecture that is an interesting workaround. Also, photon generation follows a probabilistic pattern which makes things complicated when the number of qubits grows.

Most of these qubits operate at room temperature, but the photon sources and their detectors must however usually be cooled to temperatures between 4K and 10K, which is much less demanding than the 15 mK of superconducting qubits or the 1K of silicon qubits.

Many startups are playing in this field, such as **PsiQuantum**, **Orca Computing**, **Xanadu** (continuous variables) and **Quandela**.

**Flying electrons** are at a pure research stage qubit technology using traveling electrons. It is based on using single-electron transport circulating on wave guide nanostructures build on semiconductors circuits, mostly AsGa, leveraging Coulomb coupling, quantum charge Hall effect and surface acoustic waves. Single- and two-qubit quantum gates can be realized on such circuits. Electrons can fly on distance of 6 to 250 microns. Electrons are created with producing THz photons which are converted into electrons. One qubit uses two-electron paths for states  $|0\rangle$  or  $|1\rangle$ <sup>270</sup>. At the end of processing, these flying electrons are detected by a quantum dot.



This technique could also be used to create shuttling electrons qubits connecting static quantum dots-based qubits together.

A few labs in the world are working on this including NPL in the UK, Ruhr-Universität Bochum, ERATO-JST and AIST in Japan, CEA-Leti and Institut Néel in Grenoble, France.

### Exotic qubits

Many research labs are working on using exotic qubits of various kinds. Most of the time, these qubits are at the fundamental research stage and far away from industrialization or even, sometimes, with a real single functional qubit.

<sup>270</sup> See [Electrical control of a solid-state flying qubit](#) by Michihisa Yamamoto, Christopher Bäuerle et al, 2017 (17 pages), [Coherent control of single electrons: a review of current progress](#) by Christopher Bäuerle, Xavier Waintal et al, 2018 (35 pages, source of the illustration) and [Macroscopic Electron Quantum Coherence in a Solid-State Circuit](#) by H. Duprez et al, 2019 (10 pages).

We have for example large molecules having a spin<sup>271</sup>, rare-earth ions in an insulating solid state matrix<sup>272</sup>, cold atoms trapped in optical lattices and magnetic microtraps<sup>273</sup>, various topological materials<sup>274</sup>, various forms of graphene<sup>275</sup>, silicon carbide qubits using a technique similar to and competing with NV centers<sup>276</sup>, carbon nanotubes-based mechanical oscillators<sup>277</sup> and so on.

## Pros and cons

None of these techniques have been proven at scale. They all have different advantages and disadvantages:

- **Qubits stability** which is evaluated in particular by their coherence time. Associated with the activation time of the quantum gates and the error rate, it conditions the number of quantum gates that can be chained in an algorithm. The best are trapped ions qubits.
- **Qubits fidelity** related to the errors level that is evaluated with single and double gates as well as with measurement. Again, the best-in-class are trapped ions.
- **Qubits geometry** is the way they are linked together, which will condition many parameters such as the execution speed and the depth of the algorithms that can be exploited. Best-in-class qubits for this respect are again trapped ions in 1D structures, although this doesn't scale well. The worst are IBM superconducting qubits.
- **Large scale entanglement** if possible, without being limited to the immediately neighboring qubits. So far, nobody does it.
- **Operating temperature** and for the accompanying electronics. The best are NV centers which are supposed to work at ambient temperature, and the worst are superconducting qubits, requiring 15 mK.
- **Qubits miniaturization** and their control electronics which impacts scalability. This rather favors electron spin qubits.
- **Manufacturing process** which depends on many parameters. In the case of cold atoms, for example, it is not necessary to create specialized circuits, whereas it is necessary for all other technologies.

---

<sup>271</sup> See [Optically addressable molecular spins for quantum information processing](#) by S. L. Bayliss et al, April 2020 (9 pages) as well as [Chemical tuning of spin clock transitions in molecular monomers based on nuclear spin-free Ni\(ii\)](#) by Marcos Rubín-Osanz et al, 2021 (11 pages). It involves one lab in Spain and three in France (ICMM Orsay, LCPQ Toulouse and LNCMI Grenoble).

<sup>272</sup> See [Universal Quantum Computing Using Electronuclear Wavefunctions of Rare-Earth Ions](#) by Manuel Grimm et al, 2021 (19 pages).

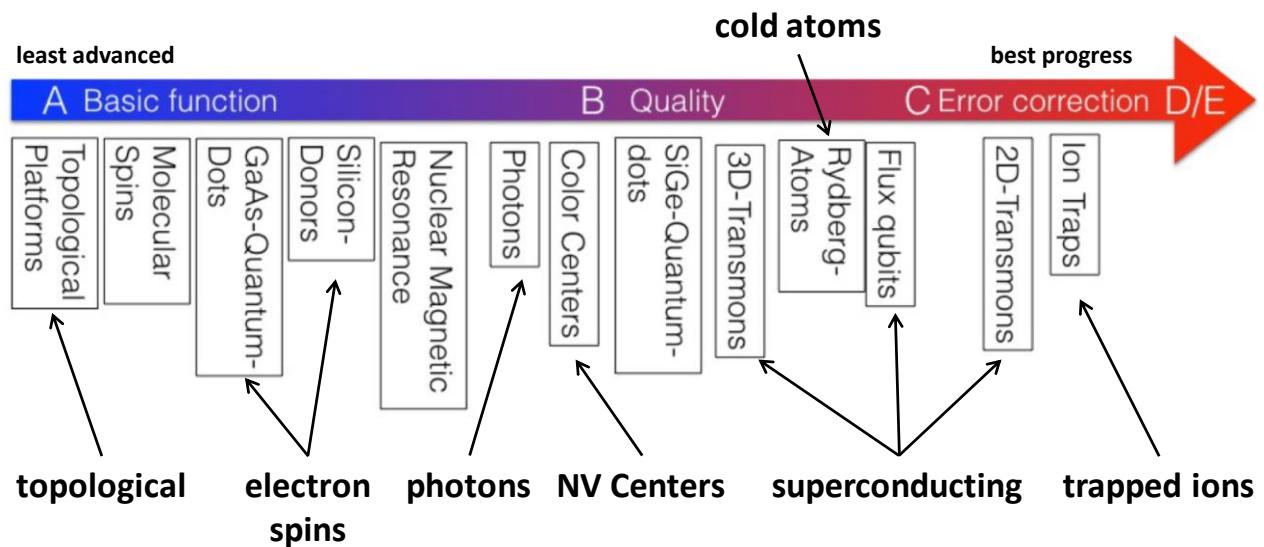
<sup>273</sup> See [Quantum Information Processing in Optical Lattices and Magnetic Microtraps](#) by Philipp Treutlein, Immanuel Bloch et al, Max-Planck Institute, June 2006 (15 pages). This is a variation of cold-atoms qubits adapted to cluster states and MBQC. See also [Quantum simulations with ultracold atoms in optical lattices](#) by Christian Gross and Immanuel Bloch, 2017 (8 pages).

<sup>274</sup> See [Anomalous normal fluid response in a chiral superconductor UTe<sub>2</sub>](#) by Seokjin Bae et al, July 2021 (5 pages) and [Multicomponent superconducting order parameter in UTe<sub>2</sub>](#) by I. M. Hayes, July 2021.

<sup>275</sup> See [Visualization and Manipulation of Bilayer Graphene Quantum Dots with Broken Rotational Symmetry and Non trivial Topology](#) by Zhehao Ge et al, 2021 (19 pages).

<sup>276</sup> See for example [Room temperature coherent manipulation of single-spin qubits in silicon carbide with a high readout contrast](#) by Qiang Li et al, July 2021 (18 pages). Like NV centers, these qubits have to potential to operate at room temperature. Silicon carbide qubits are also investigated in David Awschalom's team at the University of Chicago and in France at INSP Sorbonne-Université. See also [Developing silicon carbide for quantum spintronics](#) by Nguyen T. Son, David Awschalom et al, 2020 (8 pages).

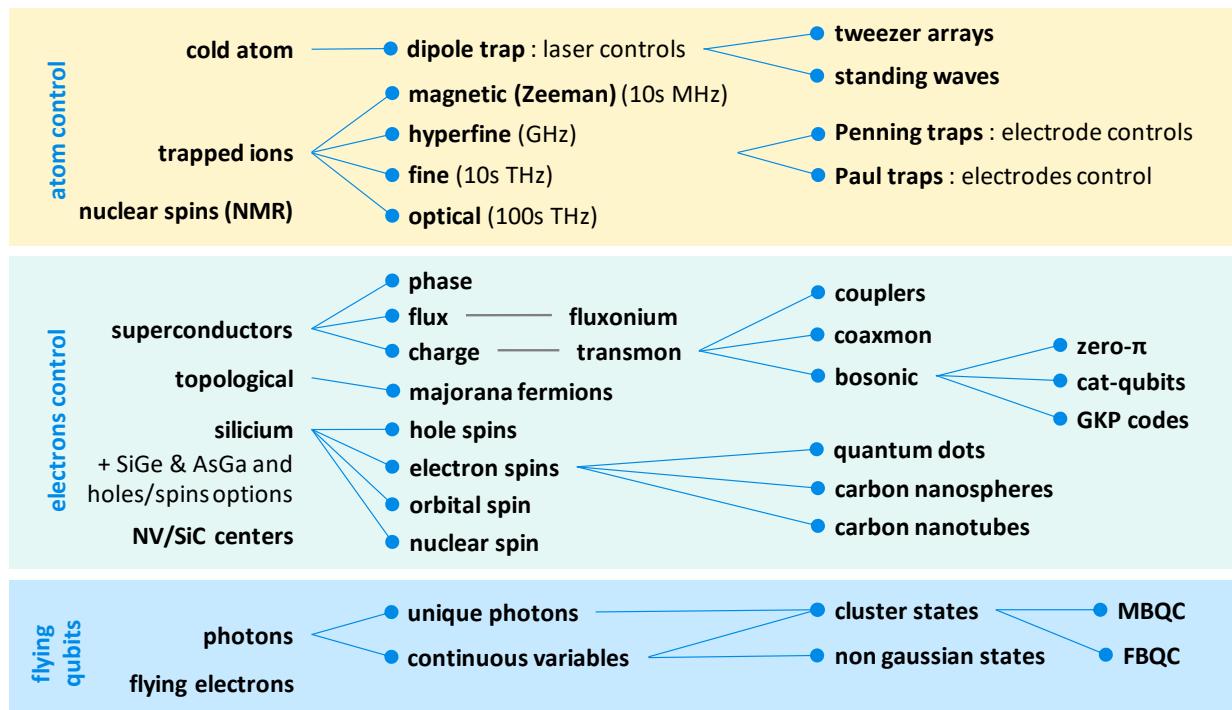
<sup>277</sup> See [Proposal for a nanomechanical qubit](#) by F. Pistoletti, A.N. Cleland, A. Bachtold, August 2021 (19 pages).



source : Entwicklungsstand Quantencomputer, BSI, 2020

The level of qubits is evolving rapidly. It is described in this excellent document from the German cybersecurity agency<sup>278</sup>. It mentions other technologies not listed in this inventory.

Here's another way to put it<sup>279</sup>. It segments the types of qubits according to three dimensions: the clock frequency of the quantum gates (roughly, the gates number that can be executed per second), the number of operations before errors occur, and the quantum gates fidelity (separating the one- and two-qubit gates). These last two axis are roughly homothetic because the number of operations before errors are generated depends on the error rate.

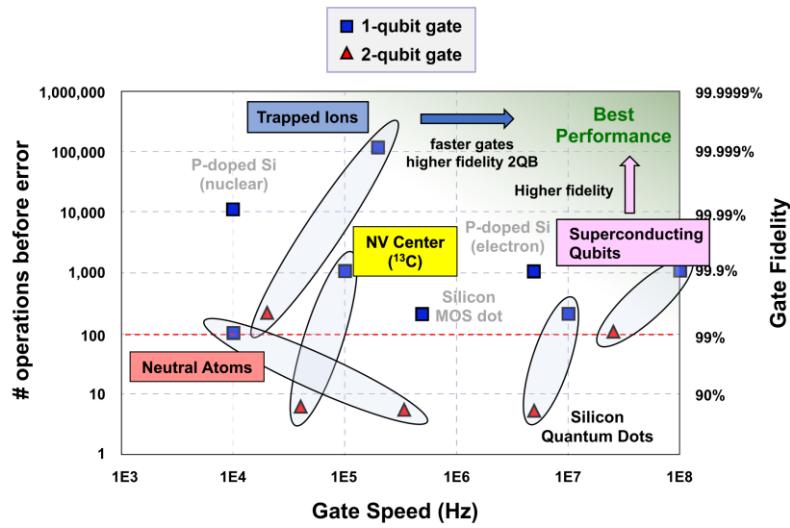


(c) Olivier Ezratty, November 2021

<sup>278</sup> See [Entwicklungsstand Quantencomputer](#) (*State of the art of quantum computing*, in English, June 2020 (266 pages)).

<sup>279</sup> See [Introduction to Quantum Computing](#) by William Oliver from MIT, December 2019 (21 slides). The schematic comes from [Engineering Quantum Computers](#) by William D. Oliver, December 2018 (15 slides).

Trapped ions have better gates than superconducting qubits but are quite slow. Silicon qubits are for the moment quite fast (at least, as fast as superconducting qubits). Cold atoms are slower. A last axis is missing: the number of qubits as of today and technology scalability. The chart was made in 2019 and may be outdated on some types of qubits. In the section devoted to quantum computing commercial vendors, we cover with more detail the science and technology of the main types of qubits, starting on page 239.



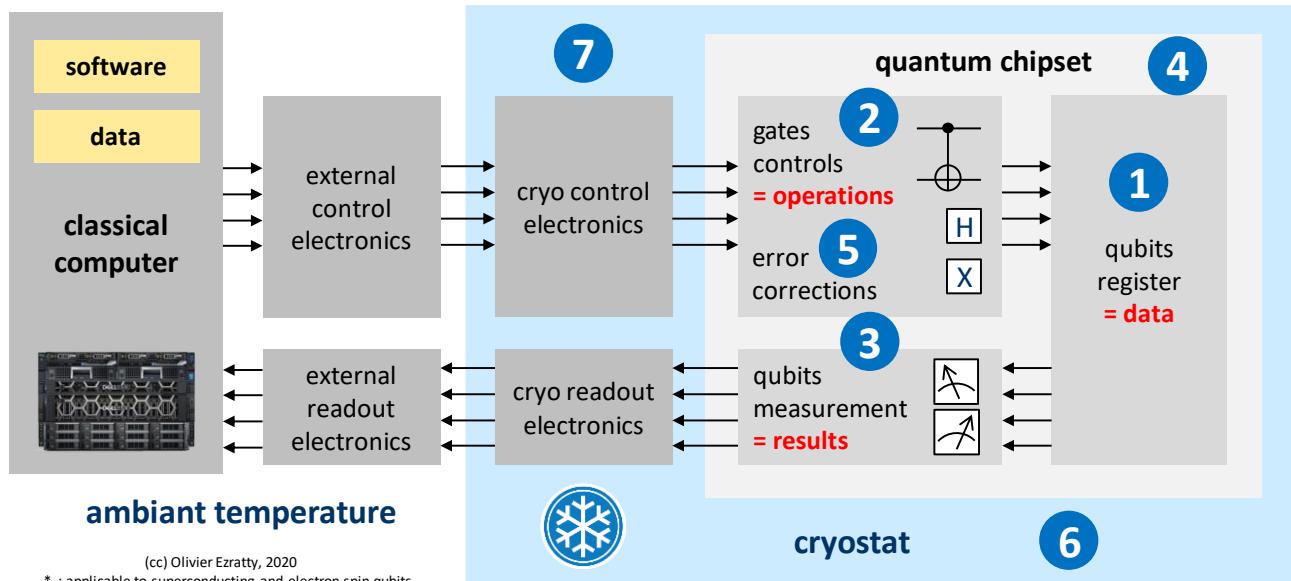
## Architecture overview

We will provide here an overview of the general architecture of a quantum computer, using the example of a superconducting qubit accelerator.

First of all, a bit like some external GPUs, quantum computers are implemented as co-processors or accelerators of classical computers that power and control them. A quantum computer is always driven by a classical computer, as can be a GPU for video games or for training neural networks in deep learning.

These conventional computers are used to run the programs that are driving the quantum processor with physical operations to be performed on the qubits and are interpreting qubits readout results.

The classical computer closely controls the operation of the quantum computer by triggering at a precise rate the operations on the qubits that are performed by the quantum gates and by quantum readout. It takes into account quantum gates execution time and the known qubits coherence time, i.e., the time during which the qubits remain in a state of superposition and entanglement.



In addition to its classical control computer, our quantum computer includes at least the components labeled from 1 to 7 that we will describe one by one, first with an overview below, then later, with a more detailed view<sup>280</sup>. The other types of quantum computers have similarities and differences that we will mention whenever relevant.

**1 Quantum registers** are collections of qubits. In 2021, the benchmarked record was 65 superconducting qubits with IBM. Quantum registers store the information manipulated in the computer and exploit the principle of superposition and entanglement allowing simultaneous operations on a large number of register values. To make a parallel with classical computing, this is memory. But processing is done directly in memory.

**2 Quantum gate** controllers are physical devices that act on the quantum register qubits, both to initialize them and to perform quantum gates on them. These gates are applied iteratively, according to the algorithms to be executed. They can also be used to manage error correction codes. Quantum gates feed registers with both data and instruction. These are not separated operations like with classical microprocessors.

**3 Measurement** qubit states is used to obtain the result at the end of the sequential execution of an algorithm's quantum gates and to evaluate error syndromes during quantum error correction. This cycle of initialization, calculation and measurement is usually applied several times to evaluate an algorithm result. The result is then averaged to a value between 0 and 1 for each qubit in the quantum computer's registers.

The values read by the physical reading devices are then converted into digital values and transmitted to the conventional computer which controls the whole and implements results interpretation. In common cases, such as with D-Wave and IBM, computing is repeated at least 1000 times. The reading devices are connected to their control electronics via superconducting wires in the case of superconducting computer qubits.

**4 Quantum chipset** usually includes quantum registers, quantum gates controls and measuring devices when it comes to superconducting or electron spin qubits. These are fed by microwaves coming from outside the chipset. Devices are more heterogeneous for other types of qubits, such as those that use lasers for initialization, quantum gates and qubit measurement like with trapped ions and cold atoms. Current chipsets are not very large. They have the size of a full-frame or dual-format photo sensor for the largest of them. Each qubit is relatively large, their size being measured in microns for superconducting qubits or down to 100 nm for electron spin qubits whereas modern CMOS processor transistors now have transistor sizes around 5 nanometers.

The chipset for superconducting and electron spin qubits is a chip of a few square centimeters. It is usually integrated in an OFHC (Oxygen-Free High thermal Conductivity) copper package which is purified and freed from oxygen, limiting thermal conductivity. This package is fitted with coaxial connectors so that it can be fed by the microwaves controlling qubit gates. In the latest superconducting processors from IBM and Google with 53 qubits, more than 160 of these connectors are required. The chipset package is integrated in two small concentric aluminum and Cryoperm (from **MuShield**) magnetically insulated enclosures.

**5 Error correction** is implemented with special code operating on a large number of consolidated qubits named logical qubits. They can be physically organized to optimize error correction, such as with surface codes and color codes. It's one of the biggest challenges ahead for creating scalable quantum computers. As of 2021, no quantum computer is large enough to accommodate logical qubits, given the number of physical per logical qubits exceeds the maximum number of qubits currently available.

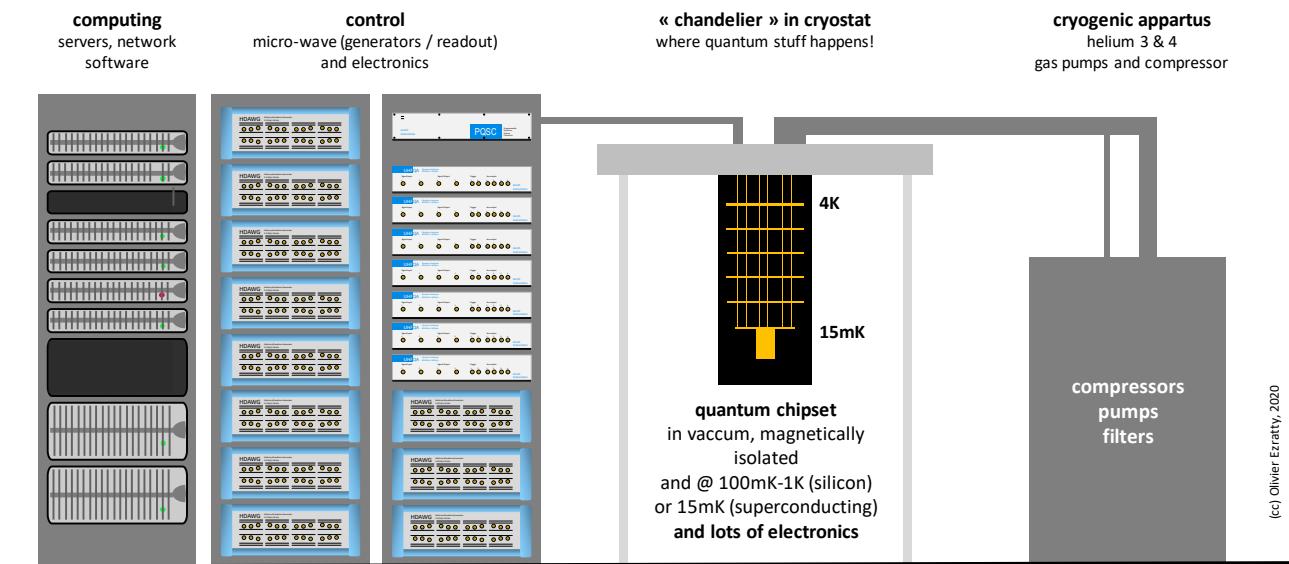
---

<sup>280</sup> To make the diagram *above* which explains all this, I was inspired by slide 14 of the presentation [Quantum Computing \(and Quantum Information Science\)](#) by Steve Binkley, US Department of Energy, 2016 (23 slides).

⑥ **Cryogeny** usually keeps the inside of the computer at a temperature close to absolute zero. It contains part of the control electronics and the quantum chip(s) to avoid generating disturbances that prevent the qubits from working. The Holy Grail would be to operate qubits at room temperature but the corresponding architectures such as in NV centers are not yet operational and there are still practical performance reasons to operate it at low-temperatures.

⑦ **Control electronics** in the cryostat enclosure. The qubit control electronics drive the physical devices used to initialize, modify, and read the qubit status. In superconducting qubits, quantum gates are activated with microwave generators of frequencies between 4 and 8 GHz generally located outside the cryostat. These microwaves are transmitted on coaxial electrical wires between their source and the quantum processor, with superconducting cables below 4K. Their generators still take up a lot of space. They are not very miniaturized at this stage. Interesting work aims at integrating these microwave generators and readers inside the cryostat enclosure, if only to limit the wiring. These are frequently based on cryoCMOS technology, CMOS components that are tailored to work at low temperature, 4K for many and as low as 20 mK for some.

The diagram below is a rough representation of an entire superconducting qubits based quantum computer. The blue equipment corresponds to the microwave generators and analyzers of Zurich Instruments.



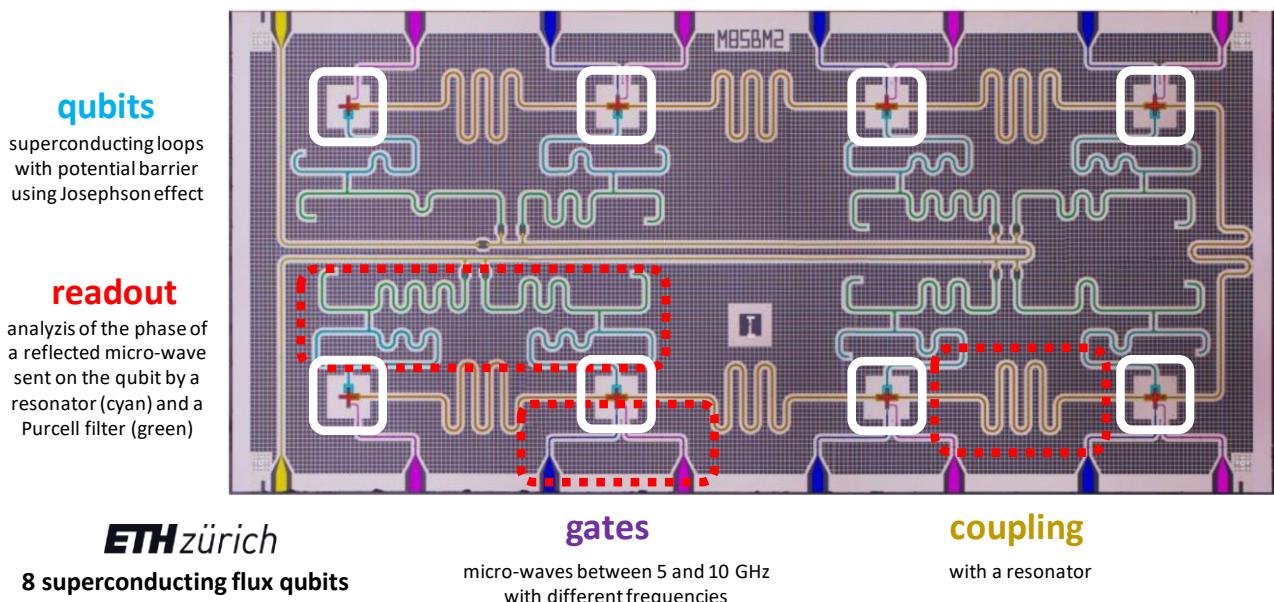
## Processor layout

To better understand the previous explanation, here is a chipset layout with 8 superconducting qubits, from ETH Zurich. Although it's already a few years old, the underlying concepts are generic<sup>281</sup>.

- **Qubits** are located in the white rectangles. These are tiny Josephson effect superconducting circuit loop.
- **Coupling circuits** link them together. It's used to control entanglement between pairs of qubits.

<sup>281</sup> Image source: [The European Quantum Technologies Roadmap](#), 2017 (30 pages) and the thesis [Digital quantum computation with superconducting qubits](#) by Johannes Heinsoo, ETH Zurich, 2019 (271 pages).

- **Single-qubit gates** use the blue and purple contacts. It sends microwaves to the qubits. These pins are powered via cables by very high frequency current sources, sending microwaves photons, between 4 and 8 GHz. These frequencies must be different between adjacent qubits of the same circuit to avoid crosstalk. It is the combination of these frequencies that will trigger different types of quantum gates and entanglements between adjacent qubits.



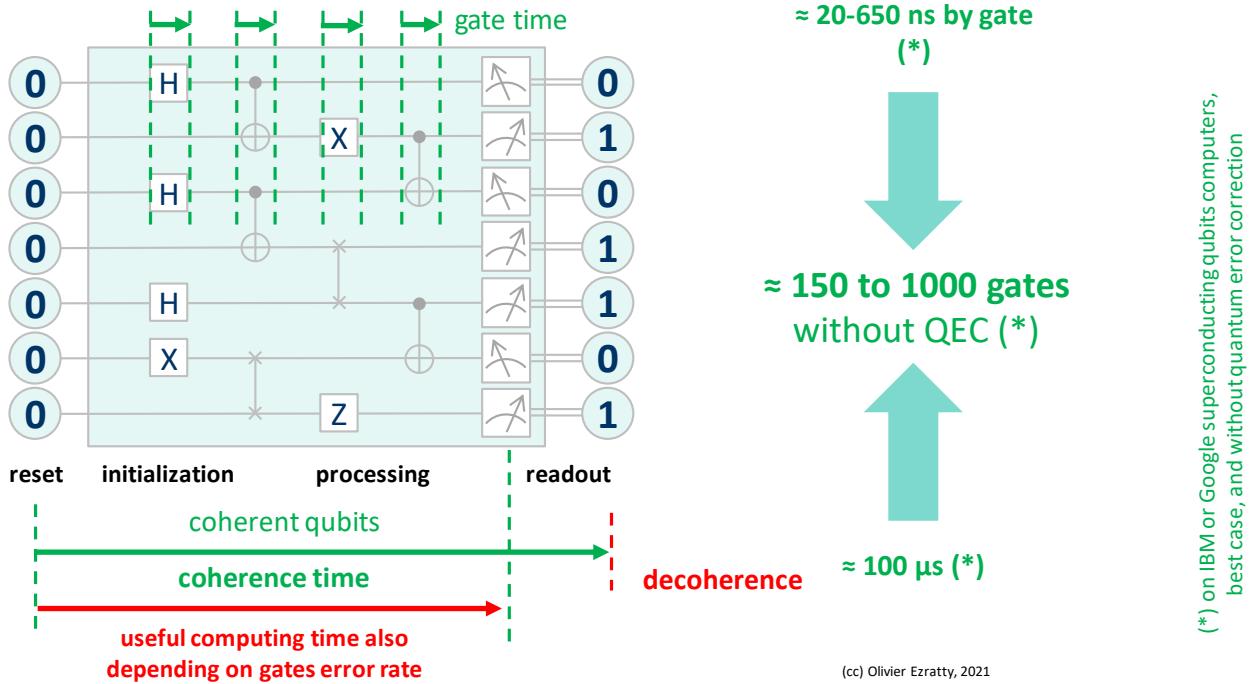
- **Measurement** takes place with other circuits, also fixed in the component. In superconducting qubits, these are magnetometers which are then connected to the outside of the vacuum chamber and cooled by superconducting cables. These are driven by microwaves.

Qubits must interact with each other but as little as possible with their environment until measurement. This is one of the reasons why they are usually cooled to a temperature close to absolute zero and magnetically isolated from the outside. The choice of materials for the chipsets also plays a role in minimizing the noise that could affect the qubits and bring them out of their coherent state.

In the diagram *below* is the how and why of the relationship between qubit gates time and coherence time during which the qubits remain stable. The orders of magnitude of these times for a typical quantum computer, particularly a superconducting qubits one, give at best a ratio of 1 to 500 between gate times and coherence time. This means that the number of quantum gates that can be used in an algorithm is limited on NISQ systems. In the first generations of IBM quantum computers, the X, Hadamard and CNOT gates lasted 130 ns, 130 ns and 650 ns respectively.

These indications provide an upper limit on the number of gates that can be chained in a quantum algorithm. Note that these times are longer for quantum computers with ion traps, but the gate times are also longer. In CMOS qubits, coherence times are longer and gate times are low.

However, the available computing time is more limited by the quantum gates error rate. It constrains what is called the computation depth, i.e. the number of quantum gates that can be chained together without the error rate of the gates mitigating the results. Algorithms must therefore optimize the number of gate cycles to be executed, which is furthermore constrained by the physical connectivity between qubits.



In diagrams describing quantum algorithms, such as the one *above*, the double bar after measuring the state of a qubit conventionally indicates that a normal bit has been recovered, at 0 or 1. By the way, all this reminds us that there are as many output qubits as input qubits in a quantum computation since they are physically the same!

## Error correction

One of the pitfalls of existing qubits is their significant error rates generated with quantum gates and measurement and coming mostly from the fateful quantum decoherence.

Decoherence is mostly generated by the interactions between the qubits and their environment. It progressively destroys the quantum information sitting in the qubits, and particularly the entanglement between these. It leads to an inevitable failure in computation after a short time. Error rates for each operation and readouts are commonly between 0.1% and several %, depending on the qubit type and quality. But even 0.1% is an intolerable level for most calculations.

In conventional computing, errors are way less frequent but must still be corrected. While some errors may be detected and fixed during computing in microprocessors, most errors are happening in memory, storage and telecommunications. These errors are discrete, corresponding to some unwanted bit flip. In quantum technologies, errors happen first and foremost in computing and within qubits and they are continuous and analog by nature. For single qubits, you can represent them by small rotations in Bloch spheres and for several qubits entanglements, it looks like vanishing off-diagonal values in their density matrix.

### Types and sources of errors

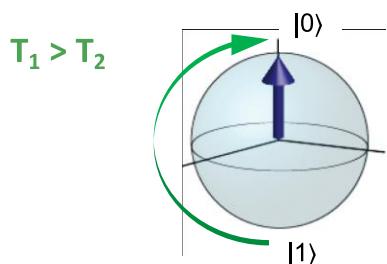
A qubit is coherent when its superposition and entanglement with other qubits is preserved over some period of time. Qubits coherence time is an indication of how long register qubits remain coherent, with untouched superposition and entanglement. It is generally evaluated with two times, T1 and T2.

**T1** corresponds to the end of coherence linked to a loss of amplitude ("energy relaxation"). It is also called "longitudinal coherence time", "spontaneous emission time", "population lifetime" or "amplitude damping" and corresponds to a loss of energy in qubits<sup>282</sup>.

**T2** corresponds to a phase shift, i.e. a rotation around the z-axis in the Bloch sphere. It's also called the "transverse coherence time", "phase coherence time" or "phase damping"<sup>283</sup>.

### T<sub>1</sub>: relaxation, dampening

- Environment exchanges energy with the qubit, mixing the two states by stimulated emission or absorption
- Important during read-out
- **Intuitively time to decay from |1> to |0>**

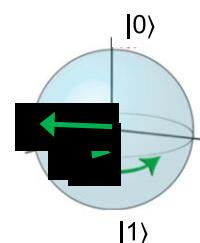


$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

These are not cut-off times,  
but "half-lives."  
Decay is *continuous*.

### T<sub>2</sub>: dephasing

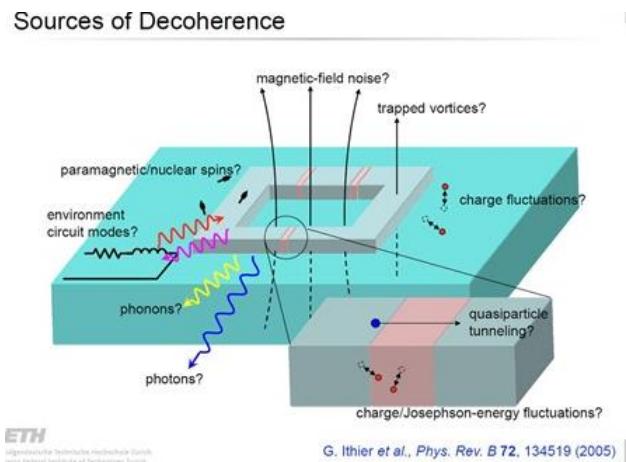
- Environment creates loss of phase memory by smearing energy levels, changing phase velocity
- Important during "computation", bounds circuit depth (number of consecutive gates)
- **Intuitively time for  $\phi$  to get imprecise**



There are three main categories of errors to correct<sup>284</sup>:

- **Flip errors** as shown in the Bloch sphere above, are amplitude errors that tend to push the amplitude back to |0>. It is related to the T1 mentioned previously.
- **Phase errors** are rotations around the equator. It's related to the T2 also mentioned above.
- **Leakage errors** that see the qubit drift and stabilize in another energy state than the basic |0> or |1>. This can occur in the |2> level of a superconducting qubit, which we are trying to avoid, or with variations in the hyperfine energy levels of trapped ion qubits.

Error sources are multiple, leading notably to the progressive **decoherence** of qubits which affects qubits superposition and entanglement. They are linked to the various interactions between qubits and their immediate environment<sup>285</sup>. These include :

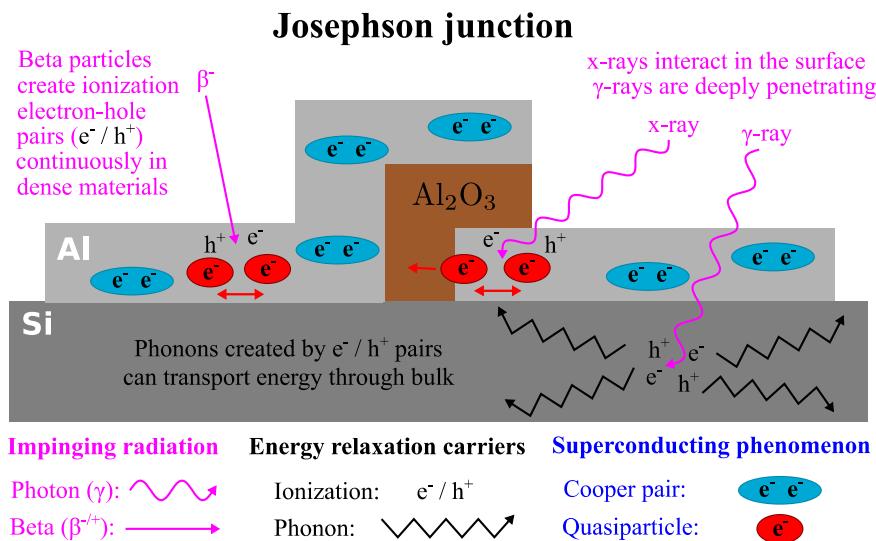


<sup>282</sup> Source for the diagram: [How about quantum computing?](#) by Bert de Jong, June 2019 (47 slides).

<sup>283</sup> T1 is measured with setting a qubit in the |1> state and measuring the time it takes for the qubit to come back to |0> following the equation  $e^{-t/T1}$ . T2 is measured with initializing a |0> with an H gate creating a superposed |0> + |1> state. We wait for time t and apply another H gate which is supposed to bring back the qubit in the |0> state. After some time, we'll get a 1/2 average result since the superposed state will be sent back to |0> or |1>. After an H gate and measurement, this turns into 50%/50% chance to have a |0> or |1>. Source: [Lecture 19: How to Build Your Own Quantum Computer](#) by Isaac Chuang and Fen Zhao, MIT, 2003 (4 pages).

<sup>284</sup> Here is a small inventory of noise sources for superconducting qubits. The diagram on this page is taken from the presentation [Sources of decoherence](#), ETH Zurich, 2005 (23 slides).

- **Calibration errors** of quantum gates that occur in particular in the calibration of superconducting qubits. They are the ones that can notably trigger leakage errors.
- **Thermal noise** from components around the qubits. This is the reason for the existence of attenuators around superconducting qubits and their operation at very low temperatures. It comes among other things from shocks between atoms.
- **Electrical and magnetic noise** which can have many origins depending on the qubits. It explains why D-Wave isolates its quantum computer with 16 metal layers to limit the impact of terrestrial magnetism on its qubits.
- **Vacuum quantum fluctuations** originating errors which we studied quickly in a previous section, page 120<sup>286</sup>. It's an endogamous source of errors within qubits while all others are exogamous.
- **Gravity** given this type of error and vacuum fluctuation ones appear to be minor compared to the previous ones<sup>287</sup>.
- **Radioactivity**, particularly coming from cosmic rays. Radiations can be X-rays, gamma rays (their electromagnetic nature was discovered in 1914) and beta particles and their ionizing effects. The phenomenon can be partially reduced with thick lead shielding of the processor<sup>288</sup>.



Generally speaking, errors are generated by various interactions, electromagnetic or mechanical, between qubits and their immediate environment and are associated with the phenomenon of quantum decoherence. The first objective of physicists is obviously to reduce these physical sources of error. They are progressing steadily but are barely managing to gain one or two orders of magnitude in error rates, whereas in an ideal world, we would need ten orders of magnitude improvements.

<sup>285</sup> Any operation will generate an error. An error can be generated at the time of correction, at the time of detection or at the time of application of a gate. Doing nothing on a qubit can also generate errors because of its finite coherence time.

<sup>286</sup> See [Observation of quantum many-body effects due to zero point fluctuations in superconducting circuits](#) by Sébastien Léger, Nicolas Roch et al, Institut Néel, 2019 (8 pages) which describes the phenomenon on superconducting qubits.

<sup>287</sup> See about gravity: [A model of quantum collapse induced by gravity](#) by Franck Laloë, 2020 (14 pages) and [Gravitational Decoherence](#), 2017 (78 pages).

<sup>288</sup> See [Impact of ionizing radiation on superconducting qubit coherence](#) by Antti P. Vepsäläinen et al, August 2020 (24 pages), the source of the illustration. See also [Correlated charge noise and relaxation errors in superconducting qubits](#) by C.D. Wilne, Roger McDermott et al, Nature, December 2020 on Arxiv and June 2021 in Nature (19 pages) which describes the correlated errors appearing in superconducting qubits and how it could impact the architecture of quantum error correction codes.

Some of these effects are avoided by cooling the qubits to a temperature close to absolute zero, but this is not enough. Researchers are therefore working hard to ensure that the noise affecting the qubits is as low as possible so that qubits coherence time can be as long as possible.

We have to manage this contradiction: qubits remain coherent, in a state of superposition and entanglement, if we do not disturb them, but we spend our time disturbing them with quantum gates operations! There are three ways to address these issues: improving gates fidelity, implementing quantum error correction codes and at last, reduce the number of gates needed to run algorithms.

## **Qubits fidelity**

In a universal gates quantum computer, three types of errors are usually evaluated: errors in single-qubit quantum gates, errors in two-qubit gates, and errors qubits measurement.

These error rates are between 0.1% and several 1%, which is much higher than the current error rates of traditional computing, which are negligible<sup>289</sup>. Qubits "fidelity" for any of these three dimensions is 100% minus the related error rate.

The chart below consolidates a comparison of some fidelity levels of superconducting, trapped ion and cold atom quantum computer qubits, this information being provided by their suppliers<sup>290</sup>.

It shows that two-qubit gates and readout error rates are generally higher than one-qubit gates error rates<sup>291</sup>. We must therefore always pay attention to two-qubit gates fidelity, particularly given these gates are the source of much of the quantum computing power.

But these fidelities are not always measured in the same conditions. Some are measured with only a couple interacting qubits while others are done with all the register's qubits being active. It can create significant differences favoring the first kind of measurements.

The best fidelity achieved as of 2021 was 99.989% for Honeywell's 4 ion trapped single-qubit processor and 99.38% for Google Sycamore's 53 qubit dual-qubit gates<sup>292</sup>. Google's single qubit gates fidelity is 99.84% which is a performance considering the number of qubits in their system (53). The two-qubit CZ gates fidelity of the 24 Chinese superconducting qubits is 99.5%<sup>293</sup>.

Another observation relates to IBM's most recent fidelities with their best-in-class 27, 65 and 127 qubit systems as of November 2021. It did show 2-gates and readout fidelities that are lower as the number of qubits grows. Still, for a given a qubits number, IBM improves its processor fidelities over time.

These error rates are currently prohibitive when executing many quantum gates in a row. With each operation, error rates add up and the reliability rate decreases.

---

<sup>289</sup> In classical calculation, errors are very rare. We talk about single particle perturbations (PPI) and single event upset (SEU) which trigger "soft errors" or logical errors. The SER (Soft Error Rate) combines the SDC (Silent Data Corruption, not detected) and the DUE (Detected and Unrecoverable Error, detected but not correctable). The unit of error measurement is the FIT (Failure in Time), which corresponds to one error per billion hours of use. The MTBF of electronic equipment (Mean Time Between Failure) is generally measured in years or decades. Errors are generally caused by isolated particles (ions, electrons, photons), particularly from cosmic rays like high-energy gammy rays. This affects in particular the electronics used in aerospace, which must be hardened to withstand them, as well as those used on Earth but at altitude. Memory is often more affected than processors. Hence error correction systems that use for example a parity bit and cyclic redundancy check used in telecommunications.

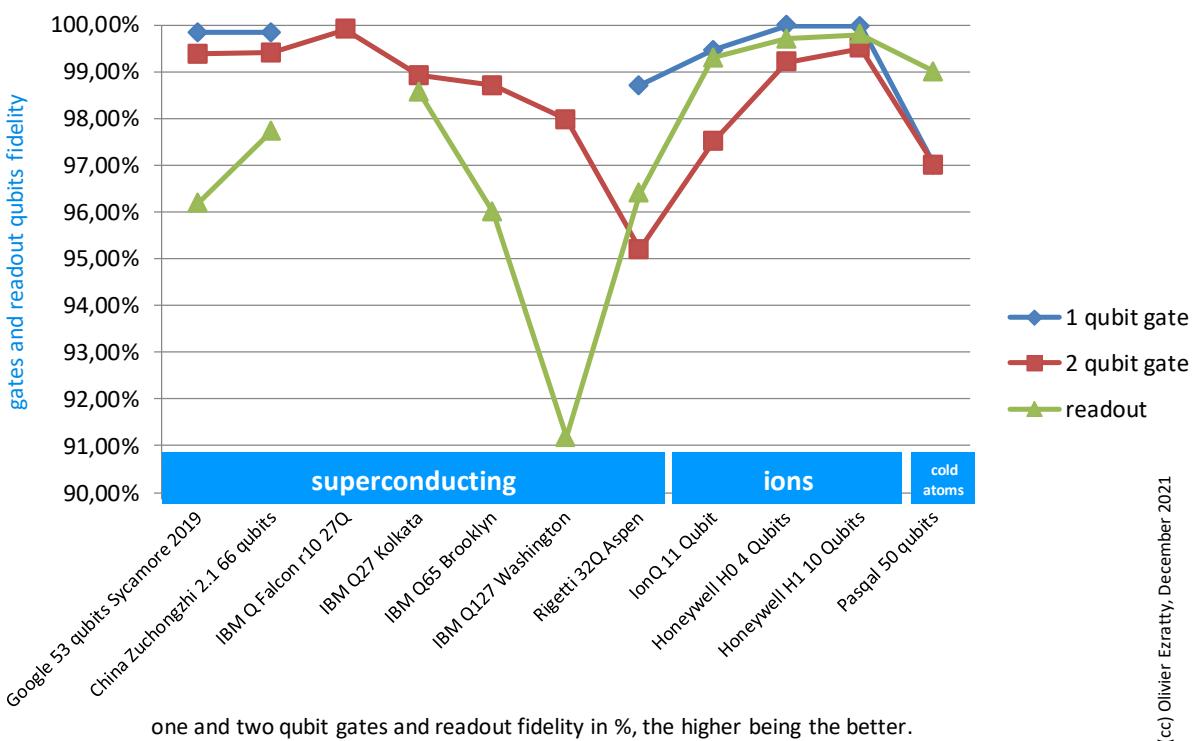
<sup>290</sup> Source for qubit reliability data mainly comes from [Qubit Quality on Quantum Computing Report](#) website, 2020. Plus some additional data coming from vendor sites.

<sup>291</sup> See [An introduction to quantum error correction](#) by Mazyar Mirrahimi, 2018 (31 slides) as well as [Introduction to quantum computing](#) by Anthony Leverrier and Mazyar Mirrahimi, March 2020 (69 slides) which completes it well.

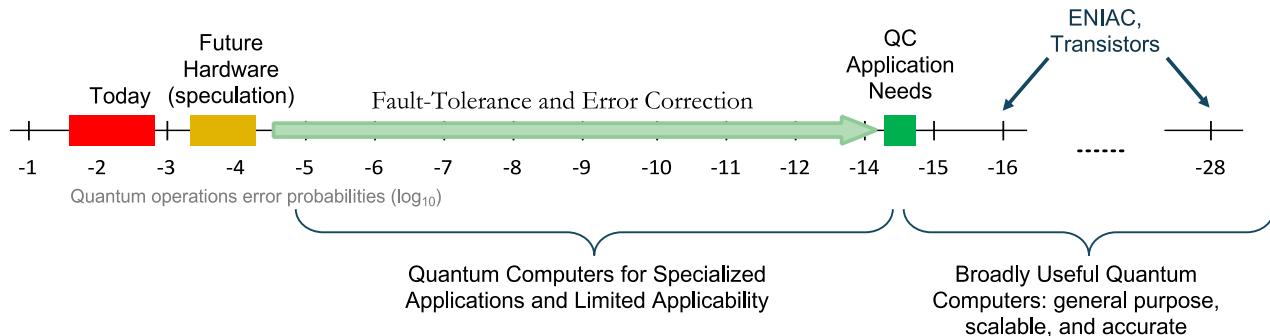
<sup>292</sup> See the NASA and Google paper describing Google's performance: [Quantum Supremacy Using a Programmable Superconducting Processor](#) by Eleanor G. Rieffel et al, August 2019 (12 pages).

<sup>293</sup> Data source: [Superconducting Quantum Computing](#) by Xiaobo Zhu, June 2019 (53 slides).

Imagine chaining a few dozen two qubits gates! At this rate, the error rate can very fast exceed 50% at the end of a rather simple algorithm and, generally, well before the fateful qubit coherence time limit.



Hence the fact that the power of a quantum computer is always evaluated not simply by the number of available qubits but by the number of operations that can be done with a reasonable error rate at the end of the calculation. To avoid this quantitative constraint, we should have qubits with quantum gate error rates of  $10^{-10}$  or even  $10^{-15}$ .



The *above* diagram illustrates this discrepancy between today's physical qubits and the need to perform reliable calculations (without error correction)<sup>294</sup>.

A formula is used to evaluate the dependency between quantum gates error rates ( $e$ ), the number of qubits ( $n$ ) and the number of usable gates ( $d$ ), called "circuit depth":  $nd < 1/e$ . As the error rate decreases, the usable circuit depth increases, and the range of usable algorithms expands<sup>295</sup>.

<sup>294</sup> Diagram source: [How about quantum computing?](#) by Bert de Jong, June 2019 (47 slides).

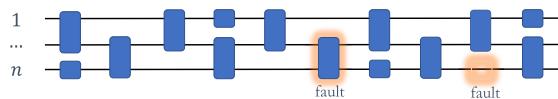
<sup>295</sup> Schematic source: [Quantum advantage with shallow circuits](#) by Robert König, 2018 (97 slides).

## Circuit depth in the Noisy Intermediate-Scale Quantum Technology Era

Noise sets a limit on the maximum size of a computation without error correction.

Rough estimate:  $nd \ll 1/\epsilon$

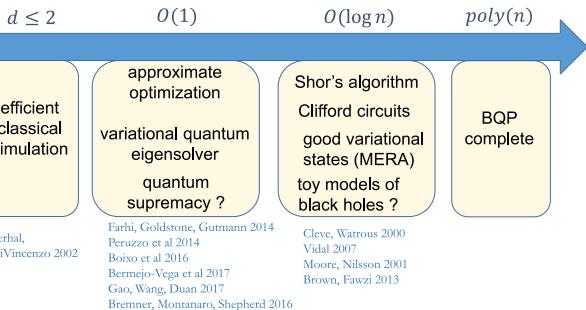
$n$  = number of qubits (width)  
 $d$  = circuit depth  
 $\epsilon$  = error rate



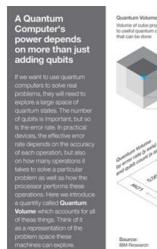
Deep circuits → few qubits → efficient classical simulation.

Shallow circuits → many qubits → potential for a quantum advantage.

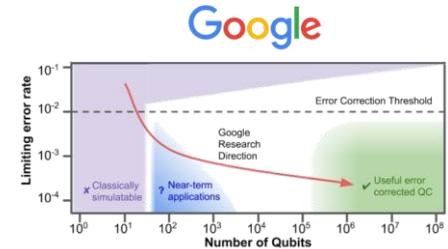
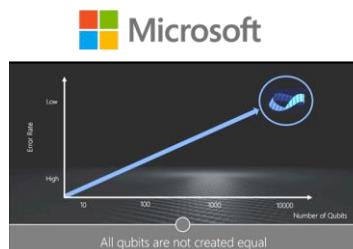
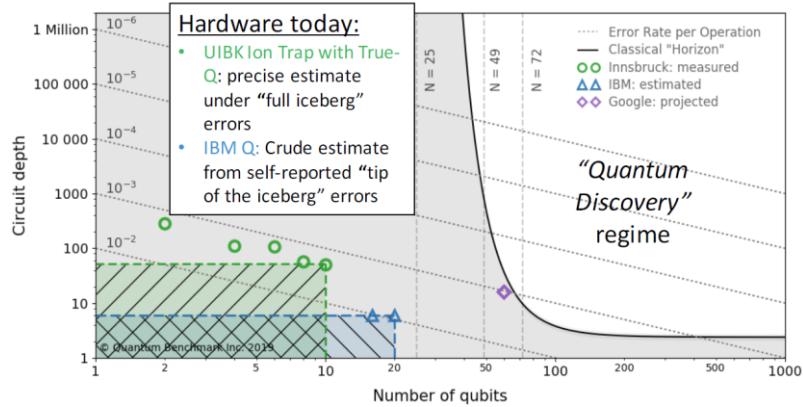
## Shallow circuits and their potential



It is presented in another way in this **Quantum Benchmark** diagram, with the number of qubits on the abscissa and the depth of the circuits on the ordinate (number of gates that can be linked in a quantum calculation), conditioned by the skewed dotted lines that correspond to the error rates of the quantum gates. The white zone is the *quantum supremacy* zone, also known as the *quantum discovery regime*<sup>296</sup>.



## Scaling up Quantum Computers



All this explains why IBM communicates on the notion of **quantum volume**, which we'll describe later. Microsoft and Google do the same in their marketing, without having adopted IBM's quantum volume metric.

For a quantum computer to be useful and scalable, you need a lot of qubits, a low error rate for quantum gates and qubits readout, and a long qubit coherence time to be able to execute algorithms without much time constraints although quantum error correction codes can be interesting workarounds this last constraint.

## Error rates evaluation

How are quantum gates and measurement error rates evaluated? One method is the **Randomized Benchmarking** (RBM) process which consists in chaining a random sequence of quantum gates whose result is known in advance and with comparing the results obtained with the right responses. Usually, a random sequence of Clifford gates is launched and then executed backwards.

<sup>296</sup> Slides presented by Joseph Emerson of Quantum Benchmark at the Quantum Computing Business conference organized in Paris on June 20, 2019 by Bpifrance. They position Google very close to the area of interest with their 72 qubits, but public benchmarks of these qubits have not yet been published after their announcement in March 2018. The 53 qubits of the Sycamore generation announced in October 2019 are however at about the same place (purple diamond).

The error rate increases with the number of chained quantum gates and depends on their type. We can evaluate the error rate of a given gate with the **Interleaved RBM** which injects the gate periodically into the random gate set used. We then measure the difference in error rate between the sequence with and without these added quantum gates<sup>297</sup>.

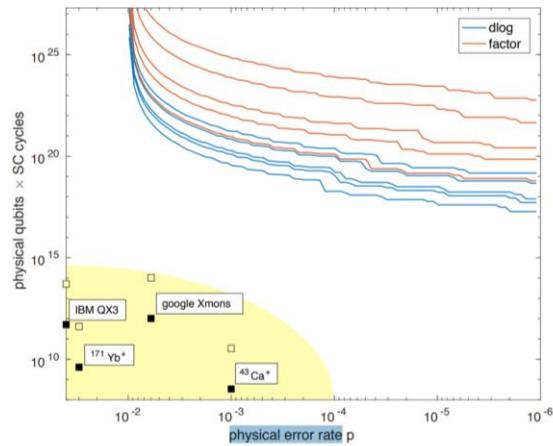
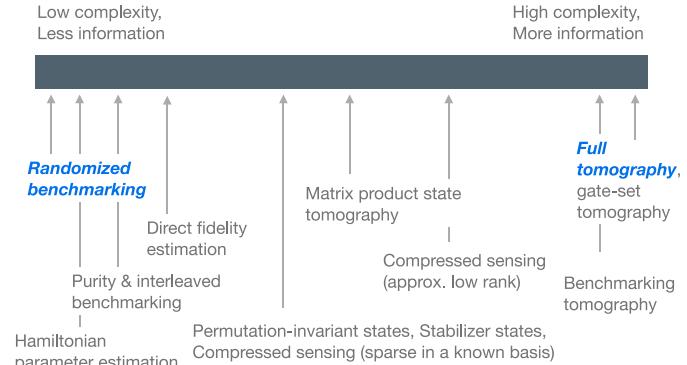


Figure 2.4: Comparison of algorithmic demands with currently achieved hardware performance. The plot shows required resources as number of qubits times rounds of error correction in the surface code for dlog (blue) and factoring (orange) for common key sizes as a function of the physical error rate  $p$ . The squares show current realizations assuming one day run time (solid) or 100 days (empty); the yellow area shows expected near-term progress. Both scales are logarithmic.

### Strategies for Characterizing Noise



You'll have to look elsewhere to find out more data<sup>298</sup>. The RBM method has some drawbacks for clean noise quantification. It is apparently not suitable for the detection of any noise patterns<sup>299</sup>.

Several other methods exist, such as **quantum state tomography** (QST) that we already covered in the [section](#) dedicated to measurement, page 168, which is based on a repeated measurement of qubit states that allows the reconstruction of a mean density matrix and the associated errors, for one or two qubits after a calculation.

Another method exists that is based on some mathematical tools identifying a match between the noise rate of one and two-qubit gates of an algorithm and the total noise rate of the complete algorithm. In short, it links macro noise (algorithm) to micro noise (quantum gates).

## Error correction codes categories

Quantum error correction can't work the same as classical error correction. Qubits cannot be independently replicated with some measurement that would be performed on one replicated qubit. On top of that, we are correcting analog errors in multiple dimensions, not just a 0/1 error flip that could be labelled as a simple "digital error"<sup>300</sup>.

<sup>297</sup> I found this information in [Quantum Computing: Progress and Prospects](#), 2018 (206 pages), page 2-20. The process of benchmarking quantum gates is detailed in [Randomized benchmarking for individual quantum gates](#) by Emilio Onorati et al, 2018 (16 pages). The origin of the method is [Scalable noise estimation with random unitary operators](#) by Joseph Emerson et al, 2005 (8 pages). See this other, more recent test protocol: [Efficient learning of quantum noise](#) by Robin Harper et al, 2019 (15 pages).

<sup>298</sup> As in the aforementioned German ANSSI report [Entwicklungsstand Quantencomputer](#) (*State of the art of quantum computing*), which dates from 2018 and highlights the huge gap between the performance of qubits, particularly at IBM and Google, and the need for integer factorization to break common RSA keys. See also [Efficient learning of quantum noise](#) by Robin Harper et al, Nature Communications, 2019 (15 pages) and [Characterization, certification and validation of quantum systems](#) by Martin Kliesch, April 2020 (87 pages).

<sup>299</sup> The chart comes from [Characterization of quantum devices](#) by Steve Flammia, University of Sydney, 2017 (118 slides) which provides an excellent overview of the various qubits benchmarking techniques.

<sup>300</sup> The stakes of QEC are very well explained in [Approaches to Quantum Error Correction](#) by Julia Kempe, 2005 (29 pages).

The techniques explored for more than two decades consists in implementing quantum error correction codes called **QEC** for Quantum Error Correction or rather **QECC** for QEC Codes<sup>301</sup>.

The other solution being considered deals with using NISQ, for Noisy Intermediate Scale Quantum computers, those current quantum computers that use noisy and uncorrected qubits. This is done with algorithms, often hybrid classical/quantum algorithms, which are supposed to be errors resili-ent.

Error correction codes apply to both universal gate quantum computing and quantum telecommuni-cations. In the first case, they are integrated into the concept of fault-tolerance quantum computing (**FTQC**), which is more or less synonymous with large-scale quantum computing (**LSQC**). Error correction is a mean to slow down qubits decoherence and extend the available computation time.

We must distinguish “logical error correction codes” and “physical codes” that are directly managed in the hardware, such as bosonic codes, which include GKP, binomial codes and cat-codes<sup>302</sup>. The latter implement in a cavity a "Schrödinger cat" that allows to manage a projection space used for error correction, as in the error correction algorithms based on stabilizing codes that we will see later.

The chart *below* in blue makes an inventory of the main quantum error correction codes with their origin and date of creation<sup>303</sup>. This error correction zoo is very dense<sup>304</sup>. It is a very rich scientific field of quantum technologies and has been growing regularly since 1995. It includes several fami-lies of error correction codes.

The best-known are the **stabilizer codes** that correct flip and/or phase errors with three, five (Laflamme), seven (Steane) or nine qubits (Shor). These codes replicate qubits several times with entanglement. They follow the same processing in parallel. Then, the QEC compares the results at the output of algorithms in order to keep the statistically dominant results.

All this is done without reading the value of the qubits which would make the whole system col-lapse. This is implemented with ancilla qubits that are used to detect error syndromes without af-fecting the qubits used in calculation.

The trick consists in duplicating the information on several qubits and do qubits rotations in the Bloch sphere then some projective measurement.

This will not deteriorate the information contained in the qubits. This measurement enables the de-tection of error syndromes. We then use single-qubit gates to correct the qubits for which an error was detected. It goes through some classical processing.

The QEC zoo also contains topological codes including **surface codes** and **color codes** and many other specimens such as the **DFS** (Decoherence Free Subspaces) protocol that encodes quantum information in a subspace that is unaffected by physical errors or so-called holographic codes<sup>305</sup>. This scientific field is prone to a lot of creativity!

---

<sup>301</sup> This theme has, like many quantum specialties, its own conference. See [International Conference on Quantum Error Correction](#) and the [videos](#) with all the presentations of the 2019 edition.

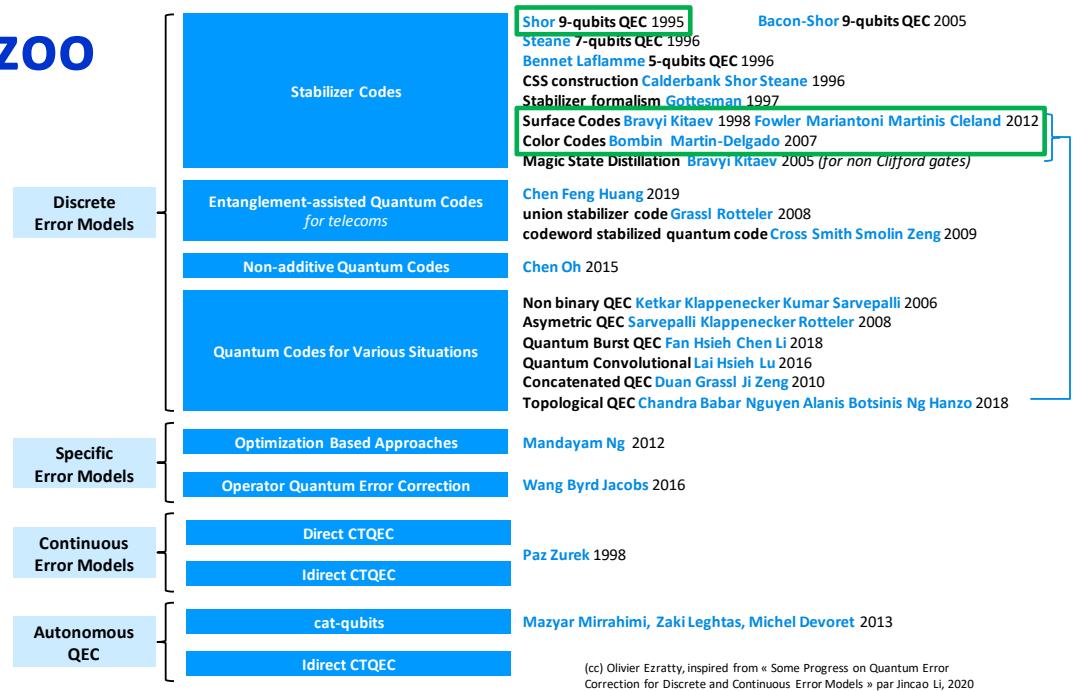
<sup>302</sup> Cat-codes are used by the startup Alice&Bob. Knowing that their creation goes back to the work of Mazyar Mirrahimi and Zaki Leghtas in 2013, with whom the founders of Alice&Bob worked. Error correction codes are constantly being updated. Thus, a pro-posal recently emerged from QEC that goes further than cat-code and does not depend on hardware architecture. See [Novel error-correction scheme developed for quantum computers](#), March 2020 which refers to [Quantum computing with rotation-symmetric bosonic codes](#) by Arne L. Grimsmo, Joshua Combes and Ben Q. Baragiola, September 2019.

<sup>303</sup> Illustration inspired by a scheme discovered in [Some Progress on Quantum Error Correction for Discrete and Continuous Error Models](#) by Jincao Li, 2020 (15 pages).

<sup>304</sup> See [Quantum Error Correction for Beginners](#) by Simon J. Devitt, William J. Munro, and Kae Nemoto, 2013 (41 pages).

<sup>305</sup> Color codes are variations of stabilizing codes. See some explanations in [The Steep Road Towards Robust and Universal Quantum Computation](#) by Earl T. Campbell, Barbara M. Terhal and Christophe Vuillot, 2016 (10 pages).

# QEC ZOO



There is also a method based on **neural networks**, developed by researchers at the University of Erlangen in Germany<sup>306</sup>.

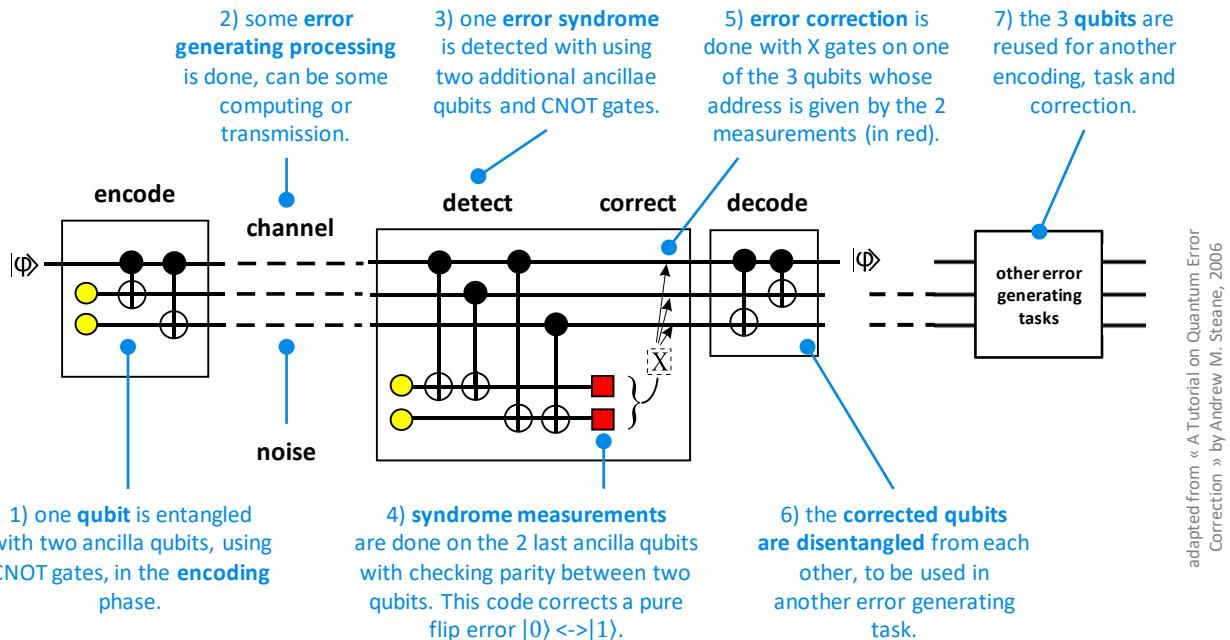
The general principle of a classical quantum error correction code is illustrated in the diagram *below* with a six-step correction<sup>307</sup>:

1. **Encoding:** the qubit to be corrected will first be replicated a certain number of times via CNOT gates on several auxiliary qubits (here 2). The resulting qubits are entangled. In the example, we get the state  $\alpha|000\rangle + \beta|111\rangle$  for an input state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ .
2. **Processing:** it will potentially generate an error coming from various sources of noise. This can be a calculation as well as some telecom transmission of a qubit.
3. **Detection:** one or more error syndromes are detected via quantum gates that associate qubits with other ancilla qubits. In the example below, it detects pure flip errors.
4. **Measurement:** the state of these ancilla qubits is measured to become classical bits. It creates the index of the qubit to be corrected in the upper 3 qubits. This is some non-destructive measurement for the corrected entangled qubits since it's done in a different basis.
5. **Correction:** the address obtained with syndrome measurement is used to correct the faulty qubits with an X gate (for a phase error, we'd use a Z gate). There are alternative forms of QEC that do not involve the measurement of the syndrome by qubit reading but by its direct use with quantum gates that correct the defective qubit without going through conventional bits.
6. **Consolidation:** finally, the corrected qubits are disentangled to recreate an isolated corrected qubit  $|\psi\rangle$ . This consolidation seems to be used with error correction for quantum telecommunications. When applied to quantum computing, the corrected entangled qubits can be kept to move on to the next step, i.e. another computing operation to be corrected.

<sup>306</sup> Seer [Neural networks enable learning of error correction strategies for quantum computers](#), October 2018 and [Reinforcement Learning with Neural Networks for Quantum Feedback](#), Thomas Fösel et al, 2018 (7 pages).

<sup>307</sup> Based on [A Tutorial on Quantum Error Correction](#) by Andrew M. Steane, 2006 (24 pages). See also [An introduction to quantum error correction](#) by Mazyar Mirrahimi, 2018 (31 slides).

7. **Reuse**: the correct qubit or qubits can now be used for subsequent operations that will also be corrected with the same process.



Error correction codes charts such as Shor's on [Wikipedia](#) are usually not complete. They usually lack the measure/correction. They can rely on direct error correction<sup>308</sup>.

They also do not specify where to place the error correction codes in a quantum algorithm. It seems that this is required at each and every stage of some quantum computation. Error correction codes will be repeated a number of times that is roughly proportional to the computational depth of the quantum algorithm. It will be the role of the compilers to position QEC in the code sent to the quantum accelerator. It may depend on their knowledge of the fidelity rates of the quantum gates used in the hardware. In the end, the QEC will increase computation time by one to several orders of magnitude depending on the ratio of physical qubits per logical qubits. It has to be taken into account when evaluating the time-based quantum computing advantage brought by a given algorithm.

Looking at the genealogy of these error correction codes, we must start with the simplest ones that correct qubit sign errors with three qubits like the example above from Andrew Steane. A similar QEC corrects qubit phase errors by exploiting Hadamard gates<sup>309</sup>.

The 1995 **Shor's 9-qubit error correction code** consolidates these two methods, with the corrected qubit being replicated 8 times. This code corrects both flip and phase errors<sup>310</sup>.

Here is what such a complete code looks like<sup>311</sup>. In the first phase the corrected qubit is replicated two times and each resulting qubit is again replicated two times with CNOT gates. The first three blocks of 3 qubits implement a flip error correction. It outputs 3 qubits which then implement a phase error correction.

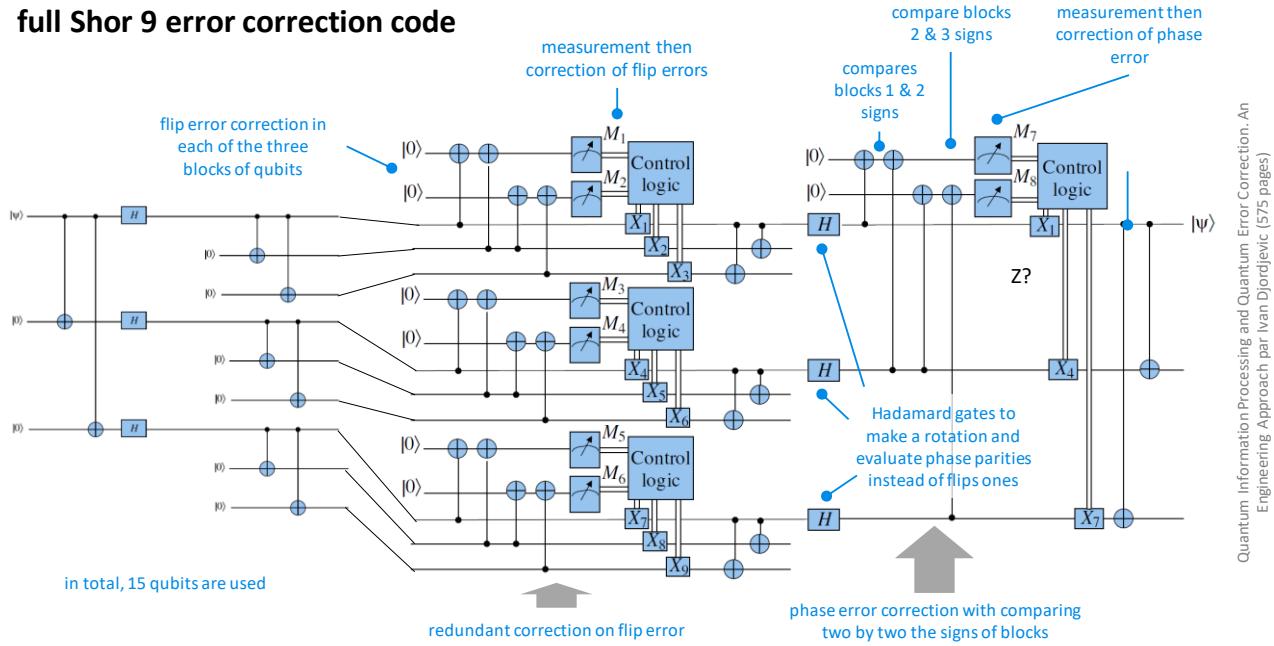
<sup>308</sup> See [Quantum Error Correction An Introductory Guide](#) by Joschka Roffe, 2019 (29 pages) which explains the generic operation of error correction codes and [Quantum Error Correction for Beginners](#) by Simon Devitt, William Munro and Kae Nemoto, 2013 (41 pages). These are the two main sources of information that allowed me to write these pages on QEC. See also a description of various error correction codes in [Software for Quantum Computation](#), a thesis by Daniel Matthias Herr from ETH Zurich, 2019 (164 pages).

<sup>309</sup> Source of the diagram: [Quantum error correction](#) by Fred Bellaïche, April 2018.

<sup>310</sup> The details of the process are well documented in the [Wikipedia sheet of quantum error correction](#).

<sup>311</sup> Adapted from a schema found in [Quantum Information Processing and Quantum Error Correction. An Engineering Approach](#) by Ivan Djordjević (575 pages).

## full Shor 9 error correction code



**Raymond Laflamme** (1960, Canada) demonstrated in 1996 that at least five physical qubits are needed to create a "logical qubit" integrating flip and phase error correction. With Emanuel Knill, he also demonstrated that any single qubit error was a linear combination of flip and phase errors, leading to factoring error correction to flip and phase errors corrections<sup>312</sup>.

In practice, the 7-qubit **Steane** code is the most referenced because it is not redundant like the Shor code. These 3-, 5-, 7- and 9-qubit codes are part of a generic group called **stabilizer codes** formalized by Daniel Gottesman in 1997. We are now going to dig a little deeper into how they work.

### Projections and stabilizers

We will better understand how an error correction works without reading the state of the qubit to be corrected. Let's take the case of a simple flip error correction code with three qubits.

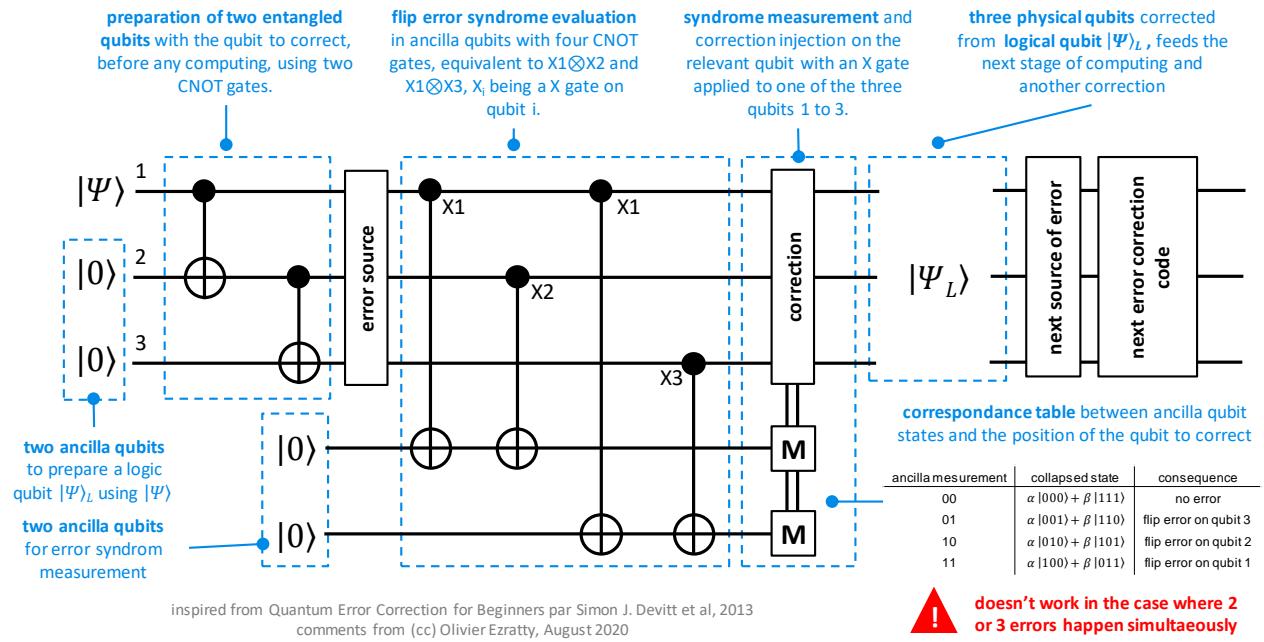
These three entangled qubits can have an error  $X_1$ ,  $X_2$  or  $X_3$  or no error ( $I$ =identity).  $X$  is an amplitude inversion Pauli gate. It creates an amplitude inversion of the corresponding entangled qubit as shown in the equations. These new states correspond to three errors and the absence of errors.

$$\begin{aligned} |\psi_L\rangle &= \alpha|000\rangle + \beta|111\rangle \xrightarrow{I} \alpha|000\rangle + \beta|111\rangle, \\ |\psi_L\rangle &= \alpha|000\rangle + \beta|111\rangle \xrightarrow{X_1} \alpha|100\rangle + \beta|011\rangle, \\ |\psi_L\rangle &= \alpha|000\rangle + \beta|111\rangle \xrightarrow{X_2} \alpha|010\rangle + \beta|101\rangle, \\ |\psi_L\rangle &= \alpha|000\rangle + \beta|111\rangle \xrightarrow{X_3} \alpha|001\rangle + \beta|110\rangle. \end{aligned}$$

These four states have the interest of being mathematically orthogonal for all the values of the  $\alpha$  and  $\beta$  defining the state of the qubit to be corrected. The trick is to perform a measurement of these values in the vector space corresponding to these four values and not in the original qubit computational base. This will not deteriorate the superposition of the original qubit. The syndrome extraction is called a "Stabilizer code" or "stabilization code", which will feed the ancilla qubits. The process is the same to evaluate and correct a phase error but with  $Z$  gates instead of  $X$  gates.

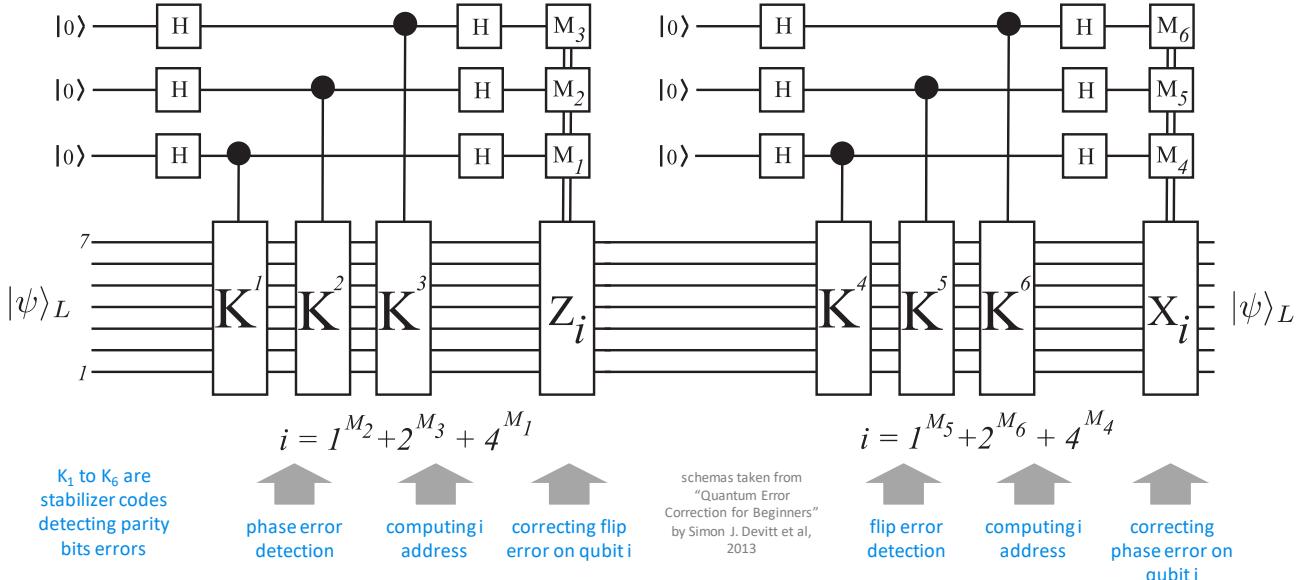
<sup>312</sup> This is demonstrated in [A Theory of Quantum Error-Correcting Codes](#) by Emanuel Knill and Raymond Laflamme, 1996 (34 pages). But also independently in [Mixed State Entanglement and Quantum Error Correction](#) by Charles Bennett, David DiVincenzo, John A. Smolin and William K. Wootters, 1996 (82 pages). See also [Magic States](#) by Nathan Babcock (28 slides).

### 3 qubits flip error correction code



The disadvantage of the solution is that it cannot detect errors that would occur at the same time on two or three of the entangled qubits. No error-correcting code can correct all errors!

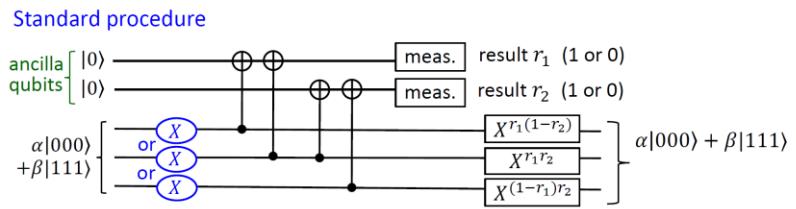
### 7 qubits error correction code named [[7,1,3]] in the stabilizers formalism



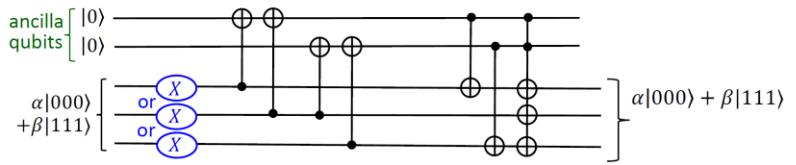
The stabilizer codes formalism generically describes the error correction codes we have just studied with three parameters:  $[[n, k, d]]$ .  $n$  is the number of physical qubits used in the code.  $k$  is the number of logical qubits, usually 1, and  $d$  is the smallest number of simultaneous qubit errors that can transform one valid codeword into another. In this notation, Shor's 9 qubit code is a  $[[9, 1, 3]]$ , Steane's is a  $[[7, 1, 3]]$ , Laflamme's is a  $[[5, 1, 3]]$  and a 3-qubit flip or phase correction code is a  $[[3, 1, 1]]$  stabilizer code.

The stabilizer codes use a syndrome table that provides a correspondence between the errors on each qubit and the detected syndrome. The number of ancilla qubits used to create this table must therefore be sufficient to identify the qubits to be corrected in the logical qubit. In the above example with a logical qubit with 7 physical qubits, the 3 ancilla qubits allow the identification of eight scenarios, sufficient to determine which of the 7 physical qubits must be corrected. The eighth scenario is the absence of error, therefore needing no correction.

It seems that the qubits correction can be applied in two manners: the one presented so far with a measurement of ancilla parity qubits generating classical bits allowing to determine on which qubits to apply a quantum error correction gate, and another method allowing this without the measurement and to apply the correction directly with quantum gates. The first solution seems to be more commonly used.



**Automated version:** replace measurement with controlled operation



The autonomous method also branded aQEC (autonomous quantum error correction) would be more energy and time saving (comparison *above*<sup>313</sup>). It is also a way to possibly run the error correction autonomously within a quantum processor, without going through the classical part, should qubits control be performed very close to the qubits. But in that case, the ancillas can't be reused. Some energy dissipation must be handled, using a technology called reservoir engineering, which is actually implemented in cat-qubits<sup>314</sup>. Otherwise, whatever, the ancilla qubits used in QEC must be reset to |0⟩ and this reset is a dissipative process. The thermal bath is just elsewhere!

## Continuous error correction

Juan Pablo Paz and Wojciech Zurek proposed in 1998 a continuously operating error correction code, the CTQEC, for "continuous-time QEC" based on differential equations and acting at reduced time intervals. There are two methods for acting directly on the information (direct CTQEC) or via auxiliary qubits (indirect CTQEC). It could perhaps be useful on the side of quantum telecommunications.

## Logical Qubits

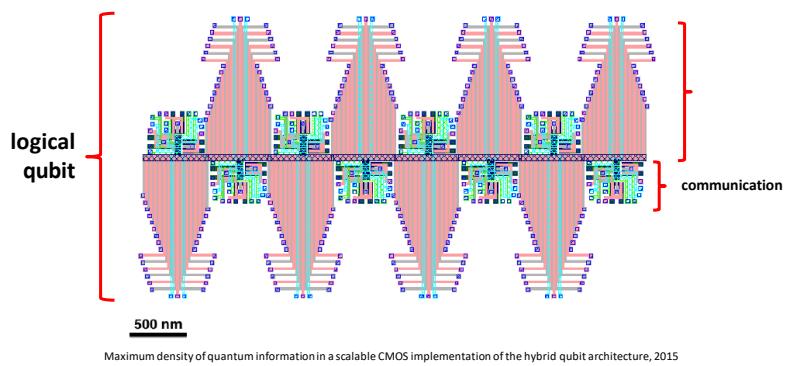
With quantum computers available online such as those from IBM having up to a few dozen qubits, it is the role of software to implement dynamic error correction codes and more precisely, compilers that will transform the developer's code into executable machine code at the physical level of the qubits and integrating QEC code. Given that we have just enough qubits to test small QEC like Steane's 7-qubits codes.

At one point in time, logical qubits will maybe be implemented entirely in the hardware architecture, exposing logical qubits to the classical computer driving the quantum accelerator. This will simplify the connection between the classical control computer and the quantum processor.

<sup>313</sup> Seen in [Quantum error correction \(QEC\)](#) by Alexander Korotkov, 2017 (39 slides). [List of all courses](#) on quantum computing.

<sup>314</sup> See [Protecting a Bosonic Qubit with Autonomous Quantum Error Correction](#) by Jeffrey M. Gertler et al, University of Massachusetts-Amherst and Northwestern University, October 2020 (23 pages). This study investigates autonomous QEC on bosonic codes qubits using reservoir engineering. See also [Autonomous quantum error correction and quantum computation](#) by Jose Lebreuilly et al, Yale, Amazon and University of Chicago, March 2021 (18 pages) and [Autonomous quantum error correction with superconducting qubits](#) by Joachim Cohen, ENS Paris, 2017 (164 pages).

A QEC (Quantum Error Correction) could be performed at the hardware level by creating qubit assemblies that generate ready-to-use physical logical qubits. Here is an old example with seven superconducting physical qubits to create one simple logical qubit<sup>315</sup>. The number of physical qubits to be assembled to create a logical qubit depends on the error rate of the qubits.

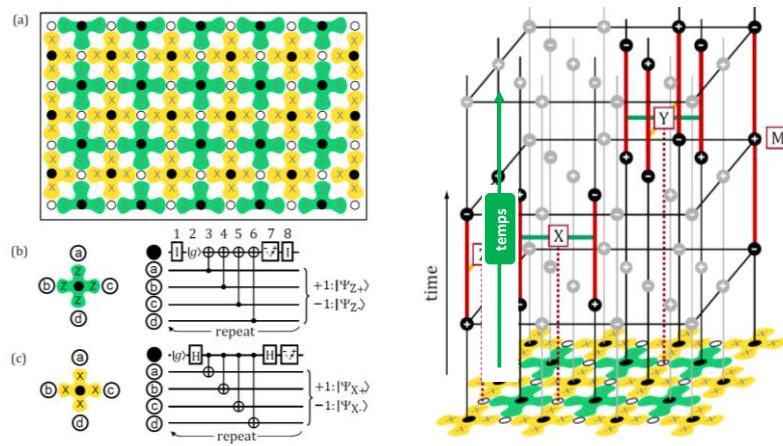


Maximum density of quantum information in a scalable CMOS implementation of the hybrid qubit architecture, 2015

The higher the qubit error rate, the more qubits must be assembled. This number can reach several thousand qubit physical qubits<sup>316</sup>.

We're still a long way from that! Current estimates are 10,000 physical qubits to get a logical qubit. This corresponds to the plans published by **IBM**, **Google** and **PsiQuantum** with 100 logical qubits created out of one million physical qubits. On the physical architecture side, **topological qubits** are an analog version of *surface codes* that should allow to reduce this ratio of logical/physical qubits, just like cat-qubits, which are forecasted to require fewer than 100 physical qubits to create one logical qubit.

Trapped ions can use **lattice surgery** to connect and entangle these topologically corrected physical qubits<sup>317</sup>. **IonQ** is planning to create logical qubits corrected with a Bacon-Shor QEC (a variation of Shor's code with 13 qubits<sup>318</sup>) thanks to their much better fidelities<sup>319</sup>. For qubits that can be organized in such a way as to be physically well connected with their immediate neighbors, the most often considered error correction is the **surface code**, created in 2012.



Surface codes: Towards practical large-scale quantum computation, 2012

It uses matrices of processing qubits (in white in the diagram *opposite*) connected to measuring qubits (in black) via **Pauli X** (inversion) and **Pauli Z** (phase change) gates.

<sup>315</sup> It comes from [Maximum density of quantum information in a scalable CMOS implementation of the hybrid qubit architecture](#), 2015 (17 pages).

<sup>316</sup> See [What determines the ultimate precision of a quantum computer?](#) by Xavier Waintal, 2019 (6 pages) which describes the limits of error correction codes. Other useful contents on error correction include: [Error mitigation in quantum simulation](#), Xiao Yuan, IBM Research, 2017 (42 minutes), [Code Used To Reduce Quantum Error In Logic Gates For First Time](#), 2019, [Scientists find a way to enhance the performance of quantum computers](#) by the University of Southern California, 2018 and [Cramming More Power Into a Quantum Device](#) by Jay Gambetta and Sarah Sheldon, March 2019 about the error level of the IBM Q System One announced in January 2019.

<sup>317</sup> See [Error protected quantum bits entangled](#), University of Innsbruck, January 2021 referring to [Entangling logical qubits with lattice surgery](#) by Alexander Erhard et al, Nature, 2020 (15 pages).

<sup>318</sup> Bacon-Shor code is documented in [Operator Quantum Error Correcting Subsystems for Self-Correcting Quantum Memories](#) by Dave Bacon, 2006 (17 pages).

<sup>319</sup> And [Fault-Tolerant Operation of a Quantum Error-Correction Code](#) by Laird Egan, Christopher Monroe et al, 2020 (23 pages).

This gives two ancilla qubits for two physical qubits organized in the logic below to correct flip and phase errors. This constitutes a stabilizer code of type  $[[5, 1, 2]]$  gathering four blocks with four cycles (diagram *below*, right). These surface codes are tolerant to a higher error rate of the qubits, on the other hand, they require a higher number of physical qubits per logical qubits. Surface codes create a design constraint for physical qubits that must be able to be connected to their immediate neighbors in a 2D structure<sup>320</sup>. This currently gives an advantage to Google's qubit topology over IBM's topology for superconducting qubits, which we will visualize in a later section, that starts page 252.

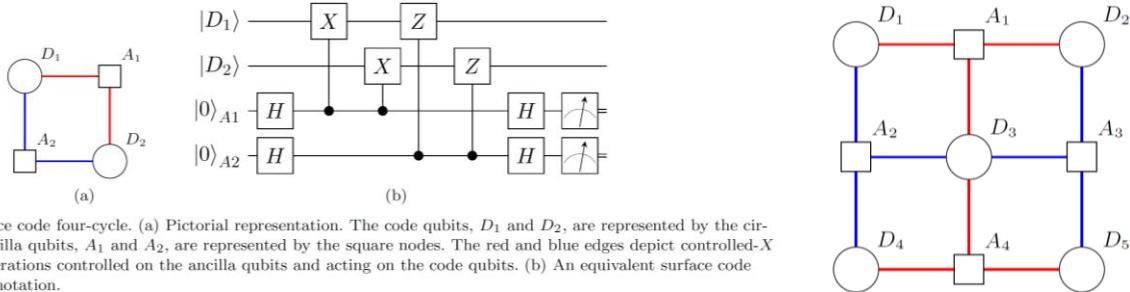


Figure 7. The surface code four-cycle. (a) Pictorial representation. The code qubits,  $D_1$  and  $D_2$ , are represented by the circular nodes. The ancilla qubits,  $A_1$  and  $A_2$ , are represented by the square nodes. The red and blue edges depict controlled- $X$  and controlled- $Z$  operations controlled on the ancilla qubits and acting on the code qubits. (b) An equivalent surface code four-cycle in circuit notation.

Another method is to use a **lattice-surgery** to connect logical qubits as proposed with trapped ions.

In July 2021, **Google** and **Honeywell Quantum Systems** both announced the creation of the first logical qubits with respectively 21 and 10 qubits, showing a real improvement in the error rate of these logical qubits when compared to their underlying physical qubits<sup>321</sup>.

## Fault-Tolerant Quantum Computing

QEC is the path to creating fault-tolerant quantum computers, and its next step, large-scale quantum computing, respectively **FTQC** (fault-tolerance quantum computing) and **LSQC** (for large-scale quantum computing).

FTQC is based on a few general principles: error-tolerant state preparation, error-tolerant quantum gates, error-tolerant measurement and error-tolerant error correction. Indeed, error correction codes can themselves introduce errors since they use quantum gates and state measurements which themselves generate errors. Moreover, error correction codes do not correct all possible errors. They just increase the apparent fidelity rate of the corrected qubits.

FTQC also involves the use of error correction codes repeatedly during long calculations, without introducing more errors than are corrected. Quantum error correction codes should not spread errors in an uncontrollable way to various qubits in the computing register.

*“Whatever comes out of these gates, we have a better chance to survive if we work together. You understand?*

*We stay together, we survive.”*

General Maximus Decimus Meridius  
(Russell Crowe) in Gladiator, 2000.

<sup>320</sup> Surface codes are well formalized in [Surface codes towards practical large-scale quantum computation](#), 2012 (54 pages) but their source of inspiration is older and comes from [Quantum codes on a lattice with boundary](#) by Sergey Bravyi and Alexei Kitaev, 1998 (6 pages). In practice, the structure of surface codes is quite complex and involves activated and deactivated substructures in the qubit matrix.

<sup>321</sup> For Google's logical qubit, see [Exponential suppression of bit or phase errors with cyclic error correction](#) by Zijun Chen et al, February 2021 in Arxiv and in Nature in July 2021 (6 pages) and [supplemental materials](#) (30 pages). And [Realization of real-time fault-tolerant quantum error correction](#) by C. Ryan-Anderson et al, HQS, July 2021 (22 pages). It uses a 10 qubit trapped-ion quantum computer to encode a single logical qubit using the Steane  $[[7, 1, 3]]$  color code.

QEC then theoretically allows to execute algorithms of arbitrary length, whereas without QEC, we are limited to a few series of gates. The challenge is to ensure that the calculation and QEC prevents errors from cascading. We must avoid linking one qubit with too many qubits with multi qubit gates in QECs.

For this respect, a 7-qubits Steane code is appropriate. And let's not forget that a CNOT gate propagates flip errors from the control qubit to the target qubit and phase errors from the target to the control.

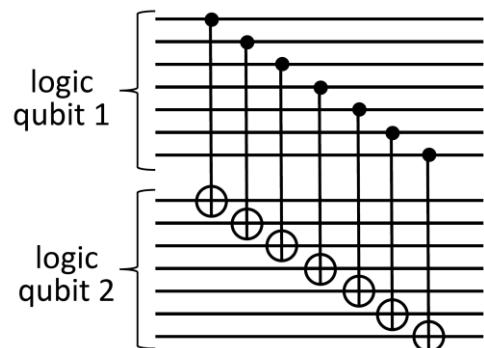
From an operational standpoint, FTQCs creation involves minimizing the number of ancilla qubits and optimizing the choice of QECs according to the type of errors generated by each type of qubit and quantum gates.

FTQC integrates a special mechanism for the correction of errors coming from quantum gates using entanglement: **transversal gates**. It is an arrangement of links between logical qubits linked together by two-qubit gates. The diagram illustrates these links between two logic qubits using a 7 qubit Steane code via CNOT gates. Each of the physical qubits of the logical qubits is connected one by one between the two logical qubits. This is still very theoretical, besides trapped ions, no qubit topology enables this kind of connectivity.

One of the problems is that error correction generates an overhead that grows faster than the exponential gain of the quantum computer ( $2^{4n}$  vs  $2^n$  according to Quantum Benchmark)<sup>322</sup>.

We can get some comfort from the **threshold theorem** demonstrated by Dorit Aharonov and Michael Ben-Or in 1999 according to which it is possible to perform error correction up to an arbitrary desired apparent error rate if the error rate of the single-qubit gates is below a given threshold which is dependent on the error correction code used and the characteristics of the qubits<sup>323</sup>.

This rate would be between 0.1% and 1% but is subject to change. The consequence of this theorem is to allow the application of error correction codes recursively until reaching the desirable error rate to execute a given algorithm. This is however based on the assumption that our qubits fidelity is stable as their number is growing, a feat that is not yet achievable!



#### Concatenation of codes $C_1$ (size $n_1$ ) and $C_2$ (size $n_2$ )

We construct a code of size  $n_1 n_2$ , where each qubit of  $C_2$  is replaced by a block of  $n_1$  qubits encoded in  $C_1$ .

#### Higher order QEC by concatenation

Level of concatenation	Error probability
Physical qubits	$\square_0 = p$
1 <sup>st</sup> encoded level	$\square_1 = cp^2 = c^{\square_1} (cp)^2$ (*)
2 <sup>nd</sup> encoded level	$\square_2 = c(cp^2)^2 = c^{\square_2} (cp)^{2^2}$
$\vdots$	$\vdots$
r <sup>th</sup> encoded level	$\square_r = c(\square_{r-1})^2 = c^{\square_r} (cp)^{2^r}$

(\*) For the Steane code  $c \approx 10^{-4}$

<sup>322</sup> To learn more about error correction, see in particular this presentation [Surprising facts about quantum error correction](#) by Andrew Darmawan, Nicolas Delfosse, Pavithran Iyer and David Poulin, 2017 (178 slides).

<sup>323</sup> See [Fault-Tolerant Quantum Computation With Constant Error Rate](#) by Dorit Aharonov and Michael Ben-Or, 1999 (63 pages).

**Transversal gates.** What is difficult to achieve is to reconcile fault tolerance and universal gate-based quantum computing. A certain **Eastin–Knill** theorem states that no QEC code can transversely implement a universal gate set, particularly the inevitable T gate. Transversal gates avoid propagating errors beyond the corrected qubits. But the T gate can't be implemented in such a way, for example with a simple Steane code or a surface code. The workaround consists in using magic state distillation, which has a huge cost of two orders of magnitude for physical per logical gates, explaining why it's often estimated said that logical qubits require over 10K physical qubits (on top of the effect of code concatenations)<sup>324</sup>.

**QEC concatenation** is exploiting this recursivity of error correction codes<sup>325</sup>. A QEC generates logical qubits which can then be used as virtual physical qubits for a new QEC, and so on. With each recursion, the apparent error rate decreases.

We stop concatenating QEC codes when we reach an error rate compatible with the expected usage of the qubits. Concatenation can be optimized by using different types of QEC at each level of recursivity<sup>326</sup>. This theorem was demonstrated only for a 7-qubit Steane error correction code and not for surface codes, and for error rates that are not growing with the number of physical qubits. This is unfortunately not what is currently observed with the majority of qubit types!

**Qubits lifetime extension.** A nagging question may arise: if we need to accumulate error correction codes, don't we risk running into the wall of qubit decoherence, particularly with superconducting qubits? Well, no. As said before, error correction codes have the direct effect of artificially extending the coherence time of the qubit registers by several orders of magnitude<sup>327</sup>. Each correction is equivalent to a reset of the qubits decoherence times  $T_1$  (flip) and  $T_2$  (phase). This explains how Google could publish an optimized version of the Shor integer factoring algorithm with 20 million qubits running, but requiring 8 hours of run-time which is many orders of magnitude longer than their qubits coherence time that sits way under a tiny 100  $\mu\text{s}$ .

**Instruction bandwidth bottleneck** is yet another engineering challenge for FTQC and error correction. Thousands of physical qubits must be driven by software-based quantum error correction. It creates a digital workload from the classical control computer down to the physical qubits and their many ancilla qubits, in a range exceeding several tens of TB/s just for factoring a 1024 bits integer with Shor's algorithm! Specific architectures can be designed to handle QEC as close as possible to the physical qubits, ideally in cryo-electronics components and with some microcode sitting at the lowest possible stage in the cryostat (for solid-state qubits), starting at 4K<sup>328</sup>.

## Gates and non-discrete states

A Shor and Steane code can correct any Pauli error, including Y gate, which is equal to  $iZX$ . It can correct any linear combination of I, X, Y and Z gates with complex numbers. This comes from the fact that any unit operation on a qubit can be expressed as a combination of  $IXYZ$  with complex factors :  $U = aI + bX + cY + dZ$ .

<sup>324</sup> See [Roads towards fault-tolerant universal quantum computation](#) by Earl T. Campbell et al, 2018 (9 pages).

<sup>325</sup> Source for the illustration above: [Introduction to quantum computing](#) by Anthony Leverrier and Mazyar Mirrahimi, March 2020 (69 slides).

<sup>326</sup> See [Dynamic Concatenation of Quantum Error Correction in Integrated Quantum Computing Architecture](#) by Ilkwon Sohn et al, 2019 (7 pages).

<sup>327</sup> See [Extending the lifetime of a quantum bit with error correction in superconducting circuits](#) by Nissim Ofek, Zaki Leghtas, Mazyar Mirrahimi, Michel Devoret et al, 2016 (5 pages) which shows that thanks to a cat-code-based QEC, the lifetime of superconducting qubits can be extended by a factor of 20!

<sup>328</sup> See the QuEST architecture proposal in [Taming the Instruction Bandwidth of Quantum Computers via Hardware Managed Error Correction](#) by Swamit Tannu et al, GeorgiaTech, Stanford and Microsoft, 2017 (13 pages slides).

This means, indirectly, that these QECs should be able to correct analog and continuous errors such as slight variations in amplitude or phase, i.e. rotations of a few degrees in the Bloch sphere.

To correct these errors corresponding to gates outside the Clifford group such as a T gate (eighth of rotation in the Bloch sphere), however, **magic states** are also used which feed circuits made with gates from the Clifford group. These states are prepared by a process called **magic state distillation**<sup>329</sup>.

These codes are very important to take full advantage of quantum computing. This is related to the fact that quantum advantage over classical computation requires a set of universal classical gates that must include a gate that is not in Clifford's group, usually, the T gate. In order to correct the errors with a T gate, specific error correction codes are needed, such as **magic state distillation**, which is a kind of error correction code of error correction codes.

But magic state distillation has an enormous overhead with the number of required physical qubits to create one logical qubit, of about two orders of magnitude (x100). Magic state distillation is implemented in surface codes described above.

That's where **color codes** come into play<sup>330</sup>. It is a class of topological stabilizer codes along with toric codes and surface codes.

They have much less overhead than surface codes and render possible the implementation of FTQC (Fault-Tolerant Quantum Computing). It is due to one key feature of these correction codes: they can be implemented with the transversal gates described in the previous section on FTQC, page 214. It could be used with superconducting and electron spin quits.

However, what is colored in these colored codes and how does it work? I have no clear idea<sup>331</sup>. It's a highly specialized scientific domain with cryptic explanations<sup>332</sup>.

## Actual computing time

There are only a few studies and research done to evaluate how long it would take to execute specific quantum algorithms in an “end-to-end” fashion. We know that, theoretically, with a FTQC of 20 million qubits, we could factorize an RSA 2048 bits key in 8 hours with superconducting qubits. Gate time is quite variable from 12 ns for superconducting qubits to 100  $\mu$ s for trapped ions qubits.

You can get an idea of the timing overhead coming from three mechanisms :

- **Non-Clifford gates** creation overhead like R/Control-R gates with arbitrary phases, based on the Solovay-Kitaev theorem. It creates a x127 to x235 gates overhead!
- **Quantum error correction** (QEC) overhead. It creates a x10 to x20 gates overhead!

---

<sup>329</sup> See [Universal quantum computation with ideal Clifford gates and noisy ancillas](#) by Sergey Bravyi and Alexei Kitaev, 2004 (15 pages). There are other solutions such as [A fault-tolerant non-Clifford gate for the surface code in two dimensions](#) by Benjamin J. Brown, May 2020, which applies to surface codes.

<sup>330</sup> This is however not the only solution to the magic state distillation physical qubits cost. See [Fault-tolerant magic state preparation with flag qubits](#) by Christopher Chamberland and Andrew Cross, May 2019 (26 pages) which describes an alternative using more ancilla qubits (“flag qubits”).

<sup>331</sup> Here's a laundry list of concepts to understand: quantum many-body physics, classification of quantum phases, topological phases and the likes.

<sup>332</sup> See for example [The ABCs of the color code](#) by Aleksander Marek Kubica, 2018 (205 pages), a rich thesis done under the supervision of John Preskill at Caltech with the help from Jason Alicea, Fernando Brandão and Alexei Kitaev. And [The cost of universality: A comparative study of the overhead of state distillation and code switching with color codes](#), by Michael E. Beverland, Aleksander Kubica and Krysta M. Svore, 2021 (69 pages).

- **Number of runs** or shots required to average probabilistic results. IBM advises using 4000 runs but this number may grow with the number of used qubits. So, a x4000 overhead! But we can anticipate that this number may not be that high with logical (error corrected) qubits.

					+QEC x20	x4000	x20x4000 = 80 000 gates
					+QEC x20	x4000	x3x20x4000 = 240K gates
					+QEC x20	x4000	x127x20x4000 = 10M gates
<b>approximation overhead</b> controlled-R and R phase change may require up to 127 series of gates from a Clifford+T gates set	<b>QEC overhead</b> one usual gate QEC requires at least 10 to 20 series of gates, including some readouts	<b>runs overhead</b> several executions to turn probabilistic results into deterministic result	<b>total overhead</b> a single « logical gate » on a « logical qubit » may require up to 10M physical gates				

one performance indicator of quantum computing is the quantum gates speed

it depends of the qubit types and implementation: 12 ns to 300 ns for superconducting qubits, 1  $\mu$ s for cold atoms, 10 ns to 5  $\mu$ s for electron spins, 100  $\mu$ s for trapped ions and 1 ms for photon qubits (which may rely on an MBQC technique, making these numbers irrelevant).

I tentatively added these three mechanisms for three scenarios: an H gate, a SWAP gate assembled with three CNOT gates and an arbitrary R gate created with a Clifford gates set plus a T gate using the Solovay-Kitaev approximation theorem. Adding all these timing overheads, you obtain between 80K and 10M gates to run to execute a single physical gate. That's quite significant! Interestingly, the longer the gates, like with trapped ions qubits, the better fidelity they have, creating a balancing effect between the QEC overhead and the gates times. All this should be taken into account when dealing with so-called quantum algorithms speedups, particularly with non-exponential speedups.

## Quantum memory

We would guess that quantum memory is some memory capable of storing the quantum state of qubits and then using them to feed quantum computer registers<sup>333</sup>. It should be able to store superposed and entangled qubits and deliver it to whatever computing is needed. But it is part of a broader category defined as “quantum RAM” or qRAM, which is able to store either classical or quantum data, the data being queried with superposed quantum addresses.

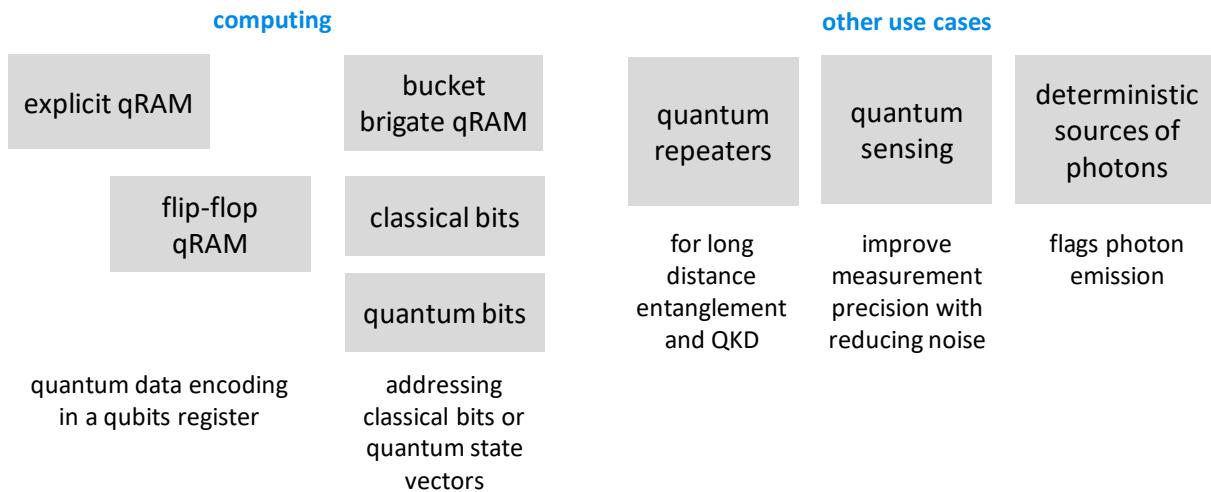
Quantum memory is also required in quantum key distribution repeaters<sup>334</sup> and can be useful in various situations like with quantum sensing and for creating deterministic sources of photons<sup>335</sup>. However, we focus here on the first category of quantum memory, aimed at quantum computing. It is a very diverse one with different logical and physical architectures.

---

<sup>333</sup> See [Architectures for a quantum random access memory](#), by the Italians Vittorio Giovannetti and Lorenzo Maccone and the American Seth Lloyd, 2008 (12 pages).

<sup>334</sup> Here's one example with [One-hour coherent optical storage in an atomic frequency comb memory](#) by Yu Ma et al, April 2021 (6 pages) and another one with [Space-borne quantum memories for global quantum communication](#) by Mustafa Gündoğan et al, 2020 (11 pages).

<sup>335</sup> See [Quantum memories - A review based on the European integrated project “Qubit Applications \(QAP\)”](#) by C. Simon et al, 2010 (22 pages).



(cc) Olivier Ezratty, June 2021

## Quantum algorithms requirements

One anticipated usage of quantum memory is to temporarily store the state of a qubit register during a data preparation process, a usual lengthy process, before transferring it to a faster quantum processing unit. With  $N$  qubits, this memory would be able to store in theory  $2^N$  different computational vector states amplitude values.

According to the non-cloning theorem, the content of this memory cannot be the copy of the state of other quantum registers. In computing, quantum memory is used to store data into some quantum memory to be later used in quantum processing. Data preparation and encoding depends on the algorithm. It is necessary for certain types of quantum algorithms such as Grover's search and quantum machine learning algorithms that we will describe later on<sup>336</sup>.

The most demanding encoding is when you encode a vector of  $2^N$  values (well, minus 1 for normalization constraints) in the whole computational state vector<sup>337</sup>. This creates a superposition with all or some of the basis states from the computational basis. Namely, we encode a vector  $\mathbf{x}$  containing  $2^N$  real (or even complex) number values from  $x_0$  to  $x_{2^N-1}$  with the normalization constraint that the square of these values is equal to 1. It ends up creating the state vector on the right with  $2^N$  amplitudes  $x_i$  associated with the vectors  $|i\rangle$  from the computational basis. This is called amplitude encoding.

$$\sum_{i=1, 2^N} x_i^2 = 1$$

normalization constraint

$$\sum_{i=1, 2^N} x_i |i\rangle = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{2^N-1} \end{bmatrix}$$

encoded state vector

Since this data encoding grows exponentially with the number of qubits, it may erase any computing speedup we would gain later. So, this is efficient only if we find a way to make this fast. One solution is to encode sparse vectors where only a few values are non zero.

## qRAM types

There are several types of qRAM:

- **Explicit qRAM** encodes data in physical qubits and then, use quantum circuits to extract the encoded data. There is no specific addressing system to selectively access parts of this memory.

<sup>336</sup> See [Quantum Machine Learning and qRAM](#) by Behnam Kia, 2018 (59 slides) as well as [Quantum Algorithms for Linear Algebra and Machine Learning](#) by Anupam Prakash, 2014 (91 pages).

<sup>337</sup> See [Quantum 101: Do I need a quantum RAM?](#) by Olivia Di Matteo, May 2020 (58 slides).

This is the scenario depicted above. Also named QAQM for Quantum Access Quantum Memory and Quantum Access Memory<sup>338</sup>.

- **Flip-flop qRAM** is a variant of explicit qRAM based on qubits circuit algorithms used to efficiently load classical data in a qubit register<sup>339</sup>.
- **Implicit qRAM** was proposed by Seth Lloyd et al in 2008 with the **bucket brigade** addressing system, based on a qutrits tree (three states quantum objects) containing wait/left/right flags<sup>340</sup>, sort of decision trees to reach the right memory cell. Also named QACM for Quantum Access Classical Memory.

This quantum addressing system can be used for accessing both *classical* bits and *coherent states* in qubits. The first case may be useful when building some oracles for algorithms like a Grover search. In the full quantum case, the coherent superposition of these addresses enables a readout of a superposition of many states amplitudes in the computational basis. Namely, we can query a given amplitude  $\alpha_i$  of the computational basis vector at the  $i$  address, encoded in binary with  $N$  classical bits or several of these, encoded in superposition.

$$\sum_j \alpha_j |j\rangle |0\rangle$$

$\alpha_j$  weighted superposition of addresses corresponding to computational basis states  $|j\rangle$

$$\sum_j \alpha_j |j\rangle |b_j\rangle$$

result of query, weights are applied to  $|b_j\rangle$  j-th memory location

In classical RAM, the memory array of  $N$  bits ( $2^N$ ) is usually organized in a 2-dimensional lattice which requires  $O(\sqrt{N})$  switches, precisely, usually a fixed number of address data to address lines and columns in memory chipsets. In bucket brigade qRAM, this can decrease to  $O(\log N)$  to address a particular computational basis vector amplitude. But this has to take into account the burden of any quantum error correction<sup>341</sup>. Various implementations of the bucket brigade solution have been proposed so far, including one using quantum walks, with the benefit of being more robust to decoherence and easier to parallelize<sup>342</sup>.

Before any qRAM data transfer to computation qubits can be done, an uncompute processing must be implemented that remove the selected computational basis vectors addresses from the related data.

In the end, when quantum data is transferred from quantum memory to computing qubits, it is achieved with teleporting the memory qubits to the computing one by one, usually with using entangled photons and, in many cases, some conversion from solid qubits to photon qubits (spin or charge to photons and the other way around). This teleportation is supposed to preserve the superposition and entanglement between the memory qubits during this transfer. Given there must be some errors generated during the transfer, which will require their own error correction codes.

<sup>338</sup> See [Quantum Associative Memory](#) by Dan Ventura and Tony Martinez, 1998 (31 pages).

<sup>339</sup> See [Circuit-based quantum random access memory for classical data with continuous amplitudes](#) by Tiago M. L. de Veras et al, 2020 (11 pages) referring to [Circuit-based quantum random access memory for classical data with continuous amplitudes](#) by Daniel K. Park et al, 2019 (9 pages).

<sup>340</sup> See [Quantum random access memory](#) by Vittorio Giovannetti, Seth Lloyd et al, 2008 (4 pages) and [Architectures for a quantum random access memory](#) by Vittorio Giovannetti, Seth Lloyd and Lorenzo Maccone, 2008 (12 pages).

<sup>341</sup> The QEC burden may be significant. also [On the Robustness of Bucket Brigade Quantum RAM](#) by Srinivasan Arunachalam et al, 2015 (19 pages) which shows that the timing advantage of qRAM bucket brigade addressing may be quickly lost due to QEC overhead. See also [Quantum Random Access Memory](#) by Aaron Green and Emily Kaplitz, 2019 (12 pages) and [Methods for parallel quantum circuit synthesis, fault-tolerant quantum RAM, and quantum state tomography](#) by Olivia Di Matteo, 2019 (111 pages) and [Fault tolerant resource estimation of quantum random-access memories](#) by Olivia Di Matteo et al, 2020 (14 pages).

<sup>342</sup> See [Quantum random access memory via quantum walk](#) by Ryo Asaka et al, 2021 (13 pages).

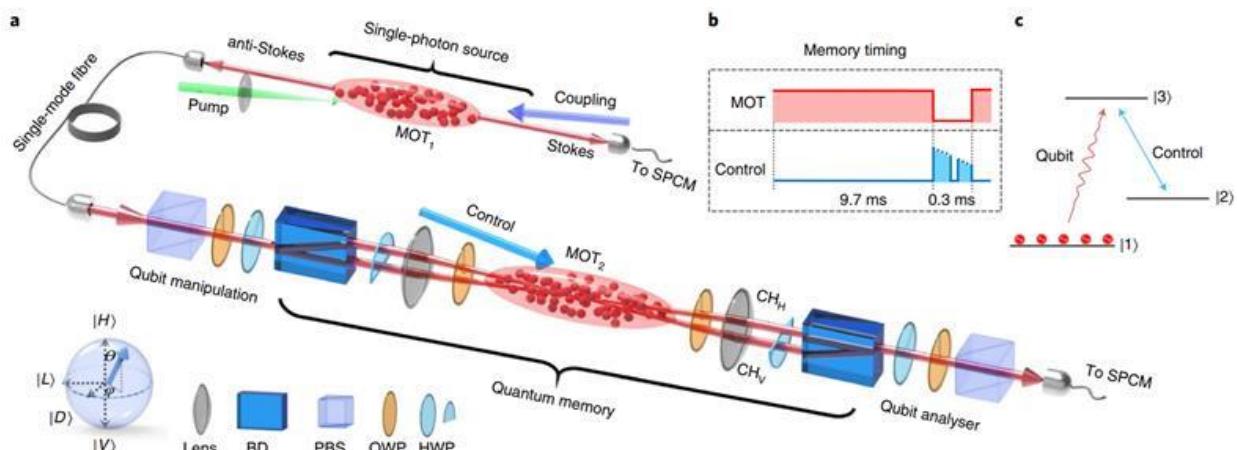
## Quantum memory physical implementations

None of the different quantum memory architectures studied over the last two decades is working yet. However, research is making progress, with targeted use cases that are more related to secure telecommunications and for quantum optical repeaters. At this stage, the advent of qRAM for quantum computing is more difficult to predict than scalable quantum computing!

The most promising quantum memory technologies are coupling cold atoms and photon polarization<sup>343</sup>:

- **Cold atoms and light polarization.** Chinese scientists used in 2019 the storage of the circular polarization state of a single photon trapped in a laser-cooled rubidium structure in a magneto-optical trap and thus made transparent<sup>344</sup>.

Rubidium atoms are cooled with lasers to  $200 \mu\text{K}$ . The same year, another team in China created a 105 qubits memory using 210 memory cells and dual-rail representation of a photon-based qubits with fidelities of 90% but these qubits seem not entangled and thus, not able to store a full state vector with  $2^N$  values, but only a N or 2N values using basis encoding in each individual qubit<sup>345</sup>. Other techniques are based on cesium with fidelities reaching 99%<sup>346</sup>.



**Fig. 1 | Experimental set-up and energy level scheme of the single-photon quantum memory.** **a**, Schematic of the experimental optical set-up. The cold atoms in the first magneto-optical trap (MOT<sub>1</sub>) serve as a nonlinear optical medium for producing time-frequency entangled photon pairs, while the cold atoms in the second magneto-optical trap (MOT<sub>2</sub>) are the medium for the quantum memory. The anti-Stokes photon is coded with an arbitrary polarization state through the QMU consisting of a QWP and HWP. After the QMU, the two orthogonal linear polarizations are separated into two beams by a polarization beam displacer (BD) that are coupled into the two balanced spatial channels CH<sub>H</sub> and CH<sub>V</sub> of the quantum memory. The memory read-outs are recombined at the second BD and the polarization state is measured by the qubit analyser. **b**, The memory operation timing shows the MOT sequence and the optimized control laser intensity time-varying profile in each experimental cycle. **c**, The atomic energy level scheme of the quantum memory based on EIT.

- A related work in **Canada** is dynamically controlling rubidium's transparency to trap single photons<sup>347</sup>.

<sup>343</sup> As in [Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble](#), 2017 (13 pages), a paper to which Frenchman Julien Laurat from CNRS contributed.

<sup>344</sup> As reported in [HKUST Physicist Contributes To New Record Of Quantum Memory Efficiency](#), 2019, which refers to [Efficient quantum memory for single-photon polarization qubits](#) (8 pages).

<sup>345</sup> See [Experimental realization of 105-qubit random access quantum memory](#) by N. Jiang et al, 2019 (6 pages).

<sup>346</sup> See [Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble](#) by Pierre Vernaz-Gris, Julien Laurat et al, Nature Communications, January 2018 (6 pages) and [Efficient reversible entanglement transfer between light and quantum memories](#) by M. Cao, Julien Laurat et al, LKB France, April 2021 (6 pages).

<sup>347</sup> See [Physicists create new, simpler-than-ever quantum 'hard drive for light'](#), by Kate Willis, University of Alberta, 2018, which refers to [Coherent storage and manipulation of broadband photons via dynamically controlled Autler-Townes splitting](#), October 2017 (17 pages).

In practice, photons are stored for a thousandth of a second but this would be sufficient for optical telecommunication repeaters. Another work in France from the Pasqal team used cold atoms to store quantum information<sup>348</sup>.

- **Optical memories** are also tested with ytterbium, a rare earth that can be controlled at high frequency. The process is similar to the previous one and consists in preserving the polarization of a single photon in a magnetic trap, rather for optical repeater applications in long-distance secure communication lines<sup>349</sup>.
- The storage of quantum states is also possible in **electron spins**<sup>350</sup> as well as with **NV centers**<sup>351</sup>.

Many new quantum memory proposals pop up from time to time. An interesting one from the University of Cambridge stores some quantum bit information in an electron spin hidden in haystack of 100,000 atom nuclei. The electron spin and the whole haystack are controlled by a laser. But the nuclei surrounding the electron make it difficult to entangle several qubits. End of story<sup>352</sup>!

## Non-linearities

We often hear about non-linearities with quantum physics, particularly with the difficulty to implement if with qubits. It's also used in neural networks activation functions. Their meaning is not the same in these different scenarios.

Superconducting qubits exploit the Josephson effect and an anharmonic oscillator to prevent the states of the superconducting loop from being separated by the same energy level. This is a non-linear effect. It enables microwaves controls for changing qubits state between  $|0\rangle$  and  $|1\rangle$  with a larger frequency than the one that would allow a switch from the  $|1\rangle$  state to the  $|2\rangle$  state, which is what we are trying to avoid.

Non-linearities are also sought after in photonics, especially to create quality two-photon quantum gates. Non-linearities occur when solid media modify the characteristics of photons such as their polarization and in a non-linear way with respect to the electric field applied to the solid. This phenomenon happens in the Kerr effect which sees some materials refractive index changing in a non-linear (quadratic) manner as a function of the electric field applied to them. Conversely, the Pockels effect used in optical modulators sees the refraction changed in a linear manner as a function of the electric field applied. This non-linearity in optics also occurs in many devices such as power lasers.

Finally, non-linearities are classically used in neural networks activation functions. These are, for example, sigmoids based on exponential fractions.

---

<sup>348</sup> See [Storage and Release of Subradiant Excitations in a Dense Atomic Cloud](#) by Giovanni Ferioli, Antoine Glicenstein, Loic Henriet, Igor Ferrier-Barbut and Antoine Browaeys, PRX, May 2021 (12 pages).

<sup>349</sup> See [Simultaneous coherence enhancement of optical and microwave transitions in solid-state electronic spins](#), December 2017 (10 pages). This is a joint work between the University of Geneva, notably Nicolas Gisin, and the CNRS in France.

<sup>350</sup> See [Researchers achieve on-demand storage in integrated solid-state quantum memory](#) by Liu Jia, Chinese Academy of Sciences, January 2021.

<sup>351</sup> See [Storing quantum information in spins and high-sensitivity ESR](#), by two researchers including Patrice Bertet of the Quantronics group at CEA/CNRS, September 2017 (13 pages). See also [A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute](#) by C. E. Bradley et al, QuTech and TU Delft, 2019 (12 pages).

<sup>352</sup> See [Light used to detect quantum information stored in 100,000 nuclear quantum bits](#) by University of Cambridge, February 2021 and [A different type of cloud computing: Quantum breakthrough uses lasers to find data in a giant cloud of atomic nuclei](#) by Daphne Leprince-Ringuet, February 2021. And [Quantum sensing of a coherent single spin excitation in a nuclear ensemble](#) by D. M. Jackson et al, Nature Physics, 2021 (21 pages).

So how can such activation functions be performed in quantum computation that relies only on linear algebra? One of the first imagined solutions consists in using a non-linear, non-reversible and dissipative quantum gate called D<sup>353</sup>. Others consists in handling the non-linearity part of algorithms in their classical parts before feeding a quantum algorithm. That's what can be done in algorithms solving Navier-Stokes fluid mechanics equations.

## Energetic cost of quantum computing

The main motivation for creating quantum computers is their computing capacity, which theoretically increases exponentially with their number of qubits. This should make it possible to perform calculations that will someday be inaccessible to conventional supercomputers. In some cases, it will only be "just" faster.

How does this computing capacity translates in terms of energy consumption? At first glance, it looked like the energetic cost of quantum computing was several orders of magnitude lower than classical computers. That was a rough interpretation of Google Sycamore's quantum supremacy demonstration published in October 2019. It did show a ratio of about one to one million in energy consumption compared to the IBM Summit supercomputer that was used as a comparison, and even when using the optimized algorithm and configuration proposed afterwards by IBM.

But as we will see in the section dedicated to [superconducting qubits](#), page 252, the benchmark was comparing apples and oranges. It was later shown by Waintal et al that, with accounting for its high error rate and noise, Sycamore's performance could be emulated on a simpler classical server cluster.

Another commonplace view is the sheer power of about 15kW that is required for cooling superconducting qubits processors. It gives the impression that quantum computers will be high-power consuming devices. Well, without remembering that a simple datacenter rack of Nvidia GPGPU is consuming up to about 30kW.

The real comparison should be made... in the future, with large-scale quantum computers. These will probably require a very large number of physical qubits to implement error correction. Controlling these qubits uses conventional energy-consuming electronics. The energy cost-savings of quantum computing will depend primarily on the ability to reduce the associated power consumption. Fortunately, there are solutions to this problem, which we study in the section dedicated to [electronic components](#), page 382, and which we put into perspective here.

### Supercomputers power consumption

The comparison benchmark comes from the world's largest supercomputers, which consume several MW (megawatts). Delivered in 2019 to the Department of Energy's Oak Ridge Research Center in Tennessee, the IBM Summit consumes 13 MW for a peak power of 200 petaflops, including 3.9 MW just for cooling ([source](#)). These MW come from the thousands of Power9s CPU chipsets and general purpose Nvidia V100 GPUs requiring a complex water-cooling system that uses two tons of water per minute.

IBM Summit occupies 500 m<sup>2</sup> and weighs 349 tons, compared to about 2 tons for a superconducting quantum computer that fits into a room of about 20 m<sup>2</sup>, the device fitting in a square cube of about 2.75m, which also gives a "mass advantage" and a "surface advantage" in its current state. However, these quantum computers are not yet competing with supercomputers. Their [quantum advantage](#) is not yet proven for practical use cases.

---

<sup>353</sup> Method proposed by Sanjay Gupta in [Quantum Neural Networks](#), 2001 (30 pages) and [Quantum Algorithms for Deep Convolutional Neural Network](#), by Iordanis Kerenidis et al, 2020 (36 pages).

New supercomputers are launched each and every year, but their scale doesn't change fast. In mid-2020, the record was scored by the Fujitsu Fugaku and its 514 PFLOPS operating within a 30 MW power envelope. In Europe, the largest commercial supercomputer at the beginning of 2019 was the HPC4 of the Italian group ENI, with 18.6 PFLOPS on 1600 HPE Proliant DL380 nodes equipped with 24-core Intel Skylake chipsets and 15 Po of storage, for a consumption of more than 10 MW and a total cost of \$100M<sup>354</sup>. As of June 2021, the largest supercomputers in Europe where the Juwels in Germany with 70 PFLOPS and, then, the HPC5 in Italy with its 52 PFLOPS.

In France, the Joliot-Curie supercomputer designed by Atos was inaugurated in June 2019 at the CEA in Bruyères-le-Châtel for the GENCI (Grand Equipement National de Calcul Intensif). Its power at the launch was 9.4 PFLOPS, later increased to 22 PFLOPS after its planned upgrades in 2020. The initial version consumed just under 1MW. It was equipped with Tesla generation Nvidia GPUs, without tensors. The HPE Jean Zay was launched late 2019 with its 1300 Nvidia V100 GPGPUs with tensors, was water-cooled and had a capacity of 14 PFLOPS. It only consumed 1MW. These evolutions show a continuous growth of HPC computing power, at the expense of a steady increase in energy consumption, even with using state of the art cooling systems.

These benchmarks are important but should not lead us to believe that these supercomputers will eventually be replaced by quantum computers. Many of the scientific applications they are used for are not suitable for quantum computing, like any digital simulation requiring large sets of data such as in weather forecasts or using the finite elements method to solve differential equations as used in computer-aided design tools.

We will always need them. On the other hand, when quantum computers scale up, they will be able to perform computations inaccessible to conventional supercomputers and, probably with a smaller energy footprint although this will require work and help from quantum thermodynamicians.

### Quantum computing energetic footprint

To date, the energy consumption of a quantum computer is relatively reasonable. A current quantum computer with superconducting qubits consumes about 25 kW, of which 16 kW comes from cryogenics. This is the case at D-Wave, Google and IBM. This power consumption is equivalent to about thirty Intel servers or one rack of Nvidia DGX servers in a datacenter.

Quantum computers based on cold atoms or photons consume even less energy, in particular because they do not require cryogenic cooling to 15 mK. They only require photon sources and detectors cooling between 4K and 10K.

When thousands of qubits will fit in these machines, their power consumption will increase due to the heat generated by the electronic activation of quantum gates and error correction<sup>355</sup>. Most of qubits energetic costs come from the signals used for gate activations and readout. These signals are microwaves (superconducting qubits, electron spin qubits), direct current (electron spins) and laser beams (trapped ions, cold atoms, photons). This spent power seems to increase linearly with the number of qubits. But error correction requires a large number of physical qubits per logical qubits, adding another power consumption multiplying factor. It will depend on the fidelity of the physical qubits and the ratio of physical qubits per logical qubits. The higher the fidelity, the lower this ratio will be. On top of that, the cryogenic cost of the qubits grows very fast as the temperature is lower.

---

<sup>354</sup> See [Eni Launches 18.6-Petaflop Supercomputer](#), Michael Feldman, January 2019.

<sup>355</sup> This is the thesis of Joni Ikonen, Juha Salmilehto and Mikko Mottonen in [Energy-Efficient Quantum Computing](#) 2016 (12 pages).

Let's breakdown the power consumption of a typical quantum computer:

**Control electronics:** its power consumption varies greatly from one technology to another and depends on the number of physical qubits managed, which will be counted in millions with large scale quantum computers (LSQC)! It is currently high for the control of superconducting qubits based on microwaves produced outside the cryostat with electronics coming from Zurich Instruments, Qblox, Quantum Machines and the likes. Microwave readouts is costly in bandwidth, requiring Gbits/s of data streams per qubit. Microwave production with cryo-CMOS components sitting in the cryostat looks promising and is studied at Google, Intel, Microsoft, CEA and elsewhere. It can significantly reduce microwave generation related power consumption. Trapped ion-based qubits control is performed with lasers and conventionally generated microwaves.

For cold atoms, qubits control exploits a couple lasers and an SLM matrix that potentially supports a thousand qubits with modest power consumption. With photon qubits, the power drain seems more important for photon detection (about 7.5W per qubit) than for photon generation (about 1mW per qubit, source: Quandela) and depends on their cooling requirements which depends on their technology. Superconducting based photon detectors are more demanding with cooling.

**Cryogenics:** it consumes up to 16 kW for superconducting and silicon qubits and a little less for other types of qubits due to higher temperatures, such as the 4K to 10K of photon generators and detectors used with photon qubits. Cryogenics is not required for cold atoms. They are cooled with laser beams and with ultra-high vacuum. The consumption of cryogenics is usually continuous, without variations between thermalization and production. Thermalization lasts about 24 hours for dilution refrigerator systems used with superconducting and electron spins qubits.

**Vacuum:** superconducting and silicon qubits require vacuum, trapped ions and cold atoms use ultra-high vacuum. Photons do not need it. Vacuum creation depends on the systems. In superconducting and silicon qubits, it results from the use of pumps and cooling. Cold atoms like those from the startup Pasqal require only 100W. Systems based on trapped ions and cold atoms use heating strips covering the vacuum chamber with a process that can take weeks. This is a fixed cost because when vacuum is in place, heating is stopped and vacuum remains stable during computations. Once vacuum is in place, the associated consumption is nullified or at least minimal.

**Computer control:** these are used with all types of qubits. They all require one to three control servers that drive the qubit gates and readout devices by exploiting compiled quantum software, that transforms qubit gates into low-level instructions for qubits initialization, control and readout. These servers are networked, either on premise or in the cloud and via conventional network switches. They represent a limited fixed cost with an estimated consumption of around 1 kW. Part of the control computing could be moved into the cryostat for superconducting and electron spin qubits, in order to implement autonomous error correction codes. The control computer would then only drive logical qubits and not the physical qubits of the configuration. All in all, it would be more energy efficient.

Many of these quantum computer components have a variable energy cost depending on the number of qubits, including the cryogenic side. Indeed, the electronics embedded in cryostats release heat in approximate proportion to the number of physical qubits used. This heat must be evacuated within the cryostat. The consumption of the control electronics also generally depends on the number of qubits. It seems that, up to a thousand qubits, this control electronics is a fixed cost for cold atoms. Only vacuum creation and the control computer seem to be fixed costs.

Another factor to take into account is the inevitable progress that will lead to a reduction in power consumption, particularly in relation with each qubit. This could be the case, for example, with lasers for qubits based on cold atoms, trapped ions and photons. This will also be the case with microwave generation and readout components for superconducting and silicon qubits, which will be progressively integrated into cryostats.

All these writings show that some benchmarking will be needed to assess the energetic cost of quantum computers, from NISQ et LSQC.

atoms		electron superconducting loops & controlled spin				photons	
qubit type	trapped ions	cold atoms	super-conducting	silicium	NV centers	Majorana fermions	photons
cryogeny	2KW	N/A	16 KW	12 KW	< 1 KW	16 KW	3KW
vacuum pumps <sup>1</sup>	vacuum	ultra-vacuum 100W	vacuum	vacuum	vacuum	vacuum	vacuum
qubits gate controls	2KW ions heating, lasers, micro-waves generation, CMOS readout electronics	5,8KW atoms heater, lasers, control (SLM, etc) and readout image sensor + electronics	1 to 5 KW depends on architectures with micro-wave generation outside or inside the cryostat		N/A	N/A	300 W for photons sources and detectors, qubit gates controls
computing	1 KW	1 KW	1 KW	1 KW	<1 KW	1 KW	700 W
# qubits used	10-50	100-1000	65	4	N/A	N/A	20
<b>total</b>	<b>5 KW</b>	<b>7 KW (1)</b>	<b>25 KW (2)</b>	<b>21 KW</b>	<b>N/A</b>	<b>N/A</b>	<b>4 KW (3)</b>

<sup>1</sup> : fixed energetic cost, for preping stage

typical configurations for Pasqal (1), Google (2), Quandela/QuiX (3), rough estimates for others

(cc) Olivier Ezratty, October 2021

## Thermodynamic constraints of quantum computing

Qubits systems that operate at cryogenic temperature are constrained by the cryostat cooling power and by the heat released within the cryostat.

Superconducting and electron spins qubits are the most challenging for that respect. Heat is generated by the inbound cable microwave attenuation filters and in the qubit readout related microwave amplifiers. In addition, the part of microwave generation and readout systems that is integrated in the cryostat have their own thermal footprint.

All this must fit into the current thermal budget of the cryostats that we have seen in the corresponding section, page 361. It is currently limited to 1W at the 4K stage and to 25  $\mu$ W in the 15 mK stage.

We will probably be able to create even more powerful cryostats with more pulse heads and as many dilutions. This will allow to gain an order of magnitude for the available cooling power. Other optimizations can be implemented to increase the available cooling power at very low temperature.

This will certainly generate some constraint for the scalability in number of qubits, particularly for LSQC (large scale quantum computers) which will require millions of physical qubits!

Several options are investigated to reduce the power consumption of the qubits-related classical electronics. An interesting one is superconducting components such as those from SeeQC. D-Wave has integrated its own superconducting microwave controls in its own quantum processor. With cryoCMOS control electronics, the heat dissipation is greater.

The other way to be less constrained is to run the qubits at higher temperatures. This is what is possible with silicon qubits, which only require a temperature between 100mK and 1K instead of 15 mK for superconductors. This increases the thermal budget for the control electronics at the qubit stage.

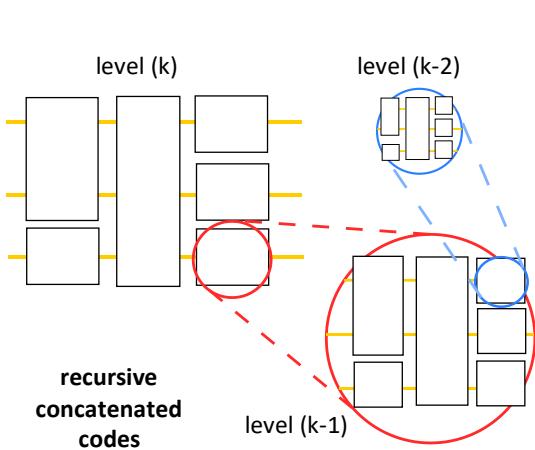
Some significant engineering is required to optimize a multi-parameter system, at least with superconducting and electron spin qubits:

1. Physical scalability requires putting as much as possible **qubits control electronics inside the cryostat**. In the interim, it's about consolidating and miniaturizing external control electronics.
2. These electronics thermal dissipation is **constrained** by the available cryostat cooling power.
3. Two paths must be investigated simultaneously: increase the available **cryostat cooling power** and reduce these **electronics thermal footprint** as low as possible. Superconducting electronics and adiabatic/reversible electronics are two interesting paths on top of more traditional cryo-CMOS components.
4. Find an efficient way to **handle digital communication** between the inside and outside of the cryostat. Fiber optics, wireless, whatever!
5. Look at various ways to **reduce qubits power drain**, with optimizing their own quantum thermodynamics, particularly when implementing error correction codes. It can also come from algorithm and compiler designs.
6. With **scale-out solutions** involving connecting several quantum computing processing units with some photonic link, look at the energetic footprint of this connectivity, on top of its probable impact on qubit links fidelity.

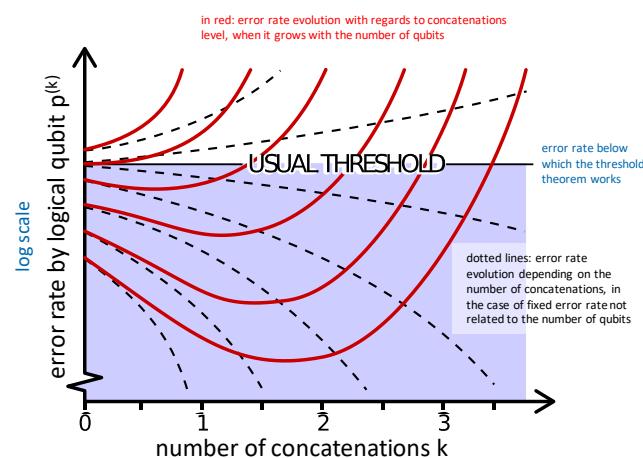
### Error correction energetic cost

Error correction is an important parameter that will condition the power consumption of a quantum computer. The key parameter is the ratio between the number of physical qubits and logical qubits. This can be very high and exceeds 10,000 in some estimates. This ratio depends on physical qubits fidelity.

The higher this one is, the lower the ratio of physical/logical qubits. To perform LSQC (large scale quantum computing), the number of qubits to control will be multiplied and generate high energy consumption. For superconducting qubits, this can result in being limited by the cryostat cooling capacity. As we'll see with Google and IBM, they have plans to scale both the cryostat size (IBM) or scale it out with multiple computing units (Google).



**concatenation quantum error correction codes russia dolls.**  
each functional block of an algorithm of level k can contain a correcting code of an underlying level k-1 and so on. in the end, we have quantum gates.



**evolution of the logical qubits error rate with the number of concatenations\***, with a stable error rate (black) and a more realistic error rate growing with the number of qubits (in red). It shows in that later case that concatenations quickly reach limits after one or two stages of correcting codes.

However, error correction codes used recursively by concatenation may simultaneously run up against another wall: the scale dependence of qubit noise. Namely, qubit gates and readout fidelities usually decrease with the number of qubits.

This has the consequence of reversing the effect of concatenation of error correction codes starting at only two or three concatenations. The error rate of logical qubits gates then increases, instead of decreasing<sup>356</sup>.

For error correction codes to be effective, the error rate of qubits should be at least ten times lower than their current level. In addition, we must also consider the fact that quantum algorithms are executed thousands of times and their result is then averaged, as IBM does with its Q System quantum computers in the cloud. This increases the power drain of a quantum computation because it extends its duration by three orders of magnitude, at least, for the time being.

## Reversibility of classical and quantum calculations

Here we will study the impact of reversibility on the energy consumption of quantum computing. We first need to define the notion of logical reversibility of computation and its thermodynamic impact.

**Logical reversibility** of a calculation is linked to the ability to reverse it after one or more operations and recover input data from output data. This can be done at the scale of a classical logic gate or an elementary quantum gate and then up to a complete calculation. If logical reversibility is possible at the level of any gate used, then it becomes ipso-facto doable for a complete calculation<sup>357</sup>. Today's classical computers are logically irreversible.

They rely on two-bit logic gates that destroy information since they generate one bit with two bits. One bit is thrown away every time. You can't reverse a simple NAND, OR or AND logic operation. We could use reversible logic gates that do not destroy information and generate as many output bits as input bits. This would lead to a logically reversible calculation. All of this was theorized by Charles Bennett in 1973 and Tommaso Toffoli in 1980. Classical computing is a big energy spender because logic gates are not logically reversible. The lower bound of energy consumption of current classical computing comes from Landauer's famous limit of  $kT \ln(2)$  energy dissipated per irreversible bit operation, which can be the erasure of a bit or the merging of two computation paths. This bound can be avoided with logical reversible computing. The implementation of this logical reversibility by rewinding calculations would reduce the energetic cost of classical computing, the energy spent in the forward calculation being potentially recovered in the reverse calculation.

**Thermodynamic reversibility** is another matter and can be obtained when the system is continuously balanced with its thermal bath. It requires handling operations in a quasi-static way, namely, slowly and with logical gates requiring a minimum energy spending. This is the field of adiabatic computing. We will study it separately, with logical reversible computing, in a part dedicated to [adiabatic and reversible computing](#), page 427.

Gate-based quantum computing is logically reversible because it uses unitary operations which are all mathematically reversible. Qubits readout is the only logically irreversible operation when it collapses qubit states to a basis state<sup>358</sup>. Qubits readout would be reversible only if the results were perfectly aligned with the basis qubit states  $|0\rangle$  and  $|1\rangle$ .

---

<sup>356</sup> This is what comes out of [Limitations in quantum computing from resource constraints](#) by Marco Fellous-Asiani, Jing Hao Chai, Robert S. Whitney, Alexia Auffèves and Hui Khoon Ng, July 2020 (8 pages).

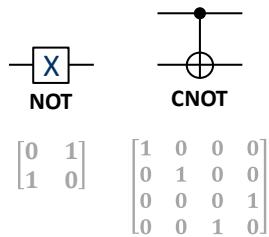
<sup>357</sup> See these detailed explanations on the reversibility of classical calculus: [Synthesis of Reversible Logic Circuits](#) by Vivek Shende et al, 2002 (30 pages).

<sup>358</sup> Measurement Based Quantum Computing, which relies mainly on measurement during the entire calculation, is irreversible by construction. This is why it is also called 1WQC for one way quantum computing.

However, quantum computing is not really physically or thermodynamically reversible. It would be reversible in the absence of noise and if measurements were not changing qubit's values. Achieving physical irreversibility would also mandate that all non-quantum qubit control electronics rely on physically and thermodynamically reversible processes or at least be energy-saving operations.

One way to achieve this would be to use adiabatic and reversible electronic components working from within the cryostat, one option being superconducting electronics like RSFQs used in D-Wave processors or with SeeQC and investigated at research labs like VTT in Finland.

**all quantum gates are mathematically reversible,**  
this is a property of the matrix linear transformations



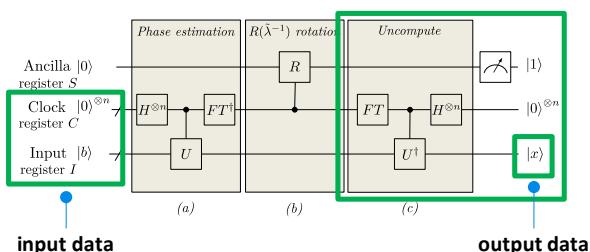
**we could theoretically run an algorithm and rewind it entirely to return to the initial state, which could help recover part of the energy spent in the system**

**can be useful for some sub-parts of algorithms run before the end of computing and measurement, used in the “uncompute trick” at the end of some algorithms like for solving linear equations with HHL. it keeps the result  $x$  with resetting all other qubits without any measurement.**

**on a practical basis:**

- **the gates are not physically and thermodynamically reversible** due to some irreversible processes like microwave generations and DACs (digital analog converters).
- **the whole digital processes taking place before micro-waves generation and after their readout conversion back to digital** could be implemented in classical adiabatic / thermodynamically reversible fashion.
- **being investigated** at Sandia Labs, Wisconsin University and with SeeQC, with their RSFQ superconducting based logic, microwaves DACs and ADCs.

(cc) Olivier Ezratty, 2021



Another explored avenue is ABQC for **Asynchronous Ballistic Quantum Computing**, promoted by Michael P. Frank's team at the DoE Sandia Labs in the USA. They plan to implement it with Josephson junctions circuits<sup>359</sup>.

Quantum reversible computing can also use quantum memory and the uncompute trick of results that are no longer necessary, such as those sitting in ancilla qubits<sup>360</sup>.

However, quantum reversibility is not the key to reducing the energy consumption of quantum computing. It is one of the available means among others and with a rather moderate impact.

The quest for energy savings mainly deals with the classical part of qubits control. Reducing the energy consumption of quantum computing can integrate various techniques that are not related to reversibility, mainly CryoCMOS electronic components and microwave amplifiers operating at low temperature (typically 1K to 4K) and superconducting components that reduce electronics energy consumption. All this while getting rid of some of the cumbersome wiring and filters currently in use. But these components must be cooled at low temperature. There's a complicated trade-off between the global electronics power consumption and the power cost of cooling it.

Understanding and tuning the energetic cost of quantum computing is thus a multi-dimensional discipline.

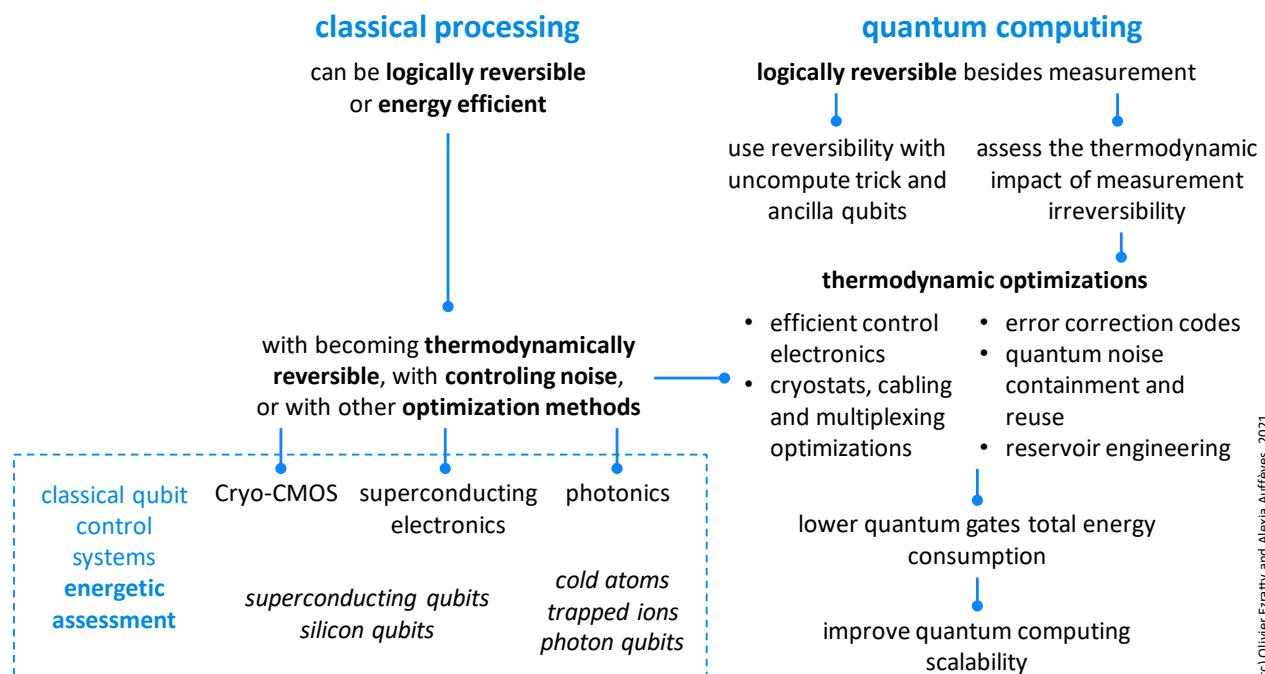
<sup>359</sup> See [Pathfinding Thermodynamically Reversible Quantum Computation](#) by Karpur Shukla and Michael P. Frank, January 2020 (28 slides) and [Asynchronous Ballistic Reversible Computing using Superconducting Elements](#) by Michael P. Frank et al, April 2020 (27 slides).

<sup>360</sup> See [Putting Qubits to Work - Quantum Memory Management](#) by Yongshan Ding and Fred Chong, July 2020.

It combines classical and quantum elements whose relative impact in terms of energy savings and scalability must be assessed comparatively with the different types of qubits available. This is what makes it an engineering discipline.

All this combines many elements of fundamental thermodynamics, classical electronic engineering and quantum physics.

This is a field that is being explored by Michael Frank's team from Sandia Labs, already mentioned, as well as by Alexia Auffèves' team from the CNRS Institut Néel in Grenoble. In November 2021, she launched a call for creating a quantum energy initiative to address these various questions<sup>361</sup>.



The *above* diagram positions all these concepts in relation to each other, with a close link between the energy aspects of classical computing and those of quantum computing. Energy efficiency comes from various sources and far exceeds the ones coming from qubits operations reversibility.

### Energy impact of distributed architectures

The temptation is great to create ever larger quantum computers, with giant cryostats in the case of superconducting qubits, like we'll see with IBM and Google's roadmaps. Another approach would be to create distributed architectures of quantum computers linked together by quantum connection based on entangled photons, a choice made by IonQ with their trapped ions qubits, noticeably because it is difficult to scale these qubits beyond a couple dozens.

In theory, this would make it possible to create computing clusters that, seen from the outside, would create a single computer, a bit like a large classical server cluster. This will be conditioned by the capability of converting qubits states to photons qubits states and by the resulting qubit connectivity between the various quantum processors units of this quantum cluster.

<sup>361</sup> See [Quantum technologies need a quantum energy initiative](#) by Alexia Auffèves, November 2021 (10 pages).

We should also take into account the energetic cost of the quantum telecommunications involved to connect these processing units. This should be relatively reasonable in relation to the consumption of the cluster nodes.

## Use cases energy impact

Another longer-term question deserves to be asked: does the potential energetic advantage of quantum computing depend on algorithms and applications? What will happen if and when quantum computing becomes widespread? Are we finally going to create a new source of energy consumption that will be added to existing sources, which are already growing fast in the digital world? What will be its impact? How can it be limited?

At this stage, it is too early to have a clear idea. Answers will largely come from the emergence or not of quantum solutions for volume applications, such as autonomous vehicle routing or personalized health solutions.

Without volume-oriented applications, quantum computers will be dedicated to niche applications equivalent to those of current supercomputers, which are mainly used in fundamental and applied research or for public services like weather forecasts.

On their end, volume applications will only be achievable once the quantum computing scalability will work and millions of low-noise qubits can be operated. This scalability will probably come from fixing some of energetic consumption issues of quantum computing. And we'll close the loop!

## Economics

Given we are at the very early stage of the quantum computing era, it's still difficult to assess the economics of this industry. It's too small to generate economies of scale giving some indications on the cost and price of a regular quantum computer. Still, we can make some projections based on a couple assumptions.

The only "priced" quantum computers on the market today are coming from D-Wave. Their units are priced at about \$14M. They have sold only a few of these. Most D-Wave customers are using D-Wave computers sitting on the cloud either with D-Wave itself or with Amazon. Some customers pay in excess of \$200K per year to benefit from a premium access to these machines. As far as we know, the other "volume" manufacturer of quantum computers is IBM but they haven't sold any unit so far, at least publicly. They installed two in Germany and Japan in their own facilities, to serve these markets through local research and university partners. The rest is provided through their own cloud services.

One can economically make a distinction between **cost** (of R&D, goods and manufacturing), **price** (how much is it sold or rented) and **value** (what value is it bringing to customers, particularly, compared with existing classical computing solutions). Right now, the equation is simple: costs are high, prices are high as well when computers are sold (particularly superconducting qubits ones) and value is low at this point, and is positioned in the educational and proof-of-concept realms.

A quantum computer cost and price depends on several parameters including its underlying R&D, bill of materials of off-the-shelf and custom-designed components, manufacturing and integration costs, economies of scale, marketing and sales costs, the cost of maintenance and consumables if any, and finally, the manufacturer's profit. The higher the sales volume, the greater the economies of scale. Volumes are currently very low given most quantum computers are just prototypes that are not yet useful for production-grade applications.

At some point, when and if we reach some quantum advantage threshold, useful applications will emerge. It will first target niche b2b and government markets. Then, when applications and innovation ramp-up, we may have a larger number of corporate users. It will justify scaling manufacturing capacities. R&D fixed costs will then be easier to amortize with volume. Cost of goods may also decrease, particularly if technology progress can help get rid of the complicated wirings and electronics that we have today in some of these devices.

Let's look one by one at the major hardware components of a quantum computer looking at how it will benefit from economies of scale:

- **Control computer(s)**: these are standard rack-mounted servers as well as the associated networking connection. These are the most generic parts of a quantum computer.
- **Chipset**: quantum registers chipsets are the cornerstone of electron-based quantum computers, such as with superconducting and electron spin qubits. Even if they are manufactured in CMOS or similar technologies, their manufacturing volume is very low. Economies of scale are therefore almost non-existent. You don't need such components with cold atoms and trapped ions qubits. It is replaced by specialized optical components to direct the laser beams controlling the qubit atoms. With NV centers, chipsets can be cheap to manufacture if done in volume.
- **Electronic components**: these are used to create, process, transmit and send the quantum gate signals to the qubits. Their technology depends on the type of qubit. These signals are micro-waves for superconducting and electron spins qubits, laser-based photons for cold atoms and trapped ions, and some other varieties of electro-magnetic signals otherwise. Standard and expensive laboratory equipment are used for microwave generations such as those from Rohde&Schwarz. More integrated equipment are sold by companies like Zurich Instruments and Qblox. It's using customized FPGA and rather standard electronic components. When these tools are miniaturized as cryo-CMOS, their small economies of scale make it rather expensive.
- **Cabling**: niobium-titanium superconducting cabling used to feed superconducting and electron spin qubits with microwaves are very expensive, costing about \$3K each. And we need about three such cables for each and every qubit. Companies providing these cables are Coax&Co, Radiall and Delft Circuits. This creates high-costs for manufacturing superconducting and electron-spin based qubits systems.
- **Cryogenics**: these are standard systems but marketed in low volumes. They can cost up to \$1M for superconducting and silicon qubits. Their cost is one to two orders of magnitude lower for the cryogenics of components such as photon qubits. Large cryostats use an enclosed cooled system with many cylindrical layers of protection, a GHS (gas handling system), a compressor (such as those coming from CryoMech and Sumitomo) and another compressor used to cool the water feeding the primary compressor.
- **Consumables**: in quantum computers operating at very low temperatures, there is at least some liquid nitrogen and gaseous helium 3 and 4. The latter two are not consumables and operate in a closed circuit in dry dilution systems. It's still expensive.
- **Casing**: this is just steel, glass and design.

As quantum technologies mature, some cost structures will increase and others will decrease. Economies of scale will do the rest. We can therefore forecast that the \$15M D-Wave computer price tag will remain for some time in the top range of quantum computers prices, at least at superconducting qubits. Some computers will be less expensive than \$1M. In practice, many quantum computers will be usable as resources in the cloud and at a more moderate cost. This is what IBM, Rigetti, D-Wave, Microsoft and Amazon (with third-party machines for the latter two) are already offering. Microsoft and Amazon quantum cloud pricing is already quite high. Then, one can wonder about its added value.

# Quantum uncertainty

Estimating if and when scalable and useful quantum computers will be available is a difficult art and science. The spread between optimists and pessimists is quite large. Some entrepreneurs expect to achieve miracles in less than one decade while some scientists, on the other hand, think that this will never happen. In between, other scientists are moderately optimists and expect the wait to last at least a couple decades. Let's look at these various opinions.

## Optimism

Google said it achieved quantum supremacy back in October 2019. It was not a true supremacy since their Sycamore setting was doing no programmable computing solving a specific problem. It was found later that, due to the qubit noise in their system, it was relatively easy to emulate it on a classical server cluster (discussed [here](#) in this ebook). So much for any quantum supremacy or advantage! It was the same with the so-called boson sampling experiments quantum advantages coming from China in 2019 and 2020. These were not much more than unprogrammable random photon mixers!

As published in their 2020 roadmaps, Google, IBM and Amazon expect to achieve true quantum supremacy relatively quickly and create a quantum computer with 100 logical qubits in less than a decade.

**Kenneth Regan** thought in 2017 that an industry vendor - probably Google - would claim to have reached quantum supremacy in 2018 and that it would quickly be contradicted by the scientific community<sup>362</sup>. This happened in 2019. That was quite a good prediction!

For the specialists who can dissect their scientific publications, the view is obviously more nuanced, especially concerning the reliability of the qubits they generate. They communicate a lot about their efforts to reduce the noise of qubits to make them more reliable<sup>363</sup>.

**Alain Aspect** does not see any strong scientific obstacle preventing the creation of reliable quantum computers. He believes that the uncertainty is mostly a technological and engineering one, but that it will take a few decades to create one reliable advantage-grade quantum computer.

However, there is nothing to prevent this process from being accelerated, if it is fueled by good talent and public/private investments. **John Preskill** has the same opinion: it'll work, but it will take several decades.

Optimists also include the many hardware quantum computing startups, all with solutions that are expected to work on a large scale within the next five years. They are found in all types of qubits: superconductors (IQM, QCI), electron spins (Quantum Motion, SQC), cold atoms (Pasqal, Atom Computing, ColdQuanta), trapped ions (IonQ, Honeywell, Universal Quantum) and photons (Psi-Quantum which predicts one million qubits in less than five to ten years, Orca Computing, Quandela).

## Pessimism

Pessimism comes from a few researchers, who are not necessarily specialized in the field in which they express themselves. Above all, they are pessimistic about the ability to fix the noise that affects qubits, whatever their type.

The first and best-known of these pessimists is the Israeli researcher **Gil Kalai** who believes that we will never be able to create quantum computers with a low error rate<sup>364</sup>.

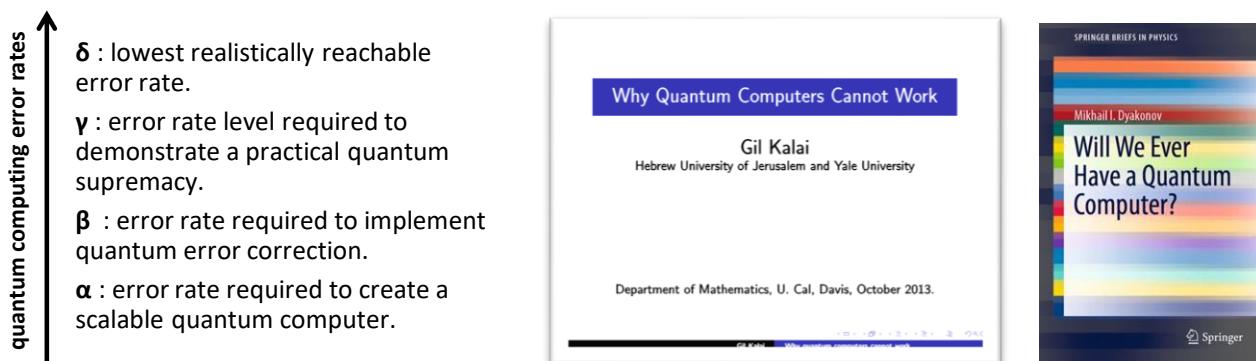
---

<sup>362</sup> In [Predictions we didn't make](#), January 2018.

<sup>363</sup> Voir [The Era of quantum computing is here. Outlook: cloudy](#) by Philipp Ball, in Science, April 2018.

According to him, we cannot create stable quantum computers because of the noise that affects the qubits. This is illustrated in the scale *below*, which sets the lowest reasonably achievable noise level well above the level required to create a scalable quantum computer.

He is working on the creation of some mathematical model that would prove the impossibility of overriding these errors, even with quantum error correction codes.



Another skeptic of quantum computing is the **Mikhail Dyakonov** (born in 1940 in the USSR) who works in the Charles Coulomb Laboratory (L2C) of the CNRS and the University of Montpellier in France. He expressed his views in an article at the end of 2018, which he later turned into a book<sup>365</sup>. His argument is more intuitive but less documented than the work of Gil Kalai<sup>366</sup>.

We also have **Serge Haroche** for whom universal quantum computing is an unreachable dream, also because of that damned noise. On the other hand, he thinks that the path of quantum simulation, especially based on cold atoms, is reasonable and realistic.

**Xavier Waintal** (CEA-IRIG in Grenoble, France) also has serious reservations about the possibility of creating large-scale quantum computers. Here again, the culprit is noise. His reasoning is based on physical explanations different from those of Gil Kalai: Qubits operations are relying on very complex n-body quantum problems and error correction codes generally deal with only two types of errors (flip, phase) but not with all sources of error. He recommends to exploit mean-fields theory which allows to model the complex interactions between qubits and their environment<sup>367</sup>. These are very fundamental questions to address.

**Cristian Calude** and **Alastair Abbot** point out that the advantage of the main quantum algorithms usable in practice would generate a modest quadratic acceleration (square root of classical computing time) that could be achieved on classical computers with heuristic approaches<sup>368</sup>.

Quantum skepticism is also evident in **Ed Sperling's** November 2017 review of the field, which included a reminder of all the obstacles to be overcome<sup>369</sup>.

<sup>364</sup> See [Why Quantum Computers Cannot Work](#), 2013 (60 slides) illustrating [How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation](#), 2011 (16 pages) and [The Argument Against Quantum Computers](#) by Katia Moskwitch, February 2017. Gil Kalai declares: "My expectation is that the ultimate triumph of quantum information theory will be in explaining why quantum computers cannot be built".

<sup>365</sup> See [The Case Against Quantum Computing](#), 2018. He even made a book about it, [Will We Ever Have a Quantum Computer?](#), 2020. As well as a debate on the subject launched by Scott Aaronson in [Happy New Year! My response to M. I.Dyakonov](#). See also [Skepticism of Computing](#) by Scott Aaronson who dissects 11 objections on quantum computing capabilities. See also [Noise stability, noise sensitivity and the quantum computer puzzle](#) by Gil Kalai, 2018 (1h04mn).

<sup>366</sup> See a response to this argument in [The Case Against 'The Case Against Quantum Computing'](#) by Ben Crige, January 2019.

<sup>367</sup> See [What determines the ultimate precision of a quantum computer?](#) by Xavier Waintal, 2017 (6 pages) that we have already mentioned. Xavier Waintal has notably developed classical algorithms for the simulation of N-body problems. They are used by various teams of researchers in condensed matter physics, notably those working on topological matter and Majorana fermions. They run on laptops and supercomputers.

<sup>368</sup> In [The development of a scientific field](#) by Alastair Abbott and Cristian Calude, June 2016.

Another argument against scalable quantum computing deals with the computational state vector amplitudes values becoming tiny as the number of qubits grows. After just applying a set of H gates on N qubits, this amplitude becomes  $1/2^N$  for each computational basis state in the qubits register. It becomes quite small as N grows beyond 50. Are these values corresponding to some physical observable that would have a value way below the physical error rate in the system? Or even below some physical Planck constant? Well, this is good food for thought. At least, the computational state vector always has a norm of 1. And the physical observables in the system remain the individual qubits basis states  $|0\rangle$  and  $|1\rangle$ .

## Managing uncertainty

One key challenge is to make a distinction between scientific unfeasibility, scientific uncertainty and technological uncertainty. This set of uncertainties raises existential questions about how to manage such a long innovation cycle. When should we invest? When are market positions being settled? Is fundamental research decoupled from industrialization? Is quantum computing a simple engineering matter?

Note that the pessimists quoted above are not Americans and most of the optimists are. Is there a cultural bias here? These variations in innovation and economic cultures have an impact on industry approaches. Major IT companies such as IBM, Google, Intel, Amazon and Microsoft can fund quantum computing R&D investments with a very long-term vision. They have the profitability, the cash and the ability to attract skills to do so.

More or less well-funded startups in Canada and the USA such as D-Wave, Rigetti, IonQ or Psi-Quantum can also adopt a fairly long-term view, even if it still depends on their ability to commercialize quantum computer prototypes and to attract long-term oriented investors. The corresponding amounts are not necessarily crazy. Rigetti has so far raised \$190M, which is pocket money compared to many of the world's "no deep techs" Internet unicorns.

The engineering problems to be solved deal with qubits materials and manufacturing techniques, quantum error correction, control electronics, large-scale cryogenics and of course algorithmic and software advances. The required approach is multidisciplinary with mathematics, fundamental quantum physics, thermodynamics and chemistry, and finally, code, including machine learning which is notably used for qubits calibration.

We can also extrapolate the evolutions of the last ten years in quantum computing. When he was the co-founder of D-Wave, Geordie Rose enacted in 2003 his own equivalent of Moore's empirical law, [Rose's Law](#), predicting a doubling every year of the number of qubits in a quantum computer. So far and since 2007, D-Wave has delivered on this promise. But this progress has been sluggish for gate-based quantum computers. And these charts have not been updated for a few years. Some charts even included numbers corresponding to non operational systems like Google's 2018 72-qubit Bristlecone or the 129 qubits from IonQ and Rigetti which never saw the day of light. Between 2018 and 2021, we have not seen a real increase in the number of operational qubits.

This exponential law is observed in the evolution of other operating parameters of quantum computers such as the stability time of qubits, their error rate and the number of consecutive operations performed reliably<sup>369</sup>.

*"For me, the most important application of a quantum computer is disproving the people who said it's impossible. The rest is just icing on the cake."*

Scott Aaronson  
2019.

<sup>369</sup> In [Quantum Madness](#) by Ed Sterling, November 2017.

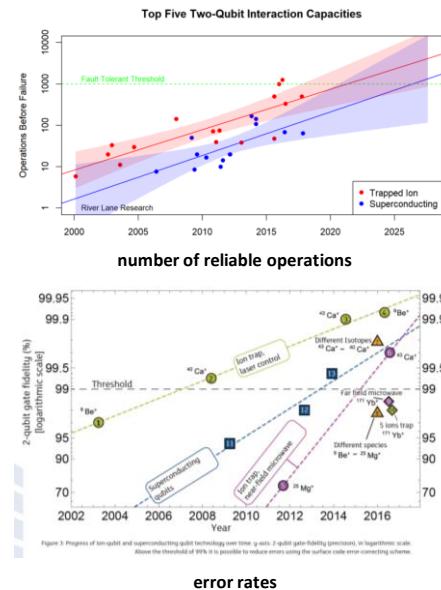
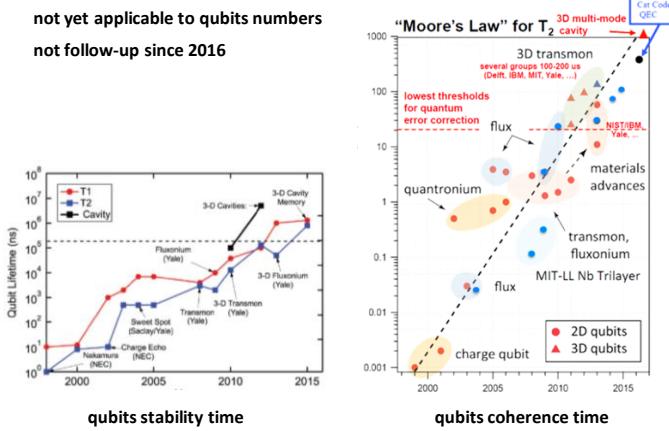
<sup>370</sup> Some of the diagrams below come from the [Technical Roadmap for Fault-Tolerant Quantum Computing](#), a UK report published in October 2016 and from [this other source](#).

Recently, **Rob Schoelkopf** from Yale enacted its own law showcasing the progress with superconducting qubits coherence times and gates fidelities and times (below, [source](#)).

I tried to understand why the predictions of creating viable quantum computers were always quite long-term, between 5 and 50 years. One of the answers comes from the length of cycles in the associated research and manufacturing processes.

## Rose law (2003)

*"quantum Moore's law"*



## Challenges ahead

Whether you are an optimist or a pessimist with regards to the advent of scalable quantum computers, you need to adopt an educated view of the challenges ahead. Over time, as my understanding of these challenges was growing, I tended to shift from “optimism” to “neutralism”. Some of the challenges ahead are enormous. The below chart lays out some of these challenges, most of which being covered extensively in various parts of this document.

Two things come to mind: one is that quantum computers scalability is the most challenging issue to tackle with. If quantum computing capacity is known to theoretically scale exponentially with the number of qubits, it looks like the scale challenge is also an exponential one. One way to grasp it is to look at IBM and Google’s progress with their superconducting qubits. It’s been sluggish since 2019 with 53/65 qubits, given that most benchmarks show that only fewer than 20 qubits are practically usable<sup>371</sup>. There’s still some hope with bosonic codes and cat-qubits, the path chosen by Amazon, Alice&Bob, QCI and Nord Quantique. Also, scale-out options devised with trapped-ions are interesting. Other qubit types like electron spins and photons also look promising.

The second challenge deals with real algorithms speedups. Not all algorithms showcase an exponential theoretical speedup. For example, Grover’s algorithm speedup is only polynomial. All non-exponential speedups seem useless due to their implementation cost. The trick of the trade is that all speedups are theoretical but not yet practical. Another way to look at this is to envision, even with moderate algorithms speedups, an energetic advantage for quantum computing, as discussed in the related part that we just saw, starting on page 223.

These speedups are never documented with taking into account all the quantum computing food chain: data preparation, oracle operations, quantum memory access when it is required, quantum error correction, non-Clifford group quantum gates generation (particularly for all algorithms using a quantum Fourier transform, and there are many) and the number of shots/runs required (with or without quantum error corrections). I wish somebody did produce such evaluations with actual and projected data on these different aspects of gate-based quantum computing, even if it brings bad news! When bad news travel fast, fixes arrive faster, if there are any!

One broader challenge for the industry is to spur developer creativity for the design of even more algorithms and ways to assemble many quantum algorithms to create innovative solutions.

In the end, it looks like quantum simulators may be one very viable short-term option but we also still lack data to prove it.

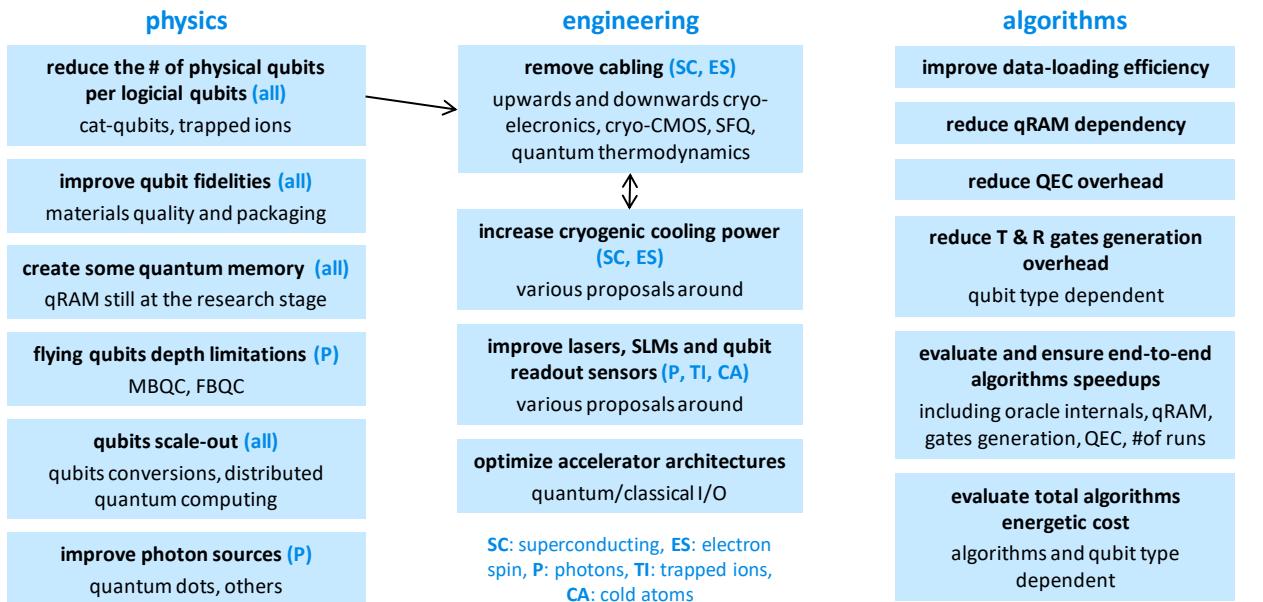
Some algorithms are being evaluated to run on these quantum simulators, like the ones from Pasqal and ColdQuanta but they have only been tested so far on classical computers emulators. The quantum software ecosystem will have to look at this!

D-Wave and other coherent Ising machines like the ones being designed by NEC and Qilimanjaro could also bring their share of hope. The debate is still out to assess what is the quantum advantage of D-Wave with its latest annealer generation, relying on their 5000 qubits Pegasus chipset. The lack of qubits connectivity seems a showstopper to really get some quantum advantage.

I still count on two things to reach quantum computing scalability and practicality. One is the great diversity of paths chosen by scientists and entrepreneurs. This creates a sort of fault-tolerance for innovation. The second, more generally, is I still believe and bet on scientists and engineers creativity to solve these highly complicated problems. Think the impossible and it will become possible!

---

<sup>371</sup> See one example here from Google with experiments on Sycamore stopping at 20 qubits: [Efficient and Noise Resilient Measurements for Quantum Chemistry on Near-Term Quantum Computers](#) by William J. Huggins et al, Google AI, June 2020 (17 pages).



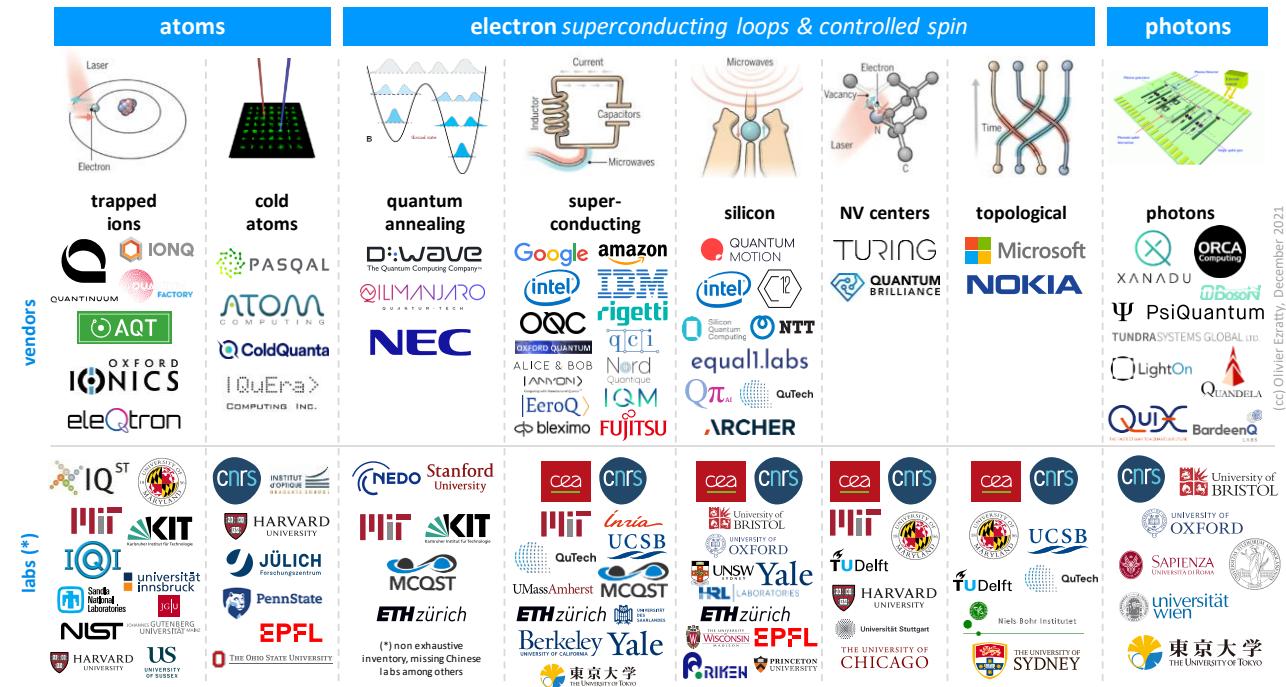
(cc) Olivier Ezratty, 2021

## Quantum computing engineering key takeaways

- A quantum computer is based on physical qubits of different nature, the main ones being superconducting qubits, electron spin qubits, NV centers, cold atoms, trapped ions and photons. They all have pros and cons and no one is perfect at this stage. Future systems may combine several of these technologies.
- Many key parameters are required to create a functional quantum computer. It must rely on two-states quantum objects (qubits). These must be initializable and manipulable with a set of universal gates enabling the implementation of any linear transformation of qubit states. Qubits must be measurable at the end of algorithms. Their coherence time must allow the execution of a sufficient number of quantum gates. Decoherence and errors must be as low as possible.
- Most quantum computers are composed of several parts: the qubit circuit (solid-state), enclosures (cold atoms, trapped ions) or guides (photons), usually housed in a cryogenic vacuum chamber (with the exception of photons and NV centers), some electronics sending laser rays or coaxial cables guided microwaves onto qubits and a classical computer driving these electronic components.
- Since qubits are noisy, scientists have devised quantum error correcting schemes. These rely on creating logical “corrected” qubits composed of a lot of physical qubits, up to 10,000. This creates huge scalability challenges.
- Many quantum algorithms also require some form of quantum memory, either for data preparation and loading (such as with quantum machine learning) or to access efficiently classical data (such as with oracle based algorithms like a Grover search). These quantum memories don’t exist yet.
- The energetic cost of quantum computing is both a potential benefit but also an immense challenge, particularly when a large number of physical qubits are required to create large scale fault-tolerant computers. All components must be carefully designed to take into account the cryogenic cooling power as well as the available space to house cabling and cryo-electronics.
- The economics of quantum computers are still uncertain due to their immaturity and the current low manufacturing volume. Uncertainty is also strong with regards to the feasibility of scalable quantum computers. The scalability challenges ahead are enormous. One of them is to benefit from an actual algorithm speedups when including all end-to-end computing operations.

# Quantum computing hardware

In a more or less bottom-up approach, we've covered successively the basics of quantum physics, the mathematical aspects of gate-based quantum computing, then quantum computing engineering and enabling technologies. Let's now move to the last stack, quantum computers, with focusing on their specifics depending on the types of physical qubits they are using. We are dealing here with all sorts of players: public research laboratories, large established companies as well as startups<sup>372</sup>.



(cc) Olivier Ezratty, December 2021

There are more and more startups in this picture. They do not shy away from Google and IBM. There are no Chinese startups yet. For the moment, the country's investments in quantum computing are concentrated in well-funded public research like with Jian Wei-Pan's giant lab in Hefei and with large cloud companies like Baidu and Alibaba. Chinese labs are missing in the chart above.

As we saw in the [section dedicated to the types of qubits](#), page 187, there are eight main categories of quantum computers grouped into three categories :

## Atoms:

- **Trapped ions** found in particular at IonQ, a spin-off from the University of Maryland, as well as at Honeywell and the Austrian startup Alpine Quantum Technologies.
- **Cold atoms** like rubidium are used to create both analog quantum computers and quantum gate computers.

## Electrons:

- **NV centers** with only a few industrial players like Quantum Brilliance. Most NV centers applications are in quantum sensing.

<sup>372</sup> Qubits drawing source: [Scientists are close to building a quantum computer that can beat a conventional one](#) by Gabriel Popkin in Science Mag, December 2016. I consolidated the logos lists since 2018. It's incomplete for the research labs at the bottom but rather exhaustive for the vendors at the top.

- **Superconducting** Josephson effect qubits used in IBM's, Google and Rigetti and in D-Wave's quantum annealing computers. This is a broad category with Josephson qubits (transmon, fluxonium, coaxmon, ...) and photon cavities-based qubits using superconducting resonators (cat-qubits, GKP) where the Josephson junctions are used to prepare qubit states, handle qubits coupling and manage error corrections, but not contain the qubit state itself (with Alice&Bob, Amazon, Nord Quantique and QCI).
- **Electron spins qubits** pushed notably by Intel, Quantum Motion, SQC, C12, Archer and CEA-Leti. There are many variations there.
- **Topological qubits** with, in particular, the hypothetical fermions of Majorana from Microsoft whose existence is yet to be proven. But other topological qubits avenues are investigated in research laboratories at the fundamental research level.

### Flying qubits:

- **Photon qubits**, which is currently not very scalable but potentially promising, particularly when coupled with a [MBQC](#) architecture that circumvents the difficulty to handle two qubits gates and the limited computing depth of flying qubits.
- **Flying electrons**, a separate track of qubits, with no commercial vendor yet involved in it. It's a fundamental research field.

Many of the commercial companies in this panorama are associated with American or European research laboratories. Google collaborates with the University of Santa Barbara in California, IBM and Microsoft with the University of Delft in the Netherlands, and IBM with the University of Zurich, among other publicly funded research organizations.

These categories of technologies have very different levels of maturity. Superconducting qubits are the most proven to date. Trapped ions are best-in-class with regards to fidelity and connectivity but do not scale well. Linear optics and NV centers have also some difficulties to scale. Electron spin-based systems could scale but are less mature. Finally, Majorana fermions are still in limbo. But other qubits types are looming around and may become promising (other topological materials, Silicon Carbide, etc.).

	atoms	electrons superconducting & spins			photons		
	 <b>cold atoms</b>	 <b>trapped ions</b>	 <b>superconducting</b>	 <b>silicon</b>	 <b>NV centers</b>		
qubit size	about 1 μm space between atoms	about 1 μm space between atoms	(100μ) <sup>2</sup>	(100nm) <sup>2</sup>	<(100nm) <sup>2</sup>		
two gates fidelities	98%	99,9%	99,4%	>98%	99,2%	N/A	98%
readout fidelity	99%	99,9%	99,4%	98%	98%	N/A	50%
gate time	1 μs	100 μs	20 ns - 300 ns	~5 μs	10-700 ns	N/A	1 ms
coherence		0,2s-10mn	100-400μs	20-120μs	2.4 ms	N/A	
qubits temperature	< 5mK	<1mK to 10K	15mK	100mK-1K	4K-ambiant	15mK	ambiant & 4K/10K photons generators & detectors
operational qubits	100-196 (simulator)	32 (IonQ)	65 (IBM) 56-66 (China)	4 (Delft)	5 (Quantum Brilliance)-10	N/A	70 (China)
scalability	1000	<50	100s	millions	100s	?	100s-1M

The *above* table is a sketchy and probably highly questionable comparison between these different qubits, particularly with cold atoms which are so far, used in quantum simulation mode and not gate-based architectures<sup>373</sup>.

## Quantum annealing

Quantum annealing is a particular quantum computer technology that is based on quantum mechanics and qubits, but with characteristics and performance levels intermediate between traditional supercomputers and general-purpose gate-based quantum computers. **D-Wave** is the main commercial player in this category. Some research laboratories are also involved in quantum annealing but not as many as those involved in the different types of quantum gate model computers.

They are located mainly in Japan, where the technique was invented in 1998 by **Hidetoshi Nishimori**<sup>374</sup>. But there are a few in the USA, including at **UCSB**<sup>375</sup>, and some in Europe, particularly in Spain, which led to the creation of **Qilimanjaro**.

The interest in Shor's factoring algorithm created much interest in gates-based quantum computing, at the expense of quantum annealing. It also created a chasm in the qubit types, transmon superconducting qubits being adapted to gates-based computing while flux superconducting qubits were the path for quantum annealing.

### quantum annealers

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>• mature <b>development tools</b> offering.</li><li>• large number of <b>software startups</b>, particularly in Japan and Canada.</li><li>• quantum annealers are available in the <b>cloud</b> by D-Wave and Amazon Web Services.</li><li>• the greatest number of well documented <b>case studies</b> in many industries although still at the proof of concept stage.</li><li>• most universal qubits gates algorithms can be have an equivalent on quantum annealing.</li></ul> | <ul style="list-style-type: none"><li>• only <b>one operational commercial vendor</b>, D-Wave.</li><li>• computing <b>high error rate</b>.</li><li>• no <b>operational proof</b> of quantum advantage.</li><li>• <b>most commercial applications</b> are still at the pilot stage and not production-scale grade but this is also the case for all gate-based quantum computers.</li><li>• <b>all algorithms are hybrid</b>, requiring some preparation on classical computers.</li></ul> |
|---|---|

The general principle consists in establishing links between superconducting flux qubits with "weights" via couplers, a bit like in neural networks used in artificial intelligence, and then converging the system to a point of system equilibrium that corresponds to a minimum energy level. This leads to automatically modify the values of the qubits (spin up or down) towards a result that corresponds to the solution of the submitted problem.

The system is iterative with several annealing passes. At the end of the process, the state of the qubits is read and generates a 0 or a 1 for each of them depending on the direction of the magnetic flux of the superconducting loop. It's called an Ising model. As a result, the solved problem search space is discrete and finite.

---

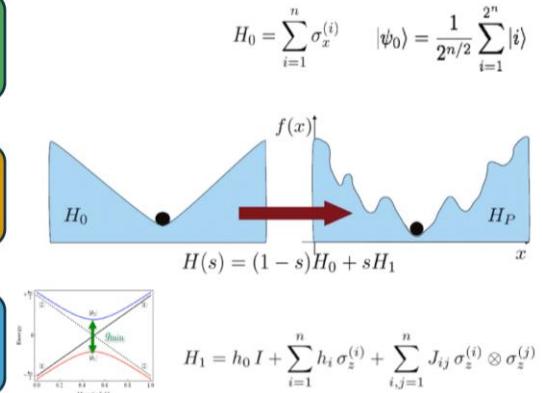
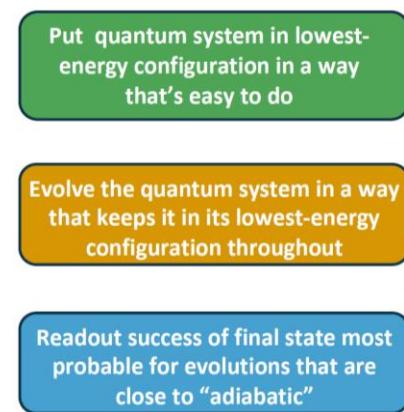
<sup>373</sup> Data sources: cold atoms (<https://arxiv.org/pdf/2006.12326.pdf>), trapped ions (<https://arxiv.org/pdf/1904.04178.pdf>, <https://www.infineon.com/cms/en/product/promopages/trapped-ions/>), silicon (<https://iopscience.iop.org/article/10.1088/1361-6528/abb333/pdf>), superconducting (Google Sycamore and IBM papers), NV centers (<https://aip.scitation.org/doi/pdf/10.1063/5.0007444>). I list only the most demanding fidelity, with two qubit gates and readouts. Single qubits gates fidelities are usually much better. Cold atoms systems are usually simulators, but data pertains to gate-based use-cases. And the 70 entangled qubits in the Chinese photons boson sampling are not gate-based and programmable.

<sup>374</sup> The history and science of quantum annealing computation is well described in [Adiabatic Quantum Computing](#) by Tameem Al-bash and Daniel Lidar of the University of Southern California, 2018 (71 pages).

<sup>375</sup> See the thesis [Superconducting flux qubits for high-connectivity quantum annealing without lossy dielectrics](#) by Christopher M. Quintana, 2017 (413 pages), directed by John Martinis who was then at Google.

There are variations in this model's implementation with regards to the qubits coupling mechanism. It can be made on one degree (Z for D-Wave) or two and three degrees of freedom (X, Y and Z, in a so-called Heisenberg model) like what **Qilimanjaro** (Spain) is planning to achieve.

The system can be initialized in a simple state or one state close to the solution of the problem, evaluated beforehand with a conventional computer algorithm<sup>376</sup>. Adiabatic algorithms are always hybrid, requiring some back-and-forth operations between classical computing and the annealer.



Quantum annealing was explored in 2016 by the IARPA agency in its **Quantum-Enhanced Optimization** (QEO) project, which aimed to create an adiabatic computer void of some of the limitations from D-Wave, particularly in terms of connectivity and quality of qubits. Appropriately, in view of IARPA's mission, the goal was to accelerate the production of quantum computers capable of executing Shor's integer factoring algorithm to break the public keys coming from intercepted communications. This project was folded into DARPA's **QAFS** project (Quantum Annealing Feasibility Study) in February 2020 which produced a 25 coherent annealer system.

**Stanford University** is also working on quantum annealing. In 2016, they created a prototype photonic based annealer with 100 qubits having an all-to-all connectivity (so... 10,000 connections)<sup>377</sup>. This connectivity is what makes such a system "coherent". This research is still going on in 2021 and involves NTT in Japan.

We can also mention the H2020 European project **AVaQus** (Annealing-based VAriational QUantum processorS) launched in October 2020, which brings together five laboratories (Institut de Física d'Altes Energies of Barcelona, Karlsruhe Institut für Technologie (KIT) of Karlsruhe, CNRS Institut Néel in Grenoble, the University of Glasgow and the Consejo Superior de Investigaciones Científicas in Madrid), associated with three startups **Delft Circuits** (Netherlands), **Qilimanjaro** (Spain) and **Heisenberg Quantum Simulations** (HQS) (Germany). The project is scheduled to end in 2023 and got a funding of €3M, independently of the Quantum Flagship program.



Located in Vancouver, Canadian **D-Wave** (1999, \$244M) was for a very long time the only supplier of commercial quantum computers even though many scientists were arguing about the exact "quantum" nature of these machines.

D-Wave was created by Geordie Rose (their first CTO and for some time also their CEO<sup>378</sup>), Haig Farris, Bob Wiens and Alexandre Zagoskin, formerly in charge of research. Geordie Rose received his PhD in Materials Physics in the mid-1990s from the University of British Columbia.

<sup>376</sup> Source of the diagram: [How about quantum computing?](#) by Bert de Jong, June 2019 (47 slides).

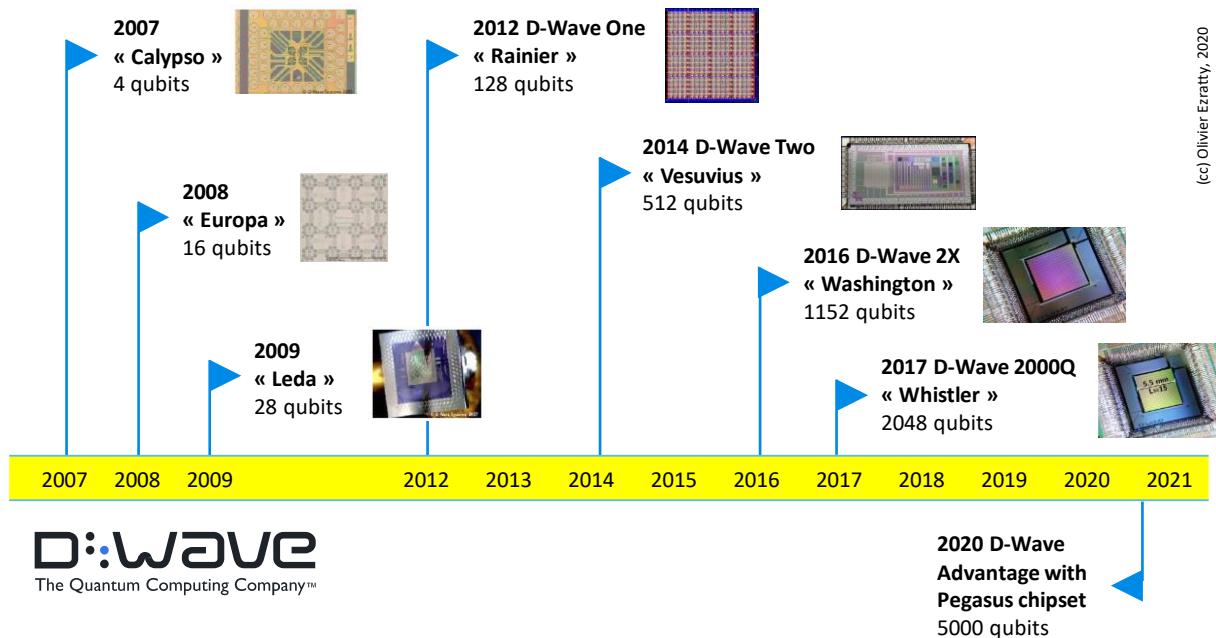
<sup>377</sup> See [A fully-programmable 100-spin coherent Ising machine with all-to-all connections](#) by Peter L. McMahon, Yoshihisa Yamamoto et al, 2016 (9 pages).

<sup>378</sup> Co-founder Geordie Rose then created **Kindred.ai**, a startup that aims to integrate General Intelligence (GIA) into robots. He left Kindred.ai in 2018 to create [Sanctuary](#), a spin-off of Kindred, dedicated to AGI, the quest for the Holy Grail of general artificial intelligence.

The creation of D-Wave is thus a direct result of this work. He met Haig Farris during his studies while the latter was teaching economics.

Founded in 1999, it took D-Wave eight years to prototype its first chip containing four qubits. It took them a total of ten years to sell their first quantum computer. During these ten years, they raised \$31M, then \$1.2M in 2012 from InQTel, the CIA's investment fund. In 2011, D-Wave signed a partnership with Lockheed Martin, which does some work for the NSA. All in all, the startup went through 13 rounds of funding!

D-Wave's 2021 management team is quite different. Only one of the co-founders is still part of it, Eric Ladizinsky, who plays the role of Chief Scientist. The CEO from 2009 to 2020 was Vern Brownell. Their CTO Alan Baratz joined the company in 2017 and became CEO in 2020. We feel a kind of recovery in hand.



Although quantum annealing accelerators have technical limitations compared to general-purpose quantum computers, they have the advantage of being there and have a strong software ecosystem. However, case studies solutions published by D-Wave and their customers and partners seem to remain "proofs of concept". Few seem to have been deployed, be production-grade, or at least provide a quantum advantage over classical computing.

D-Wave has developed its end-to-end quantum annealing computer solution. It is the first full-featured quantum computer in history with a design that allows it to be easily integrated into a clean room. The cryogenic part includes an enclosure with five layers of magnetic isolation.

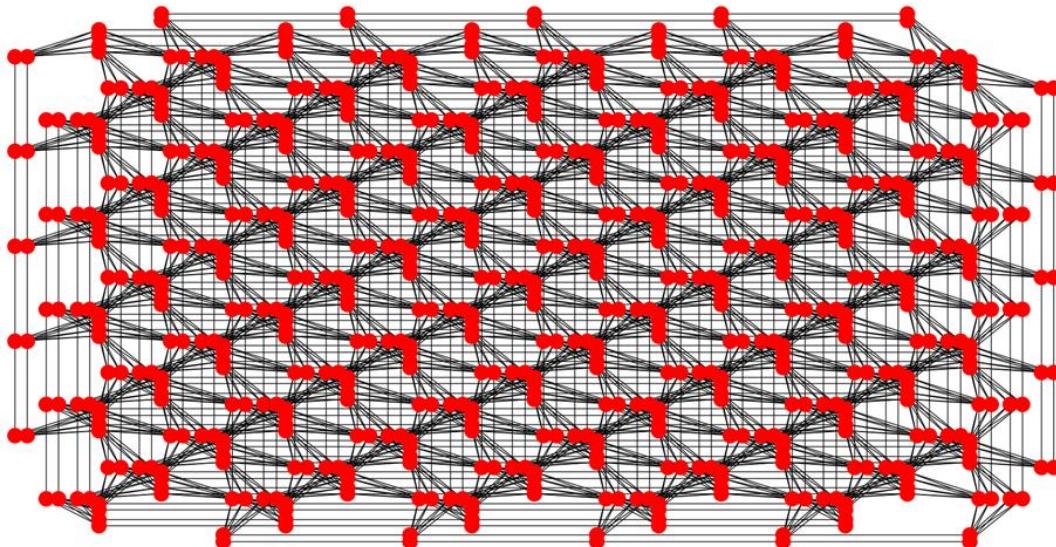
Their roadmap has progressed steadily with the first three generations of prototypes created between 2007 and 2009 and then, starting from 2012, five generations of commercial computers, starting with the D-Wave One in 2012 with 128 qubits, the D-Wave 2000Q in 2017 with 2000 qubits up to the D-Wave Advantage launched in September 2020 with 5,640 qubits and one million Josephson junctions<sup>379</sup>.

<sup>379</sup> See [Quantum annealing with manufactured spins](#) by Mark Johnson et al, 2011 (6 pages) which outlines the D-Wave process. As well as [Technical Description of the D-Wave Quantum Processing Unit](#) by D-Wave, 2020 (56 pages) and related [supplemental information](#) (19 pages). The Pegasus architecture from the D-Wave advantage is described in [Next Generation Quantum Annealing System](#) by Mark Johnson, March 2019 (27 slides) and in [Next-Generation Topology of D-Wave Quantum Processors](#) by Kelly Boothby et al, 2019 (24 pages). See [D-Wave Announces General Availability of First Quantum Computer Built for Business](#) by D-Wave, September 2020.



D-Wave Two	D-Wave 2X	D-Wave 2000Q
512 (8x8x8) qubit “Vesuvius” processor	1152 (8x12x12) qubit “Washington” processor	2048 (8x16x16) qubit “Whistler” processor
509 qubits working – 95% yield	1097 qubits working – 95% yield	2038 qubits working – 97% yield
1472 J programmable couplers	3360 J programmable couplers	6016 J programmable couplers
<b>20 mK max operating temperature (18 mK nominal)</b>	<b>15 mK max operating temperature (13 mK nominal)</b>	<b>15 mK max operating temperature (nominal to be measured)</b>
5% and 3.5% precision level for $h$ and $J$	3.5% and 2% precision level for $h$ and $J$	<i>To be measured</i>
20 <b>us</b> annealing time 12 <b>ms</b> programming time	5 <b>us</b> annealing time (4X better) 12 <b>ms</b> programming time	5 <b>us</b> annealing time 9 <b>ms</b> programming time (25% better) <b>New:</b> anneal offset, pause, quench
6 graph connectivity per qubit	6 graph connectivity per qubit	6 graph connectivity per qubit

One D-Wave Advantage was ordered by the Doe Los Alamos National Laboratory in September 2019, maybe to investigate some nukes simulation capabilities<sup>380</sup>. The previous generation launched in 2017 was the 2000Q with 2048 qubits and 128,000 Josephson junctions on a (5.5 mm)<sup>2</sup> chipset.



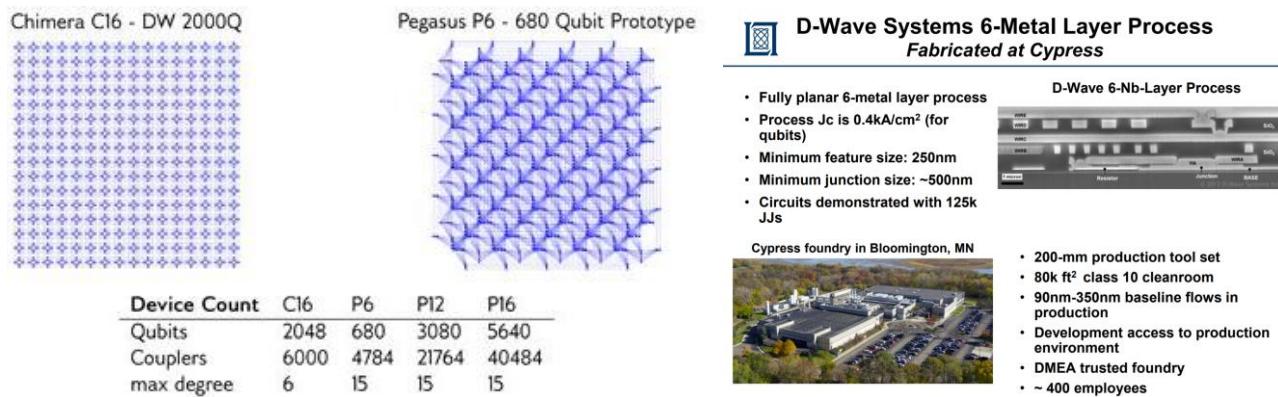
The 2000Q had a list price of \$15M. The Pegasus chipset is larger, being a square of 8.5 mm. It is manufactured in the USA in **Cypress Semiconductor fab** located in Bloomington, Minnesota. The embedding graph or qubits connectivity is branded a chimera by D-Wave<sup>381</sup>.

In the Pegasus architecture, each qubit is linked to 15 other qubits compared to 6 in the 2000Q<sup>382</sup>. It allows more complex problems to be solved with an equivalent number of qubits.

<sup>380</sup> See [Nuclear weapons lab buys D-Wave's next-gen quantum computer](#) by Stephen Shankland, September 2019.

<sup>381</sup> D-Wave's chimera matrix requires a conversion process of its qubit mesh problem. This process is so far mostly exploited for problems that fit well with this qubit organization. For an arbitrary optimization problem, the conversion gives a result that is not convincing in terms of efficiency and acceleration. This is what emerges from the work of Daniel Vert, then PhD student at CEA LIST, in [On the limitations of the chimera graph topology in using analog quantum computers](#) by Daniel Vert, Renaud Sidney and Stéphane Louise, CEA LIST, 2019 (5 pages) and in [Revisiting old combinatorial beasts in the quantum age: quantum annealing versus maximal matching](#) by the same authors, October 2019 (36 pages). D-Wave's chimera structure limits the way a QUBO or other optimization problem can be converted into an Ising problem solvable with D-Wave's chimera structure.

All this with a rather high error rate, measured as a precision with the Ising model parameters, which is over 2%<sup>383</sup>. The high-error rate of D-Wave annealing systems can be mitigated with some quantum error correction technique, created in 2019<sup>384</sup>.



Other researchers even found that the thermal noise involved in the annealing process could be used as a resource to enable faster and more reliable computations, involving the curious process or reverse annealing<sup>385</sup>. It could help finding a better solution than an existing solution already computed with a regular annealing process.

The D-Wave qubits are rf-SQUID type made with niobium, exploiting superconducting current loops interrupted by two Josephson effect barriers that are controlled by variable magnetic fluxes. The diagram *below* explains all this.

The cryostat uses a dry dilution system (*aka* cryogen free dilution refrigerator, we study it in a [dedicated part](#) of this ebook, page 370) similar to the ones used with gate-based superconducting qubits, cooling the quantum chip at 12-15 mK. Cryogeny consumes about 16kW out of a total of 25kW. The remaining 9kW is related to traditional computer control systems that are outside the cryostat.

The basic principle of D-Wave is to prepare what is called a Hamiltonian of an optimization problem called **Ising model**<sup>386</sup> or a **QUBO** (Quadratic Unconstrained Binary Optimization) model that can be reduced to an Ising model.

These are optimization problems where the variables can only take two values (-1 or +1 or 0 and 1) and where they are linked together by different fixed parameters which are defined as floating numbers (FP32). However, the digital/analog converters (DAC) for preparing the qubits introduce significant sampling noise so that, in the end, the precision of the data of the problem to be solved is much lower, probably below one single byte. We're far from high-precision floating point scientific computation<sup>387</sup>.

<sup>382</sup> The chimera uses cells with 8 qubits with internal and external couplings. It has 4 internal couplings within cells and 2 external couplings in pre-Pegasus chipsets and 12 internal and 3 external couplings in Pegasus chipsets.

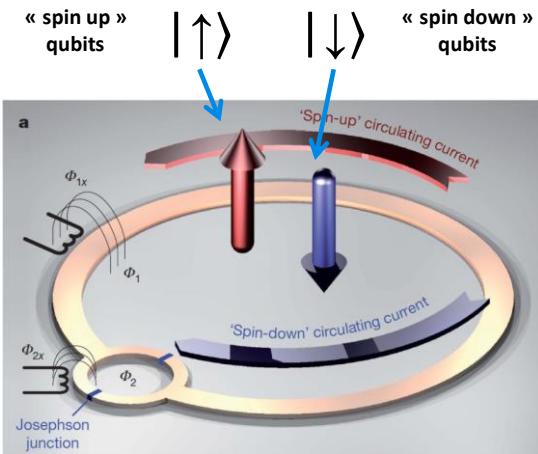
<sup>383</sup> The question remains open as to whether this architecture is scalable and provides a real quantum advantage. This is questioned in [Fundamental Limitations to the Scalability of Quantum Annealing Optimizers](#) by Tameen Albash et al, 2019. The reasons: issues of noise and thermodynamics.

<sup>384</sup> See [Analog errors in quantum annealing: doom and hope](#) by Adam Pearson et al, 2019 (16 pages).

<sup>385</sup> See [Thermodynamic study of D-Wave processor could lead to better quantum calculations](#) by Hamish Johnston, June 2020.

<sup>386</sup> It is a statistical physics model created to solve problems of simulation of ferromagnetic and para-magnetic materials associating particles having two state levels (a magnetic moment +1 or -1) which are linked together.

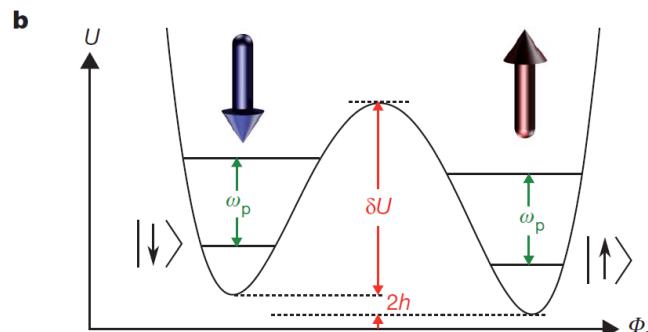
<sup>387</sup> I found this in some D-Wave documentation but could not track it back.



$\Phi_{1x}$  : flux bias on the outer superconducting loop which controls the energy difference «  $2h$  » between two states, i.e. superconducting current direction

$\Phi_{2x}$  : flux bias on the inner superconducting loop with two Josephson junctions, controlling energy level  $\delta U$  enabling the switch between two spin directions

## rf-SQUID flux qubits



schémas D-Wave et légendes [cc] Olivier Ezratty, 2021

$\omega_p$  : energy variation for  $| \uparrow \rangle$  et  $| \downarrow \rangle$  states

$\delta U$  : energy potential barrier between states

$2h$  : energy difference between the two base states

The problem to be solved is transformed into a quantum system with several interconnected qubits describing a given energy balance. This Hamiltonian must be initialized in a state that is close to the solution of the problem to be solved. This initial state is evaluated beforehand using an algorithm running on a classical computer.

The annealing process consists in making the system converge towards its minimum energy level allowing to find the optimal values of the qubits (-1 and +1 or 0 and 1) according to the fixed variables of the problem which are the  $h_i$  (the energy deltas between the two states of each qubit  $i$ ) and  $J_{ij}$  (value of the coupling between qubits  $i$  and  $j$ ). We are thus looking for a minimum energy of a complex multi-parameter system whose variables are discrete and can only take two possible values and whose parameters are low precision numbers.

« Ising model »

$$\text{system total energy (hamiltonian)} \quad \mathcal{H}_P = \sum_{i=0}^N h_i \sigma_i^z + \sum_{i < j} J_{ij} \sigma_i^z \sigma_j^z$$

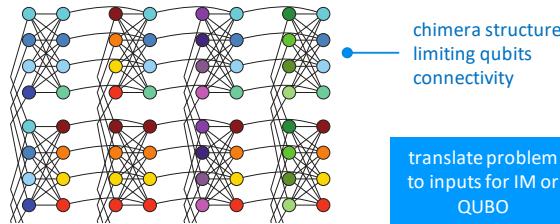
$H_P$  : system hamiltonian

$h_i$  : energy difference between two states of qubits  $i$

$V_i$  : vertices containing qubit  $i$

$J_{ij}$  : coupling between vertices  $V_i$  and  $V_j$  with close  $i$  and  $j$

$E$  : edge, connecting qubits

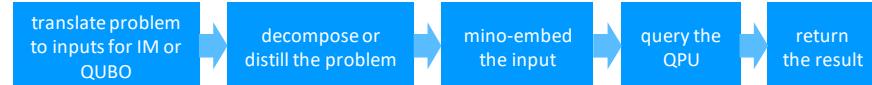


### computing process:

starts with converting the problem into an Ising model or QUBO (Quadratic Unconstrained Binary Optimization)

- 1 initialization of qubits states to  $| \uparrow \rangle$  or  $| \downarrow \rangle$
- 2 setting qubits bias levels  $h_i$
- 3 slowly growing  $J_{ij}$  couplings
- 4 system converging to minimal  $H_P$
- 5 readout  $| \uparrow \rangle$  or  $| \downarrow \rangle$  states for all qubits, giving the solution to the problem of finding the energy minimum for  $H_P$

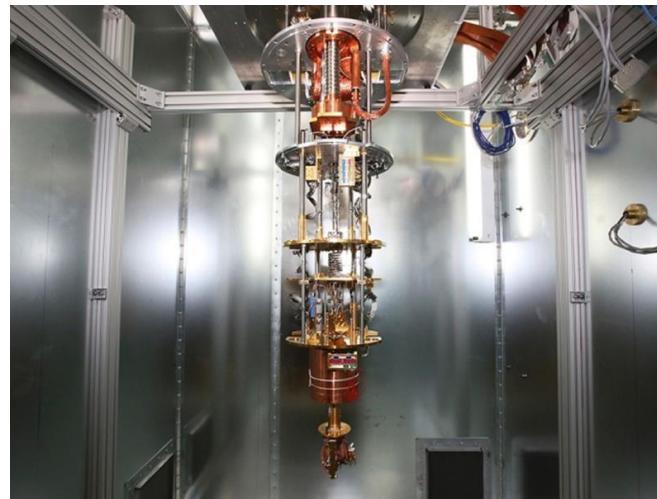
(cc) Olivier Ezratty, August 2021



Annealing uses the quantum tunnelling effect which allows the system to easily find global minima instead of being stuck in local minima, a problem reminiscent of the gradient descent in neural network training<sup>388</sup>. It should be mentioned that D-Wave systems require frequent recalibration. It's also the case with most gate-based superconducting qubit computing systems.

The initialization of the D-Wave 2000Q takes 25 ms, the system convergence time (annealing) take 20  $\mu$ s and reading time is 260  $\mu$ s, these two steps are usually repeated several times and the results averaged, a practice common with universal gate quantum computers.

The initialization signals of the Hamiltonian are multiplexed and sent in digital format from the outside to the chip. This seems to simplify the cabling of the cryogenic enclosure of the computer compared to the superconducting IBM and Google computers, as shown in the *adjacent* illustration of a 2000Q. Most of what can be seen in the intermediate stages in the cryostat corresponds to the dilution cryogenics system. Let's also mention that annealers don't need to send microwave pulses to qubits and thus, avoid the related coaxial cables used in gate-based superconducting qubits.



Some of the magic comes from the integrated DC ramp pulses generation circuits that are sitting in the quantum chip. These circuits use SFQ components, basically superconducting transistors using Josephson effect loops close to those of the qubits. Still, these components are noisy and may contribute to the noise affecting the qubits in this architecture<sup>389</sup>.

According to D-Wave, their accelerators are able to solve NP-complete problems, a category of combinatorial problems theoretically solved in polynomial time on D-Wave but which are solved in exponential time on a classical computer<sup>390</sup>. This is the case for routing problems, traveling salesman problem and the likes. D-Wave could also be used to solve statistical problems<sup>391</sup>. The assertion has not really been proven at this stage at a large scale where the quantum annealing regime would exceed the capacity of classical supercomputers.

What is quantum in D-Wave? It is mainly the tunnelling effect that allows the system to quickly search for a global energy minimum of an N-body system. It is coupled with superposition of the states of orientation of the electrical current in the Josephson loops. According to D-Wave, the system also uses entanglement, which is poor, but this has been questioned by some scientists<sup>392</sup>.

---

<sup>388</sup> See for example [Architectural considerations in the design of a superconducting quantum annealing processor](#), 2014 (9 pages) which describes the hardware architecture of the 2014 D-Wave processors, which have not changed much since then.

<sup>389</sup> See [Analog errors in quantum annealing: doom and hope](#) by Adam Pearson, 2019 (9 pages).

<sup>390</sup> See [Practical Annealing-Based Quantum Computing](#) by Catherine McGeoch et al of D-Wave, June 2019 (16 pages) which makes an inventory of the benefits of quantum annealing computing, especially in terms of the size of the problems to be solved, which should be neither too small because they are trivial, nor too large because they must then be broken down into sub-problems that are manageable with the capacity of current D-Wave processors. It seems that the problems to be solved must have global minimums and local minimums, the first being difficult to find with classical methods.

<sup>391</sup> See [Applications of Quantum Annealing in Statistics](#) by Robert C. Foster, 2019 (30 pages).

<sup>392</sup> Jonathan Dowling thought in the previous reference that the only quantum effects of D-Waves were tunneling and superposition, but without quantum entanglement.

The algorithms designed for classical quantum gate computers that we will see later are executed sequentially. All of them can theoretically be converted into algorithms executable on D-Wave and vice versa at a polynomial computing time cost, which can be substantial<sup>393</sup>. The same algorithm will require many more qubits with D-Wave than with a universal quantum computer.

On a D-Wave, the number of qubits would need to be up to 32 times the number of quantum gates of the classical quantum algorithm<sup>394</sup>.

According to **John Preskill**, there is no convincing theoretical basis for the advantage of quantum annealing, which is one form of adiabatic quantum computing<sup>395</sup>. He thinks this architecture is not theoretically as scalable as general-purpose quantum computers. The arguments about D-Wave's annealers quantumness revolve around the low-scale coherence between qubits which may prevent an efficient implementation of quantum annealing<sup>396</sup>. It is also related to the limited connectivity between qubits<sup>397</sup>.

Others estimate that D-Wave systems can generate at best some quadratic acceleration and not an exponential one, compared to traditional computing<sup>398</sup>. **Daniel Lidar** from the University of Southern California is investigating variations of quantum annealing algorithms that could solve intractable problems on classical computers<sup>399</sup>.

As of mid-2021, D-Wave had installed over half a dozen quantum computers at customer sites<sup>400</sup> and operates more than 30 of them in its own facilities, with more than half of them dedicated to their cloud access offering. Some of them are now available through the Amazon Braket cloud offering.

Like all major players in the quantum field, D-Wave has developed its own software development platform supporting the lower layers of quantum algorithms creation for its machines, which we discuss in the [development tools](#) section, page 499. The proposed tools include at a high level Qsage, a tool to define optimization problems, ToQ, an equivalent tool for constraint programming, then at an intermediate level, qbsolv which allows to distribute a complex problem over several D-Wave passes and at the lowest level, QMI instructions to drive the qubits. They also offer Quadrant, a framework to prepare D-Wave to solve learning machine problems. D-Wave also has a good number of startups that publish software for its computers in Japan.

One of the oldest D-Wave publicized case study comes from Google and NASA using a 2013 D-Wave to solve an optimization and combinatorial problem in a graph whose algorithm was designed in 1994.

---

<sup>393</sup> This is documented in [Adiabatic quantum computation is equivalent to standard quantum computation](#), 2005 (30 pages) and in [How Powerful is Adiabatic Computation?](#) by Wim van Dam, Michele Mosca and Umesh Vazirani, 2001 (12 pages).

<sup>394</sup> From "Automatically Translating Quantum Programs from a Subset of Common Gates to an Adiabatic Representation" by Malcolm Regan et al, seen in [Reversible Computation](#), conference proceedings, 11th International Conference, RC 2019, Lausanne, Switzerland, June 2019 (246 pages).

<sup>395</sup> In [Quantum Computing for Business](#), 2017 (41 slides).

<sup>396</sup> See [How "Quantum" is the D-Wave Machine?](#) by Seung Woo Shin, Umesh Vazirani et al, 2014 (8 pages).

<sup>397</sup> See the example of [Phase-coded radar waveform AI-based augmented engineering and optimal design by Quantum Annealing](#) by Timothé Presles et al, Thales, August 2021 (9 pages). In this use case, no quantum advantage can be seen with D-Wave due to limited qubits connectivity.

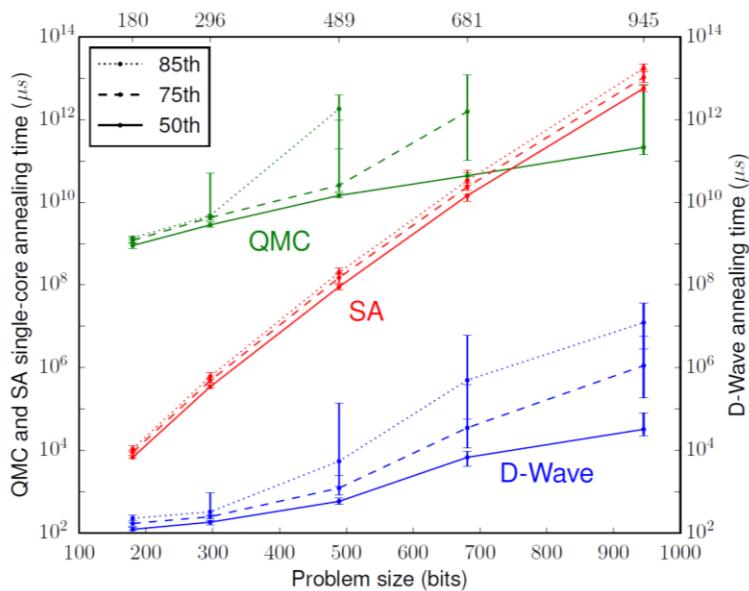
<sup>398</sup> This is the opinion of Jonathan P. Dowling in [Schrödinger's Killer App - Race to Build the World's First Quantum Computer](#) by Jonathan P. Dowling, 2013 (445 pages), pages 208 to 216.

<sup>399</sup> See his [Adiabatic quantum computing](#) page on USC Quantum Computation and Open Quantum Systems web site.

<sup>400</sup> Identified customers are the joint Google/NASA Quail research center, USRA (Universities Space Research Association), Lockheed Martin and the University of Southern California sharing one system, and Jülich Supercomputing Centre in Germany (since 2021). Other customers like in pharmaceutical companies are using D-Wave annealers through their Leap cloud offering.

Google announced in 2015 that it had achieved a performance 100 million times better than that of traditional computers, in fact, a single core of an Intel Xeon server processors<sup>401</sup>. Like many such claims, they were questionable since based on a single optimized algorithm, here, a Quantum Monte Carlo simulating quantum tunneling on a classical computer.

The elements of comparison concerned two algorithms intended for them the "simulated annealing", simulating the D-Wave computer on traditional computers and a QMC (Quantum Monte Carlo) optimized for traditional computers, and which gives better results in terms of power increase than the emulation of the quantum on HPC. Critics abounded about this performance<sup>402</sup>.



D-Wave communicates on many other of its pilot references<sup>403</sup>. Its web site references 250 case studies, the largest number of any quantum computing vendor:

- **Denso**, a Japanese car equipment manufacturer presented at CES 2017 in Las Vegas a system for optimizing a fleet of Toyota delivery vehicles.
- **Biogen, 1Qbit** and **Accenture** did prototype a screening solution to identify molecules for drug retargeting, with a problem of map staining<sup>404</sup>. It is difficult to say what this has generated in practice. Their partner **Menten AI** performs protein analysis.
- **Lockheed-Martin** produced some validation procedures for its embedded software in 6 weeks instead of 8 months with a D-Wave and its QVTRace tool<sup>405</sup>.
- **Volkswagen** simulated the operations of a cab fleet in Beijing and also a solution to develop new batteries<sup>406</sup>. The solution was used in November 2019 to optimize the shuttle route at Lisbon's WebSummit, in partnership with Here and Volkswagen's Data:Lab in Munich.

<sup>401</sup> In [Google's D-Wave 2X Quantum Computer 100 Million Times Faster Than Regular Computer Chip](#) by Alyssa Navarro in Tech Times, November 2015 and documented in [What is the Computational Value of Finite Range Tunneling](#) (17 pages).

<sup>402</sup> Including [Temperature scaling law for quantum annealing optimizers](#), 2017 (13 pages), which points out the limitations of quantum annealing.

<sup>403</sup> I found this inventory in [Quantum Applications](#) by D-Wave, May 2019 (96 slides).

<sup>404</sup> Described in [Programming with D-Wave Map Coloring Problem](#), 2013 (12 pages).

<sup>405</sup> See [Quantum Computing Approach to V&V of Complex Systems Overview](#), 2014 (31 slides) and [Experimental Evaluation of an Adiabatic Quantum System for Combinatorial Optimization](#), 2013 (11 pages).

<sup>406</sup> See [Forget quantum supremacy: This quantum-computing milestone could be just as important](#) by Steve Ranger, December 2019.

- **NASA** has experimented with D-Wave in various fields, including the detection of exoplanets by analysis of telescopic observations using the transit method, as well as for various optimization and planning problems<sup>407</sup>.
- **GE Research** experimented some hybrid maintenance resource allocation optimization application.
- **Ocado**, a British retailer, prototyped some optimization solution for its robots-based warehouse operations.
- **Los Alamos National Laboratory** with **Stanford University** prototyped the detection of the formation of terrorist networks in Syria with analyzing imbalances in social networks<sup>408</sup>.
- **Volkswagen** experimented quantum annealing to optimize car paint-shop processing in order to minimize color switching, but with no clear quantum advantage<sup>409</sup>.
- With **physical simulations of topological matter and phase change**<sup>410</sup>.
- In April 2020, D-Wave opened free access to its cloud computers to researchers looking for **solutions** to the **covid pandemic19**<sup>411</sup>. The solutions developed included solving optimization problems such as optimizing patient routing to hospitals in Japan, modeling the spread of the virus, managing nurses' schedules in hospitals, assessing the rate of virus mutation and screening molecules. It remains to be proven that D-Wave provides a real quantum advantage in solving these different problems.
- It's even possible to use the **Prolog language** to solve a decision problem on a D-wave system<sup>412</sup>.
- In February 2021, D-Wave and Google published a study showcasing a computational advantage of annealing with the **D-Wave Advantage** for simulating some condensed matter physics, 3 million times faster than with classical methods. It didn't exactly describe the classical hardware that is being compared, but it looked like a traditional Intel-based server<sup>413</sup>. These comparisons done with a single narrow algorithm are way not enough to draw any conclusions.

In summary, quantum annealing may be a technique contested by many specialists, but it has the merit of existing and being testable in many use cases<sup>414</sup>. It will probably make some progress with newly published cases running on its recent Advantage generation.

---

<sup>407</sup> See [Quantum Computing at NASA: Current Status](#) by Rupak Biswas, 2017 (21 slides) as well as [Adiabatic Quantum Computers: Testing and Selecting Applications](#) by Mark A. Novotny, 2016 (48 slides).

<sup>408</sup> See [Using the D-Wave 2X Quantum Computer to Explore the Formation of Global Terrorist Networks](#) by John Ambrosiano et al, 2017 (14 pages).

<sup>409</sup> See [Multi-car paint shop optimization with quantum annealing](#) by Sheir Yarkoni et al, September 2021 (7 pages).

<sup>410</sup> See [Observation of topological phenomena in a programmable lattice of 1,800 qubits](#), August 2018 (37 slides).

<sup>411</sup> See [Can Quantum Computers Help Us Respond to the Coronavirus?](#) by Mark Anderson, April 2020.

<sup>412</sup> See [Performing Fully Parallel Constraint Logic Programming on a Quantum Annealer](#) by Scott Pakin, 2018 (22 pages).

<sup>413</sup> See [Scaling advantage over path-integral Monte Carlo in quantum simulation of geometrically frustrated magnets](#), February 2021 (6 pages).

<sup>414</sup> To learn more about D-Wave, here are their [explanations about the structure of their hardware](#), a [video](#) explaining the structure of D-Wave chipsets, a [video from Linus](#), a blogger who gets into the bowels of a D-Wave 2000Q in quite a detailed way, the [video of Colin Williams's presentation at USI in June 2018 in Paris](#) (33 minutes) as well as [Near-Term Applications of Quantum Annealing](#), 2016, an interesting Lockheed Martin presentation on the uses of a D-Wave computer (34 slides). And testimonials from their customers in [Qubits 2017](#). See also [Brief description on the state of the art of some local optimization methods: Quantum annealing](#) by Alfonso de la Fuente Ruiz, 2014 (21 pages).

In October 2021, D-Wave made significant announcements as part of their Clarity roadmap with an upcoming Advantage 2 generation with 7000 qubits and 20-way qubits connectivity, and a gate-based model including a new quantum error correction architecture. This will be implemented in a separate (flux-based) superconducting processor, starting with a few qubits. They plan to use surface code QECs and to use some combination of RSFQ and other cryo-electronics to control these qubits.



**Qilimanjaro** (2019, Spain) is a startup based in Barcelona created by three Spanish physicists coming from different Spanish institutions (Barcelona Supercomputing Center, IFAE, University of Barcelona) and with a strong international experience and two experienced business managers<sup>415</sup>!

The founding team assembles Jose Ignacio Latorre (Chief Science Officer, also now the Director of CQT in Singapore and Chief Research of CRO Quantum at TII in Abu Dhabi, went through MIT, CERN and Niels Bohr Institute), Pol Forn-Díaz (Chief Hardware Architect, TU Delft, MIT, Caltech and IQC Waterloo), Artur Garcia Sáez (Chief Software Architect, ICFO, Stony Brook), plus Víctor Canivell (Chief Business Officer) and Jordi Blasco (Chief Financial & Legal Officer).

They develop their own quantum annealer based on coherent flux qubits. Their differentiation lies with a better qubit coherence, qubits coupling designs<sup>416</sup> and qubits connectivity.

These qubits will be first controlled by classical electronics working at room temperature. In a later stage, they plan to create cryogenic controls on a separate chipset. They rely on two fabs for their qubits designs, the one from IFAE and the one from the Institute of Microelectronics of Barcelona (IMB-CNM, which has similarities with the C2N in Palaiseau, France).

In a full-stack approach, they are also developing **QIBO**, a quantum software platform in the cloud<sup>417</sup>. It is the cloud operating service to run software batches on the future Qilimanjaro quantum annealer, classical quantum emulators and gate-based quantum computers with a design pattern to create classical/quantum hybrid algorithms. But they also plan to sell their hardware to customers willing to use it on-premises.

They initially wanted to launch an ICO (initial coin offering) to fund the company when it was trendy but abandoned it. On top of benefiting from public grants, the company started to work for an unnamed French international company involved in logistics to develop quantum inspired optimization algorithms. They then established a partnership with Abu-Dhabi to help the Emirate create its Quantum Research Centre at the Technology Innovation Institute (QRC-TII). They provide Abu Dhabi with their know-how to build the QCR research lab and team, provide access to their technology with the goal to sell them a multi-qubit quantum processor before 2023, and let them then become self-sufficient. Jose-Ignacio Latorre became their TII's Chief Scientist after the deal was made. In 2020, he also became the director of CQT in Singapore after having been a visiting professor since 2013. CQT may play a role first in Qilimanjaro's software development efforts.

Qilimanjaro also benefits from European funding through the project **AVAQUS** already mentioned. This project coordinator is Pol Forn-Díaz, head of the IFAE Quantum Computing Technologies group on top of his role in Qilimanjaro. It involves the superconducting team from Nicolas Roch at Institut Néel in Grenoble who designs the microwave amplifiers used in flux qubits readouts<sup>418</sup>.

---

<sup>415</sup> See [Startup Qilimanjaro—towards a European full-stack coherent quantum annealer platform](#) by Victor Canivell et al, 2021 (9 pages).

<sup>416</sup> They will use a Heisenberg Ising model with X and Y interactions on top of the Z interactions that D-Wave is using. It enables the preparation of Hamiltonians with more degrees of liberty, so, to solve more complicated problems.

<sup>417</sup> See [Qilimanjaro White paper](#) (54 pages).

<sup>418</sup> See [A reversed Kerr traveling wave parametric amplifier](#) by Arpit Ranadive et al, 2021 (12 pages).



At last, let's mention that NEC (Japan) is also developing coherent quantum annealers using parametric oscillators and qubits as couplers.

They ambition to have an available system by 2023 with an “all-to-all” qubits connectivity (which is actually a nearest-neighbor one) ([source](#)). They seem to reuse some research work done on superconducting qubits initially aimed at gate-based quantum computing. Meanwhile, they also work on some simulated annealing software running on their classical supercomputer, the SX-Aurora Tsubasa.

## Superconducting qubits

After describing superconducting-based quantum annealing, let's move on to gate-based superconducting quantum computers. From a physical point of view, D-Wave's accelerators and superconducting qubits ones are quite similar, using variants of the Josephson effect in superconducting circuits. However, the way they are architected and programmed is quite different<sup>419</sup>.

### superconducting qubits

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• <b>key technology</b> in public research and with commercial vendors (IBM, Google, Rigetti, Intel, Amazon, etc).</li><li>• <b>record of 65 programmable qubits</b> with IBM.</li><li>• constant progress in <b>noise reduction</b>, particularly with the cat-qubits variation which could enable a record low ratio of physical/logical qubits.</li><li>• many existing <b>enabling technologies</b>: cryostats, cabling, amplifiers, logic, sensors.</li><li>• <b>potentially scalable technology</b> and deployable in 2D geometries.</li></ul> | <ul style="list-style-type: none"><li>• low <b>qubit coherence time</b> &lt; 300 µs.</li><li>• high <b>qubits noise levels</b>.</li><li>• <b>heterogeneous qubits</b> requiring calibration and complex micro-wave frequency maps.</li><li>• <b>cryogeny constrained</b> technology at &lt;15 mK.</li><li>• <b>cabling complexity</b> and many passive and active electronic components to control qubits with micro-waves.</li><li>• <b>coupling limited</b> to neighbor qubits in 2D structures.</li><li>• <b>qubits size</b> and uneasy miniaturization.</li></ul> |
|--|---|

Superconducting qubits seem to be the kings in town, being exploited or chosen by IBM, Google, Intel, Rigetti, Amazon, many startups such as IQM (Finland) and Alice&Bob (France). It is the currently best scalable architecture, even if the results are modest with a record of 65 operational qubits for with IBM and 60 in China<sup>420</sup>.

Like all existing gate-based quantum systems, superconducting qubits computers are in the NISQ category, noisy intermediate-scale computers, with such a low qubit gates and readout fidelity that they are impractical for most industry use cases. It is observable with the discrepancy between the number of available physical qubits (53 and 65 with Google and IBM) and the number of qubits that are actually exploited with useful algorithms, that doesn't exceed 20 at this point in time. IBM's quantum volume is even capped at 6 useful qubits with their 27 qubits systems!

The workaround of low fidelity is error correction and qubits number scalability. It creates problems that are not yet solved with regards to fidelity stabilization with a growing number of qubits, solving the qubits cabling maze with cryogenic electronics and scaling cryostats cooling power.

<sup>419</sup> To learn more about superconducting qubits and the challenges of their development, see in particular this excellent presentation from MIT: [Quantum Engineering of Superconducting qubits](#), 2018 (58 slides) and [Quantum Physics with Superconducting Qubits](#) by Andreas Wallraff, ETH Zurich, 2016 (49 slides). See also [Quantum Computing: State of Play](#) by Justin Dressel, 2018 (34 slides) which includes a good explanation of how superconducting qubits work.

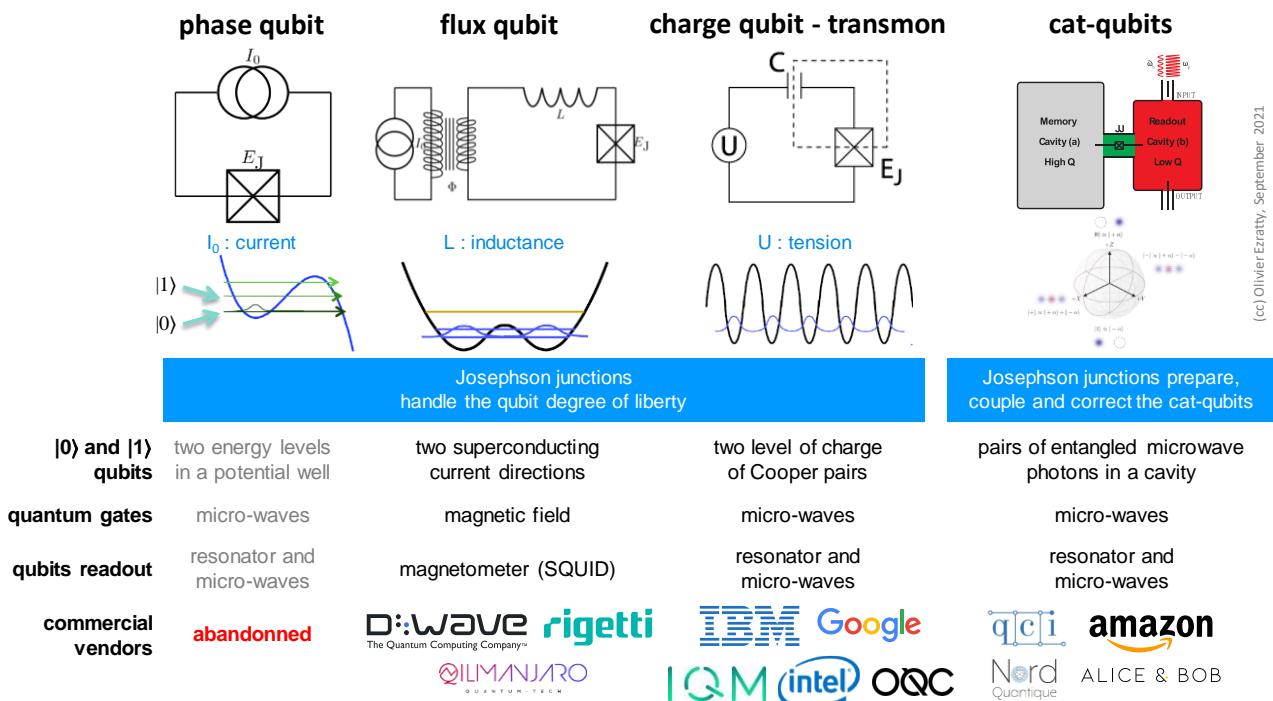
<sup>420</sup> See a general point on the issue in [Superconducting Qubits: Current State of Play](#) by Morten Kjaergaard et al, MIT & Chalmers, 2020 (30 pages).

These problems are rarely addressed explicitly in the current scientific literature. Google and IBM's current approaches to scale their systems are a bit far-fetched as we'll see later<sup>421</sup>.

The Josephson effect is used in these qubits to control the flow of a circulating current through a thin nanometric insulating barrier between two superconducting metals, creating a tunnel junction. It creates a dissipationless non-linear physical system with a single degree of freedom, the number of Cooper pairs (electron pairs) traversing the tunnel junction conjugated to the superconducting phase difference across it.

Superconducting qubits have the particularity of being the only ones that are macroscopic, in the sense that they are not linked to the control of a single particle as an atom, electron or photon as in most other qubit technologies.

At superconducting temperature, the superconducting electrons in a Josephson loop behave like a single particle, assembling electron Cooper pairs behaving as bosons which can be condensed into the same quantum state. They form artificial atoms with precisely controllable energy levels according to their parameters comprising a Josephson barrier, capacitances and inductances connected in series and/or in parallel<sup>422</sup>. One qubit is using about  $10^{11}$  electrons (100 billion).



inspired from [Implementing Qubits with Superconducting Integrated Circuits](#) by Michel Devoret, 2004 (41 pages) and [Flux Noise in Superconducting Qubits](#), 2015 (44 slides).

There are several types of superconducting qubits that differ in the way they encode quantum information in two distinct states<sup>423</sup>:

**Phase Qubits** use larger Josephson junctions than in charge qubits. Their state correspond to two levels of current energy in a Josephson junction. This approach is being tested by NIST in the USA among other places but no commercial vendor seems to use this type of superconducting qubit.

<sup>421</sup> See for example the review paper [A practical guide for building superconducting quantum devices](#) by Yvonne Y. Gao et al, September 2021 (49 pages).

<sup>422</sup> This artificial atom property was demonstrated in 1985. See [Energy-Level Quantization in the Zero-Voltage State of a Current-Biased Josephson Junction](#) by John Martinis, Michel Devoret and John Clarke, 1985 (2 pages).

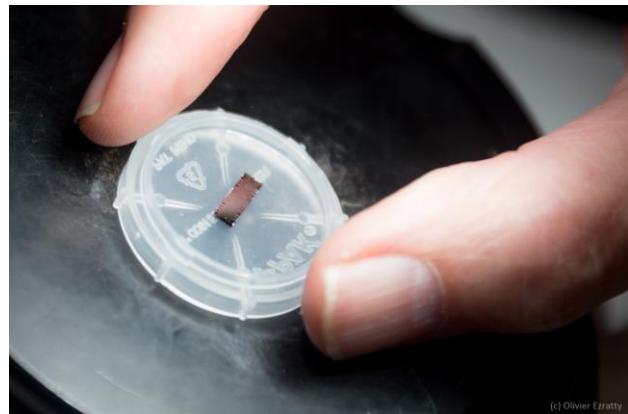
<sup>423</sup> This is well explained in [Practical realization of Quantum Computation](#), (36 slides).

A German (Jülich, University of Munster) and Russian (Kotelnikov Institute) team proposed in early 2020 to use  $\text{YBa}_2\text{Cu}_3\text{O}_{7-x}$  nanotubes (also called YBCO, for yttrium, barium, copper and oxide, which is superconducting at 92K) to create phase qubits controllable by a single microwave photon<sup>424</sup>. No commercial vendor has adopted this type of superconducting qubit.

**Flux Qubits:** their states correspond to the direction of flow of the superconducting current in its loop. It is the easiest to understand and visualize. Measuring the state of such a qubit uses a SQUID (superconducting quantum interference device) with two Josephson junctions connected in parallel, a magnetometer that measures the current direction in the qubit, thus its basis state 0 or 1. This is the approach of D-Wave, Rigetti, MIT and TU-Delft (until 2010).

**Charge Qubits:** their states correspond to current flow thresholds in the Josephson junction of the superconducting loop. Small Josephson junctions delimit a superconducting island with a well-defined electrical charge. The basic states of such charge qubits are the states of charge of the island in pairs of superconducting electrons called Cooper pairs. The most common variant is the **transmon**, for “transmission line shunted plasma oscillation qubit”, which reduces the effect of charge noise<sup>425</sup>. With transmons, the Cooper pairs box is operated in the phase regime. The non-linear Josephson junction inductance makes the LC resonator slightly anharmonic, and its two lowest energy level provide a qubit, as described later. Transmons are used by IBM and Google. To date, these are the qubits generating the lowest error rate in superconducting qubits. They are divided into at least two categories: qubits with a single Josephson junction (single-junction transmon, used by IBM) or with two Josephson junctions connected in parallel (split transmon, used by Google)<sup>426</sup>.

The first Cooper pair box circuit was made in 1997 in the Quantronics group at CEA Saclay by **Vincent Bouchiat** who characterized its ground state. The first demonstration of quantum coherent superposition with the first excited state was achieved in 1999 by **Yasunobu Nakamura** et al at NEC in Tsukuba, Japan<sup>427</sup>. A first functional qubit version of the Cooper pair box, the quantronium, was demonstrated by the Quantronics team in 2002. The modern version of the Cooper pair box circuit, the transmon, was developed at Yale in 2006. *Below, Daniel Esteve* from the Quantronics team presenting the first operational two-transmon processor in his laboratory.



<sup>424</sup> See [Energy quantization in superconducting nanowires](#), February 2020, referring to [Energy-level quantization and single-photon control of phase slips in  \$\text{YBa}\_2\text{Cu}\_3\text{O}\_{7-x}\$  nanowires](#) by M. Lyatti, February 2020.

<sup>425</sup> See [Charge insensitive qubit design derived from the Cooper pair box](#) by Jens Koch, Jay Gambetta, Alexandre Blais, Michel Devoret, Rob Schoelkopf et al, 2007 (21 pages).

<sup>426</sup> Transmon is a diminutive of "Transmission line shunted plasmon oscillation circuit" created by Rob Schoelkopf, in other words, an oscillator circuit based on shunted Josephson junction. The shunt has become a capacitance that filters low frequencies. A plasmon is the collective behavior of free electrons of metals, here in the form of superconducting Cooper pairs.

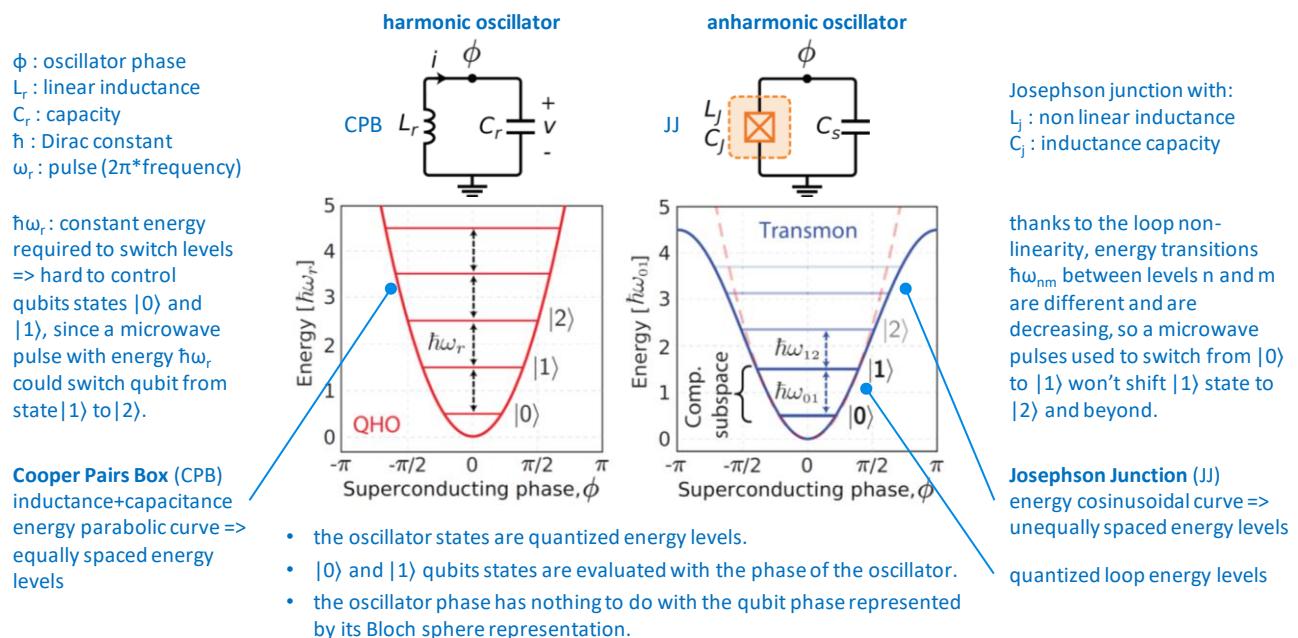
<sup>427</sup> See [Coherent control of macroscopic quantum states in a single-Cooper-pair box](#) by Yasunobu Nalamura et al, Nature, 1999 (8 pages). Published a 1<sup>st</sup> of April but very serious stuff!

At last, **cat-qubits** is a cavity-based qubit connected to a transmon qubit used only for its preparation, readout and/or correction depending on the implementation. The cat-qubit technique was devised by Mazyar Mirrahimi and Zaki Leghtas from Inria around 2013, particularly during their work at Yale with Michel Devoret. It was then adopted by Rob Schoelkopf's team at Yale. Cat-qubits belong to a broad category called bosonic qubits that are resilient to noise or generating less noise and make it possible to assemble logical qubits with much fewer physical qubits, in the 10-100 range instead of 1,000-10,000 range. Besides cat-qubits, let's mention **GKP codes**<sup>428</sup> and the **zero- $\pi$  qubits** of Peter Brooks, Alexei Kitaev and John Preskill which use two Josephson junctions.

The approach is chosen by **Alice&Bob** (France), **QCI** (USA), **Nord Quantique** (Canada) and **Amazon**. It is also investigated in many other research labs like **RIKEN** in Japan<sup>429</sup>.

The **QuCoS** QuantERA collaborative three-year European project is focused on demonstrating the scalability of cat-qubits. It combines the University of Innsbruck (Gerhard Kirchmair), ENS Lyon (Benjamin Huard), Mines ParisTech and ENS Paris (Zaki Leghtas), KIT (Ioan Pop), Inria (Mazyar Mirrahimi), the Romanian National Institute for Research and Development of Isotopic and Molecular Technologies (Luiza Buimaga-Iarinca) and Quantum Machines (Israel).

For what follows, we will focus on those transmon qubits that are the most common, and exploited by IBM, Google and Intel. They are anharmonic and therefore non-linear oscillators. Their non-linearity comes from the Josephson junction which allows to better separate two energy states of the superconducting loop (*on the right in the diagram*) than with a simple linear resonator coupling a capacitor and an inductor (*on the left*)<sup>430</sup>. In a harmonic oscillator, the energy levels are spaced equally and are multiples of the first energy level ( $\hbar\omega_r$  in the diagram).



<sup>428</sup> See [Quantum Error Correction with the GKP Code and Concatenation with Stabilizer Codes](#) by Yang Wang, July 2019 (59 pages).

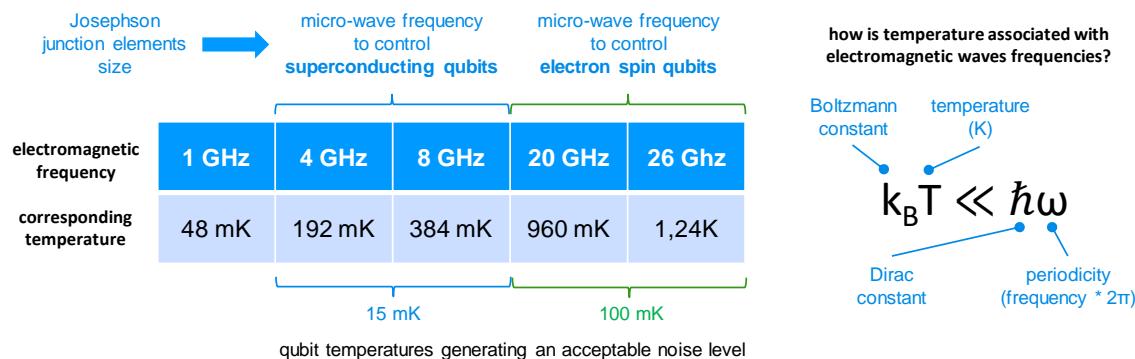
<sup>429</sup> See [Fault-Tolerant Multi-Qubit Geometric Entangling Gates Using Photonic Cat Qubits](#) by Ye-Hong Chen et al, RIKEN, 2021 (12 pages). About a realization of Mølmer-Sørensen multi-qubit cat-qubits gates.

<sup>430</sup> Schematic source: [A Quantum Engineer's Guide to Superconducting Qubits](#) by Philip Krantz et al, 2019 (67 pages), which describes well the sources of noise in superconducting qubits and their control mechanisms, as well as in great detail how microwaves are used to both generate single-qubit and double-qubit quantum gates and with qubits state readouts. The prerequisites for understanding such a paper are numerous: classical physics, quantum physics with Schrödinger equation and Bloch sphere, electrical engineering, superconductivity, electromagnetism, electronics, Boolean logic, signal and microwave processing.

The capacitance has an electrical energy (kinetic) and the inductance has a magnetic energy (potential). With the transmon qubit, the Josephson tunnel junction has a non-linear inductance which creates its anharmonicity. In both cases, the flowing current is quantized with discrete energy levels, the circles in the graph above, with corresponding different current phases.

These oscillators are usually controlled and read by microwaves pulses. These interactions between superconducting qubits and microwave photons are part of a branch of quantum physics called **circuit quantum electrodynamics**, or cQED<sup>431</sup>.

The qubits use a linear superposition of the first two energy levels. They must be well separable from the following ones. This separation is made possible because the (microwave photon) energy sent to move from one level to the other is different from one of these levels to other higher levels. Since the upper levels are less spaced, their related transition energy is lower. As the qubits are activated by microwaves, they are no longer likely to switch to a higher energy level. The anharmonic oscillator in the Josephson loop is provided by a non-linear inductance  $L_j$ . The energy level between  $|0\rangle$  and  $|1\rangle$  of  $\hbar\omega_{01}$  is higher than the energy levels needed to go to the upper levels  $\hbar\omega_{12}$  and  $\hbar\omega_{23}$ .



The  $\hbar\omega_{01}$  energy level is calibrated to correspond to microwave frequencies commonly generated by laboratory electronics in the 4 to 8 GHz band. It is also compatible with the cooling temperature of the processor and the ambient noise. Those of the superconducting qubits control around 5 GHz have an energy level equivalent to a temperature of about 250 mK, much higher than the 15 mK temperature commonly used. The microwaves for silicon qubit control are located around 20 GHz and enable qubit temperatures of 100 mK while some can even reach 1,5K.

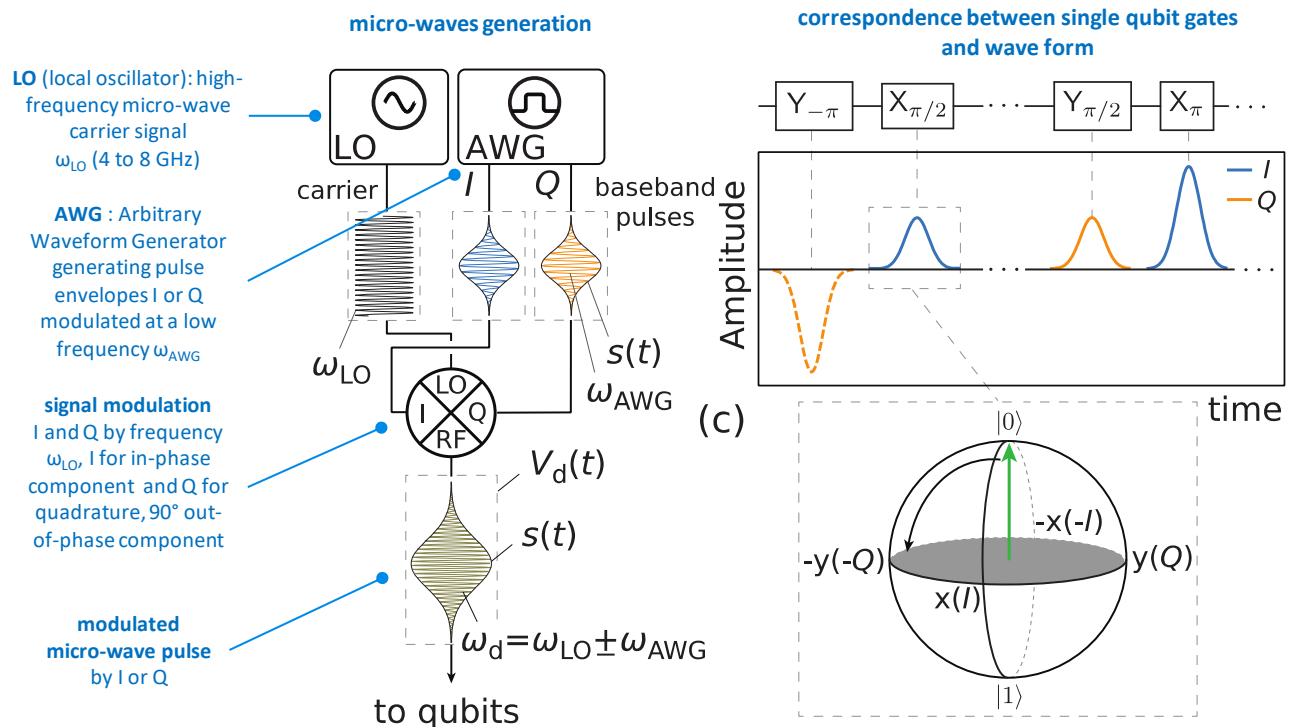
Superconducting qubits quantum gates are generated by microwave pulses sent via coaxial cables on the qubits<sup>432</sup>. Their frequency is adjusted to the energy level  $\hbar\omega_{01}$  mentioned above. This frequency is calibrated to be different on adjacent qubits to avoid crosstalk effects<sup>433</sup>. The axis of rotation of the quantum gate in the Bloch sphere is related to the microwave amplitude modulation. The duration of the pulse will condition the angle of rotation. This makes it possible to create T, S and R gates with a phase other than a quarter or half turn in the Bloch sphere<sup>434</sup>.

<sup>431</sup> See [The Invention of Circuit Quantum Electrodynamics](#) by Agustin Di Paolo, January 2019 which describes the history and fundamentals of QED. The QED was introduced in 2004 by teams from Yale University who were inspired by the work of Serge Haroche, who was awarded the Nobel Prize in Physics in 2012 for his work on the interaction between cold atoms and superconducting cavities. See on this subject the excellent [Circuit Quantum Electrodynamics](#) by Alexandre Blais, Andreas Wallraff et al, May 2020 (82 pages).

<sup>432</sup> Source for the illustrations used in the diagram above: [A Quantum Engineer's Guide to Superconducting Qubits](#), by Philip Krantz et al, 2019 (67 pages).

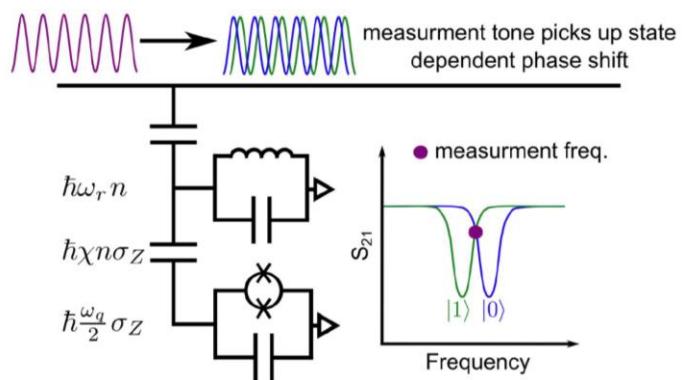
<sup>433</sup> A precise calibration of these frequencies is also necessary because of the variability of the behavior of Josephson loops, which are different from one another due to imprecise manufacturing techniques. This variability does not exist for qubits based on single particles such as trapped ions or cold atoms.

<sup>434</sup> These gates can be optimized by modulating the pulsation in an optimal way. See [Implementing optimal control pulse shaping for improved single-qubit gates](#) by J. M. Chow et al., May 2020 (4 pages) which anticipates the capacity to generate single-qubit gates in 1 ns, against a current minimum of around 20 ns.



Two qubit gates are realized with a coupling circuit positioned between the two qubits, which can be a simple capacitor or a dynamically controllable system. As we will see later, this coupling is managed with an intermediate qubit in Google's Sycamore processor and their Chinese equivalents.

Measuring the state of a superconducting qubit depends on its type. With transmon qubits, a resonator is coupled to the qubit (see an example with the already described [ETH Zurich](#) superconducting circuit). It emits a microwave that is reflected by the qubit, *aka* microwave reflectometry. The qubit state slightly affects the resonator frequency and phase. These readout microwaves are usually amplified in several stages.



One first stage can use a low-noise superconducting Josephson Parametric Amplifier (JPA) or Traveling Wave Parametric Amplifier (TWPA) operating at the quantum limit, then with a high electron mobility transistor (HEMT) amplifier running at the 4K stage and, at last, with a Low Noise Amplifier (LNA) running at room temperature.

At last, the amplified microwave is converted in digital format with an ADC (analog to digital converter) and analyzed by a FPGA circuit to identify the qubit basis states  $|0\rangle$  or  $|1\rangle$  with a microwave phase analysis<sup>435</sup>. Frequency-based multiplexed readout can also be achieved to simplify the wiring exiting the qubit chipset. The readout microwave are modulated with a higher frequency than the quantum gates frequency, between 7 and 8 GHz<sup>436</sup>.

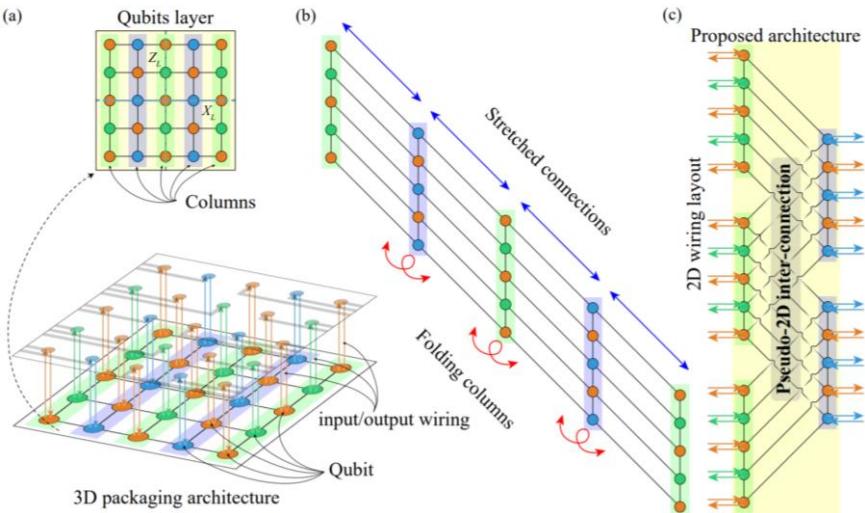
<sup>435</sup> Source of the diagram: [Google's quantum computer and pursuit of quantum supremacy](#) by Ping Yeh, Google Santa Barbara, September 2019 (80 slides).

<sup>436</sup> Other techniques for measuring the state of superconducting qubits are being considered, such as the activation of qubit fluorescence. It is done by jumping from the  $|0\rangle$  to  $|2\rangle$  state of the qubit, the transition to the  $|1\rangle$  state not being possible with the fluorescence excitation photon. See the thesis [Energy and Information in Fluorescence with Superconducting Circuits](#) by Nathanaël Cottet, 2018 (227 pages).

One of the problems to be solved lies in the internal connections in the chipset. A 3D architecture can be created with one layer for qubit readout and another for qubit operations.

The consequence of this topology is to limit the relationship between qubits with their immediate neighbors in a matrix structure.

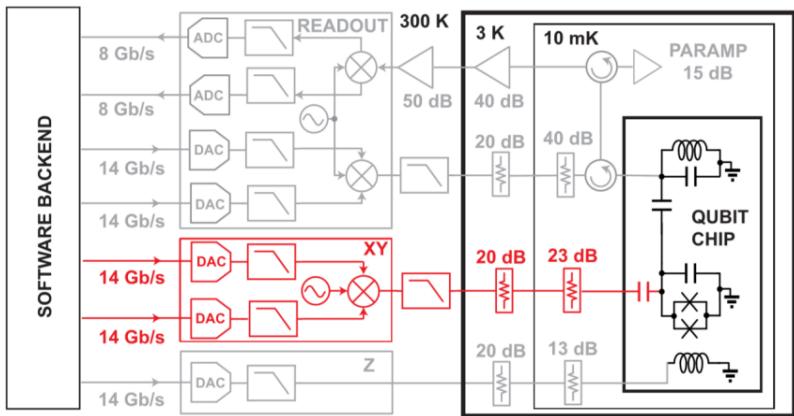
A Japanese team proposed in 2020 an original solution consisting in flattening the matrix and making it possible to connect the control elements in 2D. But at the price of overlapping part of the links between qubits<sup>437</sup>.



In the current state of the art, the cryostats housing these qubits are filled with many cables and microwave attenuators driving the qubits and with first stages amplifiers used in the qubits state readout<sup>438</sup>. Implementing quantum error correction will require 1,000 or 10,000 physical qubits per logical qubit. It will create significant challenges for scaling up the architecture at least, with the existing cabling and external microwave generation and readout systems. Thus the need for cryogenic electronics and miniaturized coaxial cabling that we have already [investigated](#).

Digital-to-analog converters, aka DACs, manage microwaves at room temperature and handle a very large volume of data of 8 to 14 Gbits/s as shown in the diagram *opposite* corresponding to Google's Sycamore.

This data is managed in real time. It does not however seem necessary to store them. It is not a big-data system!



The electronics used in research laboratory equipment is illustrated with the example *below* of a configuration used to test a 5-qubit superconducting chipset in 2015<sup>439</sup>.

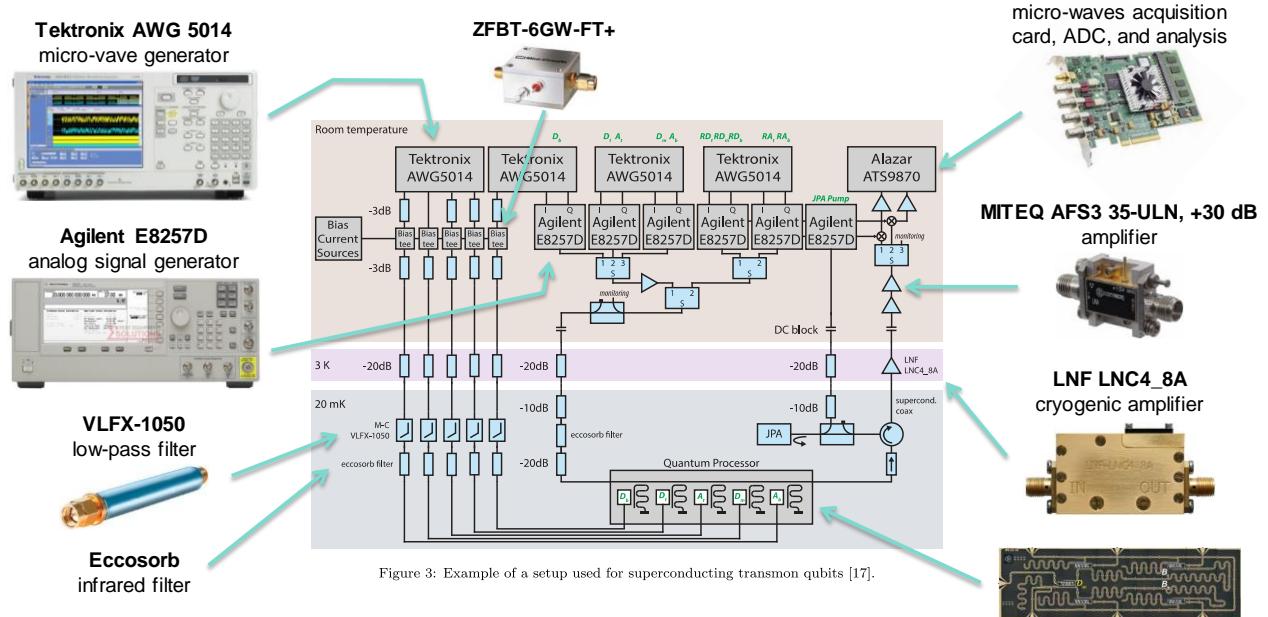
Its uses classical off-the-shelf equipment from **Rohde & Schwarz** or **Tektronix**. These external generators are appreciated for the quality of the microwave pulses they produce. For a larger number of qubits, multiple microwave generators are used from vendors like **Zurich Instruments**, **Qblox** and **Quantum Motion** that we cover in a [dedicated section](#), page 382. Others, like **SeeQC**, are attempting to miniaturize all or part of these components.

<sup>437</sup> See [Wiring the quantum computer of the future: A novel simple build with existing technology](#) by Jaw-Shen Tsai (Japan), April 2020 which points to [Pseudo-2D superconducting quantum computing circuit for the surface code](#) by H. Mukai, February 2019 (8 pages).

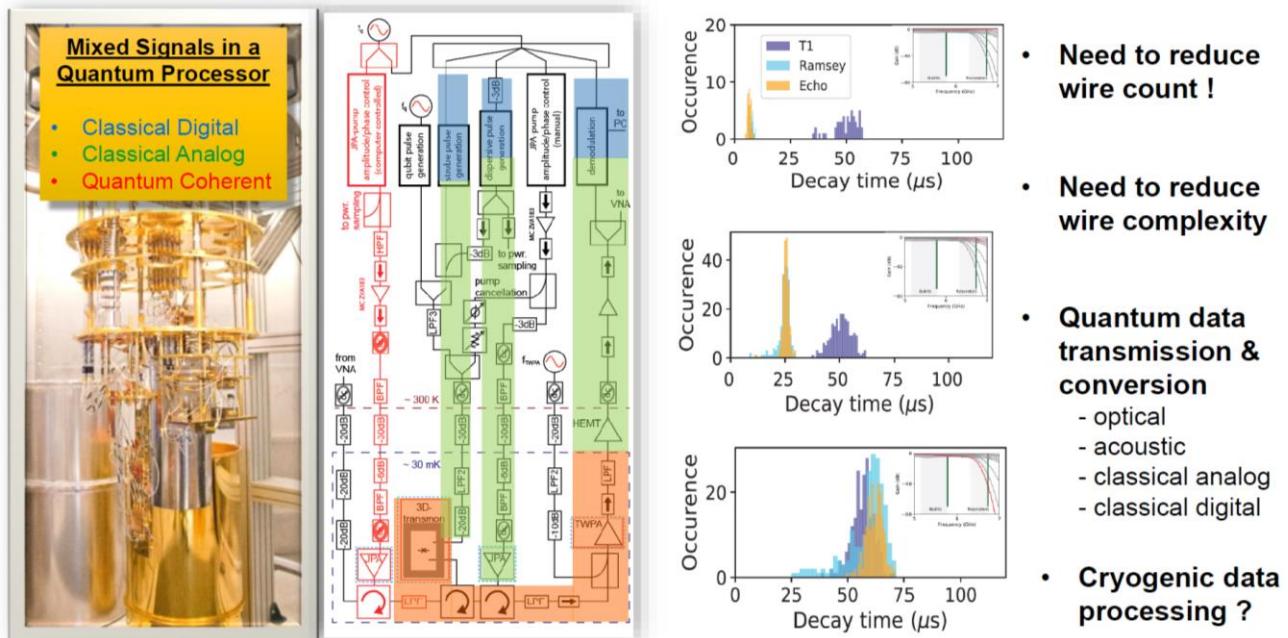
<sup>438</sup> This is well explained in [Superconducting Circuits Balancing Art and Architecture](#) by Irfan Siddiqi of Berkeley Lab, 2019 (34 slides) from which the following diagram on "The tyranny of wires" is extracted.

<sup>439</sup> The schematic comes from [The electronic interface for quantum processors](#) by J.P.G. van Dijk et al, March 2019 (15 pages). I have added visuals of the electronic components used in the configuration.

## 5 superconducting qubits lab configuration



## THE TYRANNY OF WIRES



Superconducting qubits fidelities are not best-in-class compared to trapped ions. It also decreases with the number of qubits. There is some progress being made to reduce qubit noise. It has several origins such as charge fluctuations, random electrons and materials impurities. Fidelity is currently not high enough to implement error correction codes. Some methods are proposed to improve readout fidelity.

A team of Canadian and American researchers is proposing a miniaturizable optical measurement<sup>440</sup>. A variant was proposed in 2018 by Robert McDermott of the University of Wisconsin-Madison, with the objective of improving measurement fidelity to 99%<sup>441</sup>.

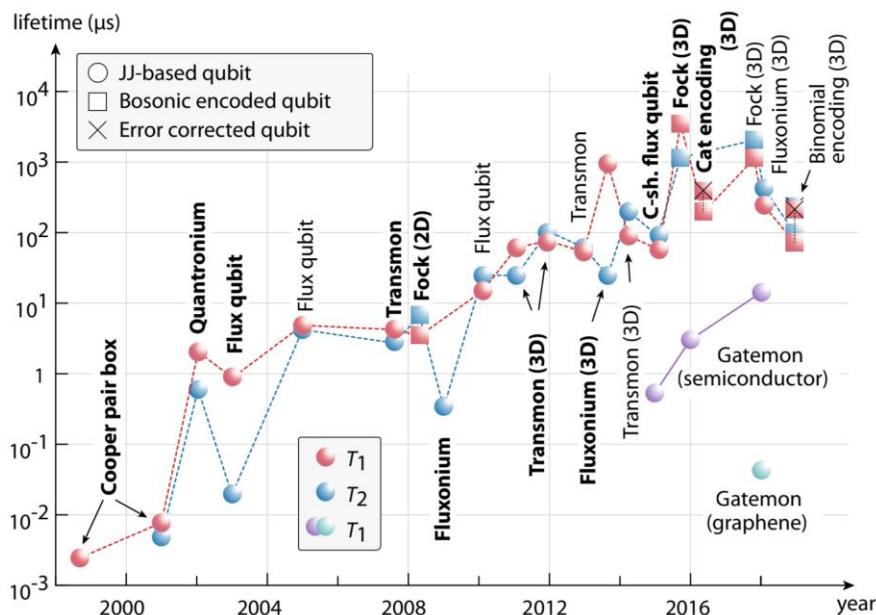
<sup>440</sup> See [Heisenberg-limited qubit readout with two-mode squeezed light](#), 2015 (12 pages).

The size of superconducting qubits is in the micron range, making it difficult to create large chips with millions of qubits. Miniaturization always seems possible but it is difficult to manage because the quality of the superconducting qubits seems to decrease with their size<sup>442</sup>.

A significant number of research laboratories are working on superconducting qubits all over the world. In the USA, at **Yale** and **MIT**<sup>443</sup>, in Europe and in Germany, in Sweden at the **WACQT** of Chalmers University, in France at the **CEA**, in Switzerland at **ETH Zurich**<sup>444</sup>, in Finland<sup>445</sup> and in **Japan**.

The Quantronics team at CEA-Saclay uses transmons for its quantum circuits, but now explores another route based on high coherence impurity spins in insulators for making qubits, with superconducting quantum circuits for controlling them. The rationale is that the electro-nuclear spin levels of such systems may indeed provide more robust qubits for which quantum error correction could be more easily manageable than for transmon qubits.

Other research conducted at the CEA consists in associating superconducting qubits with NV centers, linked by microwaves, to be used as quantum memory as well as a means of more precise readout of superconducting qubits. NV centers spins can serve as quantum memory thanks to a spin coherence time that is 1000 times longer than that of superconducting qubits (100 milliseconds vs. 100 microseconds). Another field of research is the coupling of superconducting qubits with nuclear spins (instead of electron spins, on phosphorus or bismuth nuclei) via electron spins.



<sup>441</sup> In [Measurement of a Superconducting Qubit with a Microwave Photon Counter](#), March 2018 (11 pages).

<sup>442</sup> See [Investigating surface loss effects in superconducting transmon qubits](#) by Jay Gambetta et al, 2016 (5 pages) and [On-chip integrable planar NbN nano SQUID with broad temperature and magnetic-field operation range](#) by Itamar Holzman and Yachin Ivry, Technion, April 2019 (7 pages) who prototyped miniaturized 45 nm x 165 nm SQUIDS.

<sup>443</sup> See [Quantum Computing @ MIT: The Past, Present, and Future of the Second Revolution in Computing](#) by Francisca Vasconcelos, MIT, February 2020 (19 pages). They have developed a 16-qubit superconducting chipset, manufactured by Lincoln Labs at MIT.

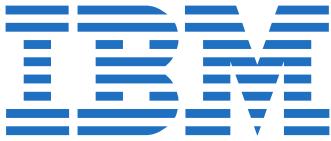
<sup>444</sup> With Andreas Wallraff's QuSurf team working on superconducting qubits and their error correction codes. This project is funded by the American IARPA agency. In 2019, they were at 7 experimental qubits. It is also supported by the ScaleQIT project (Scalable Superconducting Processors for Entangled Quantum Information Technology) funded by the European Union and by the OpenSuperQ project of the European flagship.

<sup>445</sup> VTT's goal is to manage 50 to 100 superconducting qubits. VTT has its own circuit manufacturing unit with a 2600 m<sup>2</sup> clean room of a similar size to CNRS C2V clean room in Palaiseau, France. See [Engineering cryogenic setups for 100-qubit scale superconducting circuit systems](#) by S. Krinner et al, 2019 (29 pages).

Other works aim at lengthening the coherence time of superconducting qubits, notably at Princeton<sup>446</sup>. Indeed, this coherence time of the order of one hundred micro-seconds ( $\mu\text{s}$ ) is still quite limiting<sup>447</sup>. It generates a constraint on the number of quantum gates that can be executed in a quantum software, even if the accumulated errors become prohibitive before this limit threshold. New records were broken in 2021 with 1.6 ms  $T_1$  at Princeton and Sherbrooke with a  $0-\pi$  circuit (but with a 25  $\mu\text{s}$  dephasing time, aka  $T_2$ ) and 210  $\mu\text{s}$  with transmon qubits at Yale<sup>448</sup>. IBM also reached the 1 ms  $T_1$  barrier with one experimental planar transmon qubit in May 2021 (paper pending). The best lab-level record was with a 1.48 ms  $T_2$  coherence time on flux qubits at the University of Maryland in Vladimir Manucharyan's team<sup>449</sup>. These records are however not necessarily obtained with a great number of functional qubits... when more than 2 are used!

Other researchers work on various qubits materials like tantalum on sapphire substrates, at Princeton and ENS Lyon among other locations.

As with many solid-state qubits, one of the key research goals is to transform these microwave photons into photons in the visible/infrared band to allow their long-distance transport, in particular via fiber optic-based telecommunication, which would become the basis of distributed quantum computing<sup>450</sup>.



IBM is one of the few major players in the IT world that has been investing in fundamental research for a very long time<sup>451</sup>. It is one of the most advanced in universal quantum research, having focused on Josephson superconductors for a while.

IBM's efforts are led by researchers in their Yorktown, Poughkeepsie, San Jose and Zurich labs, partnering with various American and other countries universities including ETH Zurich and EPFL in Switzerland.

IBM's choice technology is the fixed frequencies transmon superconducting qubits<sup>452</sup>. Its number of qubits increased from 5 in 2016 to 65 qubits in 2020 and 127 in 2021. IBM's quantum systems have been proposed in the cloud since 2016. These are already used by thousands of researchers, students, startups and corporations around the world.

After creating laboratory computers, IBM ventured into creating packaged ones when announcing the Q System One in January 2019 at the Las Vegas CES. It was a 20 qubits system. Its main innovation was its design. It was created with the design studios Map Project Office and **Universal Design Studio** (UK) and **Goppion** (Italy), a manufacturer of high-end exhibition devices for museums, which notably designed the protective device for the Mona Lisa in the Louvre Museum and the Queen's jewels in the Tower of London.

<sup>446</sup> See [New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds](#) by Alex P. M. Place et al, February 2020 (37 pages). Qubits are using tantalum.

<sup>447</sup> Schema source: [Superconducting Qubits Current State of Play](#) by Morten Kjaergaard et al, 2020 (30 pages).

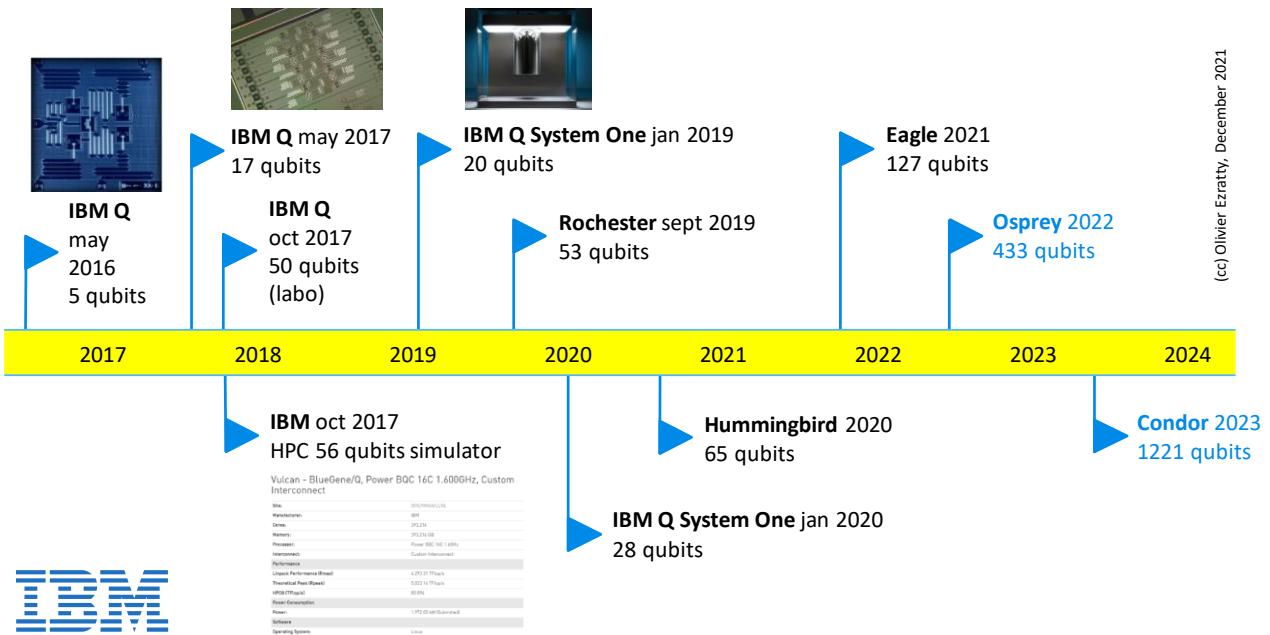
<sup>448</sup> See [Experimental Realization of a Protected Superconducting Circuit Derived from the 0– \$\pi\$  Qubit](#) by András Gyenis, Alexandre Blais et al, Sherbrooke, Princeton, U. Chicago and Northwestern University, March 2021 (31 pages) and [Direct Dispersive Monitoring of Charge Parity in Offset-Charge-Sensitive Transmons](#) by K Serniak, R Schoelkopf, Michel Devoret et al, Yale, March 2019 (11 pages) with transmons at a  $T_1$  of 210  $\mu\text{s}$ .

<sup>449</sup> See [Millisecond coherence in a superconducting qubit](#) by Aaron Somoroff, Vladimir E. Manucharyan et al, University of Maryland, 2021 (14 pages),

<sup>450</sup> See for example [Microwave-to-optical conversion via four-wave mixing in a cold ytterbium together](#) by Jacob P. Covey et al, July 2019 which discusses this conversion.

<sup>451</sup> Who does fundamental research? Mainly IBM, Microsoft, Google and large telecom companies. The Bell Labs coming from the dismantling of AT&T in 1982 are now part of Nokia after gone through Lucent and Alcatel-Lucent.

<sup>452</sup> Schema source: [Quantum Computing with superconducting qubits: Applications in Chemistry and Physics](#) by Ivano Tavernelli, IBM Research, February 2019 (58 slides).



(cc) Olivier Ezratty, December 2021

The system is 2.75 m wide, about the size of a D-Wave. These machines are still useless. The algorithms they can run can be emulated on a simple laptop with a much better response time and lower cost of ownership. For such quantum computers to be usable in industry grade applications, it would require thousands or even millions of physical qubits with a much better fidelity.

Below on the right, you can see the Q System assembly workshop. IBM is implementing a pre-industrial approach to the production of its quantum computers, despite their very limited capacities and low volume economics.



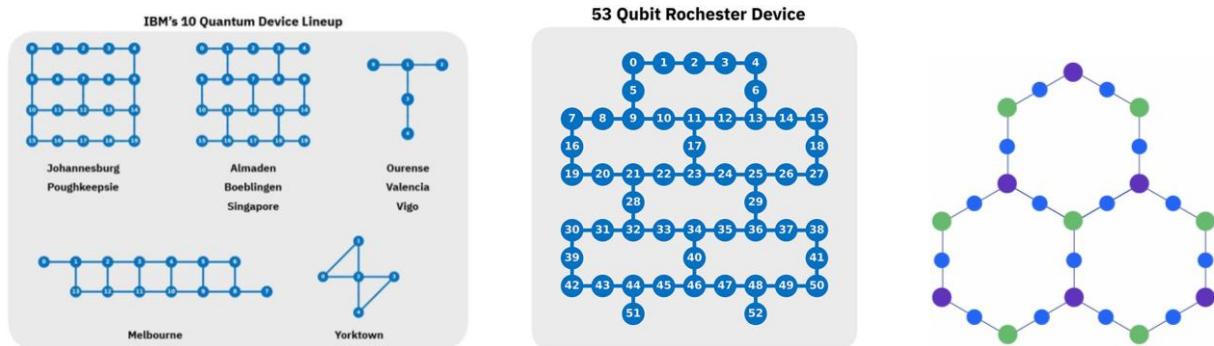
Most of these units are sitting in IBM's own data center in Poughkeepsie, with two extra systems sitting in IBM sites in Germany and Japan, plus one planned in Korea at Yonsei University. The casing front contains the suspended cryostat while the back contains all the computing, electronics and cryostat compressor and pumps. The Q Systems are also self-calibrating. IBM is continuously improving these systems and updating the related qubits lifetime and gates fidelities data on their Q Experience web site. See their best fidelities presented in the chart in page 203.

Otherwise, the different IBM quantum computers available to developers in the cloud do not have the same qubit connectivity<sup>453</sup>.

<sup>453</sup> Seen on [Quantum computation center opens](#) by Doug McClure, 2019.

This impacts the type and performance of the quantum algorithms that can be executed. Worth mentioning, the rectangles in the chart below are hexagons on the chipset physical layout.

In July 2021, IBM announced a generalization of this hexagon qubits topology, incorporated in their Falcon processors systems deployed in Germany and Japan since 2021. This heavy-hex lattice is the 4<sup>th</sup> version of IBM Quantum systems qubits topology and is used in Falcon (27 qubits) and Hummingbird (65 qubits) processors<sup>454</sup>. It uses a hexagonal arrangement with an intermediate qubit on each side of hexagons. The topology is optimized for quantum errors correction, using custom hybrid surface and Bacon-Shor subsystem codes. This topology is different from the square lattice chosen by Google in its Sycamore processors, which, however, uses coupling qubits, a solution that IBM is not relying on. IBM is using fixed frequency qubits when Google uses tunable frequency ones. The hex lattice reduces the effect of frequency collision between qubits.



In September 2020, IBM announced their plan to scale up the number of qubits of their quantum computers<sup>455</sup> with a 127 qubits version ("Eagle") introduced in November 2021, 433 qubits planned in 2022 ("Osprey") and 1221 qubits in 2023 ("Condor"). There is some inconsistency with IBM's roadmap. They expect to more than double the number of qubits in their system while announcing they will double the related available quantum volume every year. This means adding one operational qubit per year. Houston, we have a problem!

Their qubits quality and scaling improvements efforts are manyfold:

- Improving qubit readouts fidelity with using use low noise amplifiers (QLA for quantum-limited amplifiers)<sup>456</sup>.
- Microwaves signals multiplexing and intelligent filtering for qubit states readouts (starting with Hummingbird 65 qubits system in 2020).
- Stacked pairs of chipsets separating qubits from microwave controls, using TSV (through-silicon vias) starting with their 127 qubit systems in 2021<sup>457</sup>.
- Using microwave flexible cable to reduce the space used by microwave cabling in cryostats.
- Using tunable couplers to control qubits entanglement<sup>458</sup>.
- Using laser annealing of transmon qubits<sup>459</sup>.

<sup>454</sup> See [The IBM Quantum heavy hex lattice](#) by Paul Nation et al, IBM Research, July 2021.

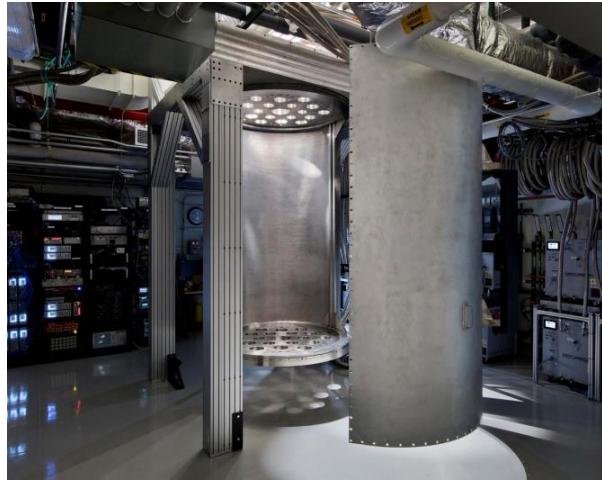
<sup>455</sup> See [IBM's Roadmap For Scaling Quantum Technology](#) by Jay Gambetta, September 2020, completed by [IBM publishes its quantum roadmap, says it will have a 1,000-qubit machine in 2023](#) by Frederic Lardinois in TechCrunch. See also [IBM Envisions the Road to Quantum Computing Like an Apollo Mission](#) by Dexter Johnson, September 2020.

<sup>456</sup> See [Rising above the noise: quantum-limited amplifiers empower the readout of IBM Quantum systems](#) by Baleegh Abdo, January 2020.

<sup>457</sup> See [Merged-Element Transmons: Design and Qubit Performance](#) by H. J. Mamin et al, March 2021 (7 pages).

<sup>458</sup> See [Tunable Coupling Architecture for Fixed-frequency Transmons](#) by J. Stehlik et al, IBM Research, February 2021 (7 pages).

- Speeding up quantum gates and improving qubits connectivity.
- Increasing coherence times, on a regular basis within a class of systems processors (like Falcon for 27 qubits)<sup>460</sup>. Their record is a T1 of 0.3 ms with their Falcon R8 processor and 0.6 ms in research.
- New materials design improving their purity and avoiding contaminations and computer aided design<sup>461</sup>.
- Improving the chipset vacuum isolation during its assembly<sup>462</sup>.
- Optimizing their quantum error correction architecture<sup>463</sup>.
- IBM announced in 2020 that it was working on a giant home-made cryostat called "Goldeneye" exceeding current market capacity, to host from a thousand to a million physical qubits<sup>464</sup>.



- Scale-out plans with interconnecting quantum computers processing units using optical channels with SiGe/Si optical resonators<sup>465</sup>. These quantum units will be cooled with a new generation of cryostats, designed by Bluefors as part of their KIDE range using an hexagonal form factor, announced in November 2021. It seems it is replacing Goldeneye in their plan. IBM will start to implement this System Two modular architecture with their 1121 qubits systems in 2023.
- Other longer-term plans consist in using constant depth circuits using entanglement and measurements ala “one way quantum computing” and MBQC that is also to be used with flying qubits like photons.

<sup>459</sup> See [High-fidelity superconducting quantum processors via laser-annealing of transmon qubits](#) by Eric J. Zhang et al, December 2020 (9 pages).

<sup>460</sup> T<sub>1</sub> and T<sub>2</sub> reached about 260 μs in September 2021 with their [Peekskill](#) 27 qubit system. It was a 3 times improvement vs previous systems.

<sup>461</sup> See [What if We Had a Computer-Aided Design Program for Quantum Computers?](#), IBM, October 2020 and [Qiskit Metal: IBM Community Building a Computer-Aided Program for Quantum Device Design](#) by Matt Swayne, October 2020.

<sup>462</sup> See [Ultrahigh Vacuum Packaging and Surface Cleaning for Quantum Devices](#) by M. Mergenthaler et al, 2020 (6 pages).

<sup>463</sup> Their views on QEC: [Hardware-aware approach for fault-tolerant quantum computation](#) by Guanyu Zhu, 2020.

<sup>464</sup> The device is 3m high and 2m wide. We can infer from the circular perforated plates visible in the pictures that they are about to use about 18 cryogenic pulse tubes, provided the holes are not used to pass large chunks of cables. IBM announced that it was considering sourcing technologies externally rather than creating everything in-house. IBM says that Goldeneye will have ten times the cooling power of existing cryostats at 100mK and eight times at 4K.

<sup>465</sup> See [Engineering electro-optics in SiGe/Si waveguides for quantum transduction](#) by Jason Orcutt et al, Quantum Science Technology, 2020.

IBM has been investing a lot since 2016 to build a community of developers and users worldwide. They launched the IBM Q network in 2017. It brings together major Fortune 500 companies, research laboratories and startups interested in developing quantum solutions. This network offers access free access to quantum systems with one (crowded) 15 bits system, 8 5-bit systems and a 1-bit small-use system. Commercial systems have respectively 5, 27, 28, 53 and 65 qubits. At last, a quantum emulator (branded a simulator) supports 32 qubits.

IBM also launched a customer Q Quantum Computation Center in Poughkeepsie, New York, a quantum center in Montpellier, France, in 2018, and then a partnership in Germany with a Fraunhofer Institute in 2019. Their task is to evangelize developers and researchers to encourage them to develop software on their Qiskit platform and their quantum systems sitting in the cloud.

IBM publishes amazing data on their developer community activity with over 325,000 developers who would have executed the impressive number of 790 billion circuits, according to data from June 2020. That's 2,43 million circuits per person. On average, quantum code is executed 4,000 times to obtain an average result. That makes an average 607 quantum gates that were executed per user. Taking into account tests and errors, it doesn't look like these are large code loads. It's more or less a quantum equivalent of a "Hello World". IBM also touts that over 235 scientific publications are mentioning the use of their quantum systems and the number is obviously constantly growing.

At last, we should mention the quantum volume benchmark created by IBM in 2017 and updated in 2019. We cover it in details in the [section dedicated to benchmarks](#), page 528.

In April 2021, IBM finalized the deployment of a 28-qubit Q System in its own site near Stuttgart, Germany, in relationship with Fraunhofer as an intermediate to reach out the developer community<sup>466</sup>. It was even inaugurated remotely by Chancellor Angela Merkel on June 15<sup>th</sup>, 2021.

IBM also announced a partnership of 10 years with Cleveland Clinic in the USA, including the delivery of their 1,121 qubits system around 2024. Meanwhile, the customer will rely on the existing cloud-based Q Experience systems<sup>467</sup>. Then, in June 2021, IBM announced a five years \$300M artificial intelligence and quantum computing research partnership with the UK. They plan to hire 60 scientists as part of the new Hartree National Centre for Digital Innovation (HNCDI)<sup>468</sup>.

IBM has however not put all its eggs in the superconducting qubits basket. Their Zurich research center is also investigating electron spins and Majorana fermions qubits at a fundamental research level, working on this with ETH Zurich and EPFL.



Google started to invest early on in quantum computing, in the early 2010s. It began by testing algorithms on a **D-Wave** quantum annealing system installed in the joint QUAIL laboratory established with NASA and located at the Ames Research Center in Mountain View.

It then started to launch a research program to build their own superconducting qubits quantum system, under the direction of Hartmut Neven. Hardware was developed by John Martinis's team between 2014 and 2020. All this was done in connection with the University of Santa Barbara in California (UCSB), where he came from with part of his team. Google initially wanted to create its own quantum annealer.

That's why John Martinis was hired for but he and Google quickly switched gear towards gate-based superconducting technology with the goal to become the first company to obtain a "quantum supremacy".

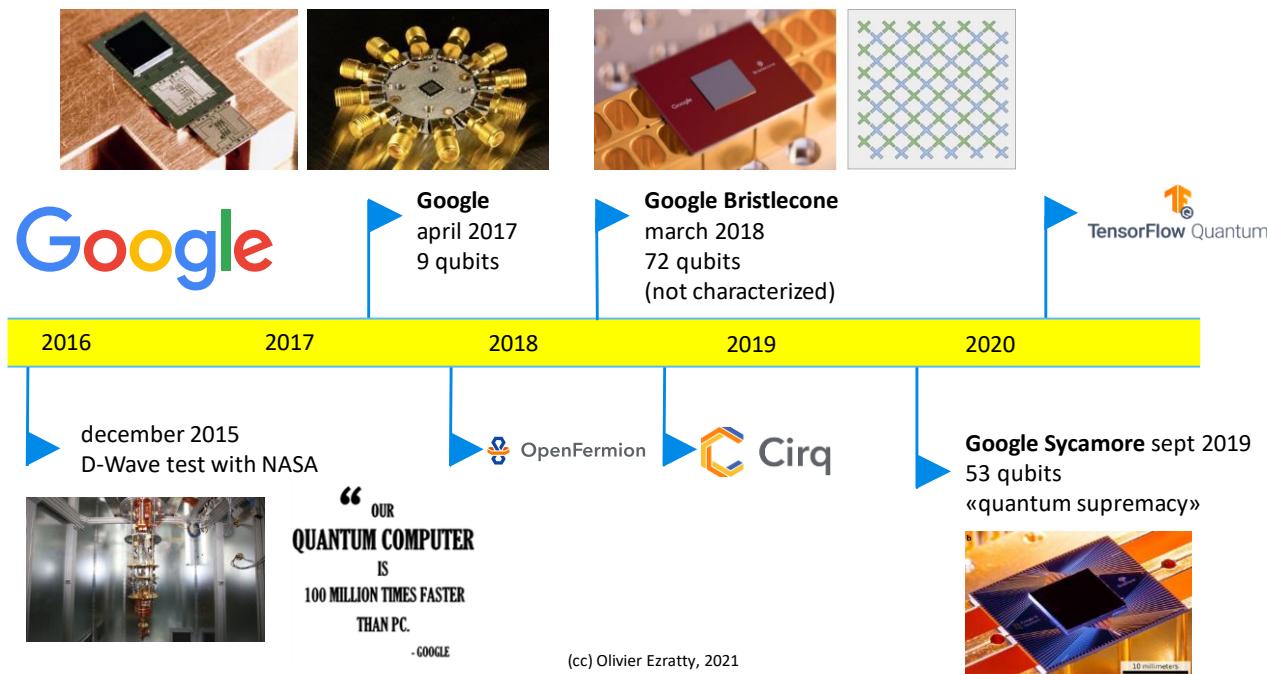
---

<sup>466</sup> See [Fraunhofer launches quantum computing research platform in Germany](#), April 2021.

<sup>467</sup> See [Cleveland Clinic, IBM launch 10-year quantum computing partnership](#) by Mike Miliard, March 2021.

<sup>468</sup> See [UK STFC Hartree Centre and IBM Begin Five-Year, £210 Million Partnership to Accelerate Discovery and Innovation with AI and Quantum Computing](#), June 2021.

On top of hardware developments leading to the famous October 2019 so-called quantum supremacy with their 53-qubits Sycamore processor, they created a quantum software platform around the Cirq framework and TensorFlow Quantum for quantum machine learning applications. At last, Google also has a cloud offering for quantum algorithm simulation.



We'll cover here their hardware ventures. Like IBM, Google is investing a lot to increase the number and quality of its qubits.

As early as 2017, Google stated its ambition to obtain some quantum supremacy as defined by John Preskill in 2011<sup>469</sup>. In April 2017, they had prototyped a first 9 qubits chipset. They announced June 2017 that they wanted to reach 49 stable qubits.

At the beginning of 2018, their Foxtail 22 qubits chipset was tested, but in quiet way. Then came in March 2018 the announcement of a record 72 qubits with their Bristlecone generation, promising a two-qubits gates fidelity of 99,56%. It was not confirmed by any verifiable scientific publication.

Google's quantum project is driven since 2006 by **Hartmut Neven**, who manages hardware and software. In 2019, he put forward an empirical law called Dowling-Neven according to which the power of computers doubles exponentially.

This was exaggerated when you look at their evaluation method<sup>470</sup>!

<sup>469</sup> See [Google says it is on track to definitively prove it has a quantum computer in a few months' time](#) by Tom Simonite, April 2017. See also [The Question of Quantum Supremacy](#), May 2018 which references two related papers : [Characterizing Quantum Supremacy in Near-Term Devices](#), 2016 (23 pages) and [A blueprint for demonstrating quantum supremacy with superconducting qubits](#), 2017 (22 pages).

<sup>470</sup> The reasoning is as follows: the number of qubits would so far increase exponentially, and the power doubles with each addition of a single qubit. All this every six months. Unfortunately, the available data on the actual power of today's quantum computers does not comply with this law. There is no doubling of the number of operational qubits every six months! There is even regression! Google announced 72 qubits in March 2018 and then 53 qubits in October 2019. At IBM, we are in the total confusion between the Q System One which went from 20 to 28 qubits between January 2019 and January 2020, which does not look like a doubling every six months. On the other hand, this doubling could eventually be achieved with other technologies such as Honeywell's trapped ions or Pasqal's cold atoms. In his presentation at Q2B in December 2019, John Preskill highlighted another exponential doubling: gate fidelity rates are steadily improving, which would increase quantum volume exponentially. At the same time, the cost of emulating quantum computing on conventional computers increases exponentially with quantum volume. Hence a doubly exponential evolution of computing power. The bug? Nothing says that the fidelity of quantum gates will continue to improve steadily. See [A New Law to Describe Quantum Computing's Rise?](#), June 2019.

Finally, in October 2019, Google announced its quantum supremacy with their Sycamore 53-qubit chipset, and with a random algorithm similar to the boson sampling algorithm imagined by Scott Aaronson in 2012<sup>471</sup>.

NASA and Google science papers were mistakenly posted on the Internet in September 2019 and then officially published in the journal Nature in October 2019<sup>472</sup>, filing 70 pages with a level of detail never seen before<sup>473</sup>. Google compared their qubits with the most powerful supercomputer of the time, the IBM Summit installed at the Department of Energy's Oak Ridge National Laboratory in Tennessee<sup>474</sup>. Computing for 200 seconds on Sycamore would take 10,000 years once emulated on the IBM Summit. This comparison didn't make much sense as we discuss quantum supremacy and advantages in [another part](#) of this ebook (page 533).

The algorithm combined a set of random quantum gates with a homogeneous distribution. This last part scans all the possible values ( $2^{53}$ ) of qubits superpositions<sup>475</sup>.



It had several characteristics that explained its choice:

- It uses **superposition on all the qubits** (53), allowing maximum performance. Usually, ancilla qubits are necessary to make some calculation. Ancilla qubits are used as buffer values. As a result, the exponential advantage decreases accordingly. Typical algorithms don't benefit from the superposition of  $2^{53}$  states but, for example, a lesser  $2^{30}$  or  $2^{40}$  states. Any quantum advantage would then vanish.
- It uses a small **20 quantum gates computing depth**. Namely, the algorithm tested at full load only chains 20 sequences of quantum gates executed simultaneously. This is related to the noise generated in the qubits which limits this depth. Many algorithms require a larger number of quantum gates, such as Shor's integer factorization.

---

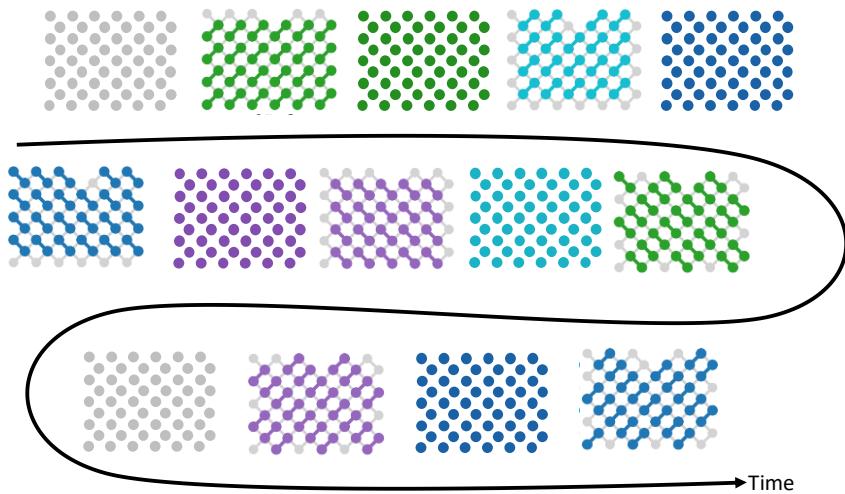
<sup>471</sup> See [Quantum Supremacy Using a Programmable Superconducting Processor](#) by John Martinis, October 2019.

<sup>472</sup> See [Hello quantum world! Google publishes landmark quantum supremacy claim](#) by Elizabeth Gibney, October 2019.

<sup>473</sup> See "[Quantum supremacy using a programmable superconducting processor](#)" by Frank Arute, John Martinis et al, October 2019 (12 pages) and [Supplementary information for "Quantum supremacy using a programmable superconducting processor"](#) by Frank Arute, John Martinis et al, October 2019 (58 pages). See also [Quantum supremacy using a programmable superconducting processor](#), a lecture by John Martinis at Caltech, November 2019 (one hour). And [another version](#), played at QC Ware's Q2B conference in December 2019 (19 slides and 32-minute [video](#)). At last, here is this video promoting Google's supremacy: [Demonstrating Quantum Supremacy](#), October 2019 (4'42").

<sup>474</sup> See [Google researchers have reportedly achieved "quantum supremacy"](#) by Martin Giles, in the MIT Technology Review, September 2019 and the [source](#) of the paper on the Internet, with illustrations. They use a type of algorithm that is of little use, but which clearly favors quantum computing and requires a limited number of quantum gates, which is good for noise-generating quantum processors. See also [Why I Coined the Term 'Quantum Supremacy'](#) by John Preskill, October 2019.

<sup>475</sup> The following explanation can be found in Kevin Harnett's [Quantum Supremacy Is Coming: Here's What You Should Know](#) in Quanta Magazine, July 2019.



Nevertheless, a large number of useful algorithms can be executed with this gate depth. This opens doors to practical uses such as in chemical simulation.

- The algorithm does use any **error correction code** that consumes many quantum gates as well as a number of qubits several orders of magnitude higher (x100 to x10000).
- They used a convoluted **cross entropy benchmarking** (XEB) to calibrate their circuits and estimate the fidelity of their one- and two-qubits gates. In the supremacy regime, the so-called computation has a 0,2% chance to produce right results. It is executed 3 million times to generate an average measurement mitigating this low fidelity<sup>476</sup>! Understanding all the data from the Google experiments is not that easy and prone to many good and bad interpretations.

On October 21, 2019, IBM researchers published an article in which they questioned Google's performance, stating that they could run their algorithm in 2.5 days instead of 10,000 years on the IBM Summit supercomputer<sup>477</sup>.

This would require adding 64 PB of SSD to the supercomputer, which they had not tested. That's about 7 racks full of SSDs at 2019 capacity. IBM wanted to contradict Google's claim of quantum supremacy, which they turned into some sort of quantum advantage<sup>478</sup>.

On top of that, randomized benchmarking used in Google's experiment is an approach that is not unanimously accepted to establish the superiority of quantum computing over classical computing<sup>479</sup>.

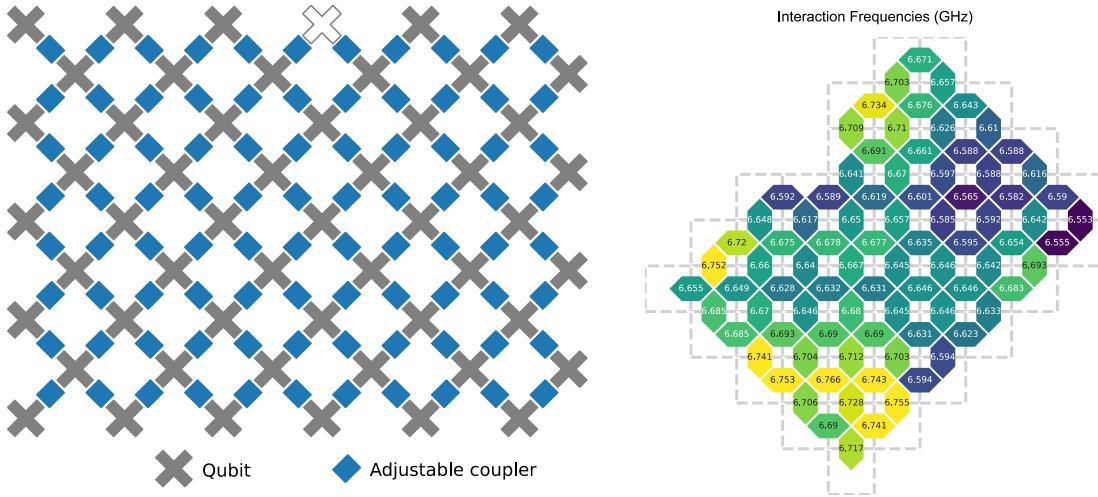
---

<sup>476</sup> See [The Google Quantum Supremacy Demo and the Jerusalem HQCA debate](#) by Gil Kalai, December 2019, where he questions the results of Google's quantum supremacy, particularly its evaluation of qubit noise at large scale.

<sup>477</sup> See [On "Quantum Supremacy" | IBM Research Blog](#) by Edwin Pednault, October 2019 and [Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits](#) by Edwin Pednault et al, October 2019 (30 pages).

<sup>478</sup> Google's quantum supremacy quibbles have gone a long way, including IBM's response. And then [Has Google Finally Achieved Quantum Supremacy?](#), October 2019, which is quite well documented. Then [Quantum supremacy: the gloves are off](#) by Scott Aaronson, October 2019 where he discusses the fact that this case is the equivalent of Kasparov vs. Deep Blue, with IBM playing the role of Kasparov. Not to mention the debate on supremacy terminology that has once again generated a lot of fuss, as reported in [Academics derided for claiming 'quantum supremacy' is a racist and colonialist term](#) by Sarah Knapton, December 2019.

<sup>479</sup> See [Lecture 3: Boson sampling](#) by Fabio Sciarrino (63 slides) and [An introduction to boson-sampling](#) by Bryan Gard, Jonathan P. Dowling et al, 2014 (13 pages). See the review [Quantum computers: amazing progress \(Google & IBM\), and extraordinary but probably false supremacy claims \(Google\)](#) by Gil Kalai, September 2019 as well as [The Quest for Quantum Computational Supremacy](#) by Scott Aaronson, September 2019, which was published three weeks before Google's announcement but was still valid (16 pages).



Still, let's have a look at Sycamore's architecture. First, with some key data from this benchmark and then, with some specifics.

Metric	Value	Unit	Comments
Number of qubits	53	qubits	Computing qubits
Couplers	86	couplers	Qubits used for coupling computing qubits
Single qubits gates	1,113	gates	Number of single qubit gates executed in benchmark
Single qubits gates duration	25	nano-seconds	Duration of a single qubit gate
Single qubit error	0,16%	percent	
Two qubits gates	430	gates	Number of two qubits gates executed in benchmark
Two qubits gates duration	12	nano-seconds	Duration of a two qubit gate
Two qubits gates error	0,93%	percent	
Readout error	3,80%	percent	
Gates depth	20	cycles	Number of series of quantum gates executed.
Gates per cycle	55,65	gates/cycle	Number of quantum gates executed per cycle
Measured fidelity	0,20%	percent	Total fidelity of system in supremacy regime
Number of iterations	3,000,000	iterations	Number of full algorithm executions
Computing time	6,000	seconds	Total computing time
Quantum computing time	30	seconds	Total quantum computing time
Readout analog to digital convertors	277	number	Generating 8 bits at 1 GB/s

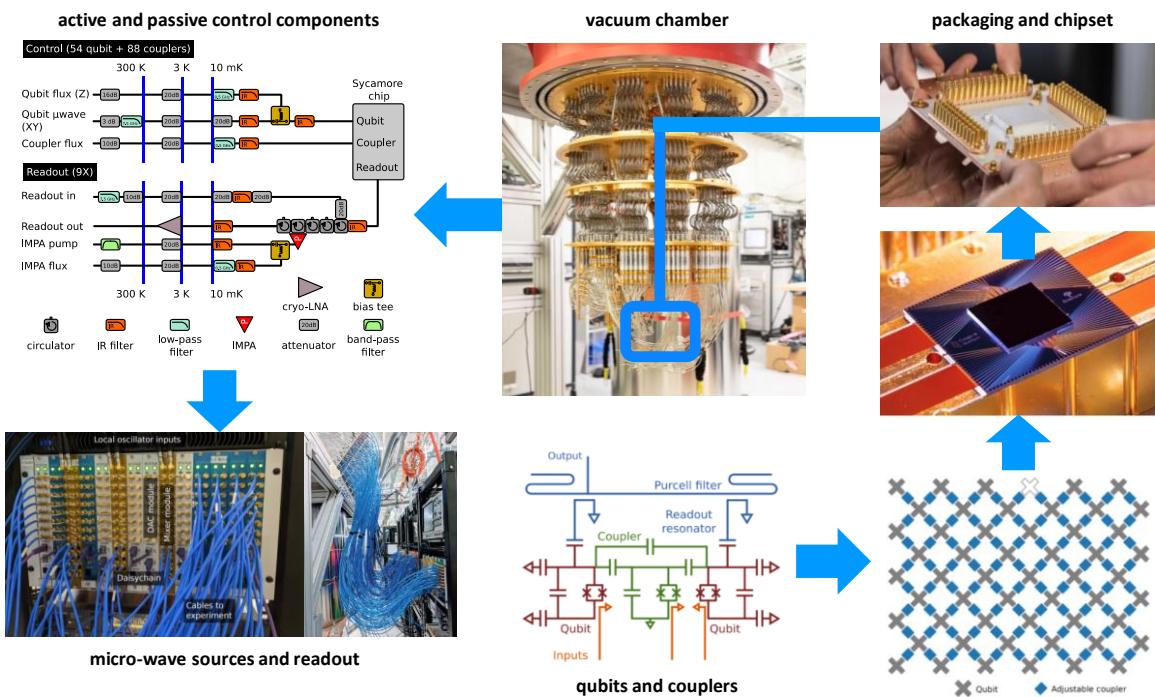
**Coupling qubits:** Sycamore uses controllable qubit couplers. There are 86 of them in all, connecting the 53 qubits of the chipset. This makes a total of 139 qubits. These couplers are in fact qubits whose frequency is controlled by a direct current line (DC). It allows the implementation of two qubits quantum gates, acting in an average 12 ns.

**Machine learning based calibration:** these qubits and couplers are controlled with microwaves carried in coaxial cables, at frequencies between 5 and 7 GHz, adjusted by a DC flux line. Google developed a deep learning based qubit calibration code, which has made it possible to refine the qubit microwaves activation frequencies to avoid crosstalk between neighboring qubits.

**Isolation:** the qubit chipset is protected by some Mu-metal shielding, another one in aluminum and a black coating to absorb infrared photons. The processor is made of aluminum and indium on silicon and includes two dies stacked on top of each other or next to the other. This is not precised.

**Microwave generation:** below is a set of schematics of the control electronics inside and outside the cryostat. The system uses 54 external microwave signal generators for the single-qubit gates (X and Y), 54 for qubit frequency control and 86 for qubit control. This is completed by 9 microwave control signals. The control electronics package includes 277 digital-to-analog converters that occupy 14 6U rack-mount cases. There is a similar number of coaxial cables ending in the cryostat.

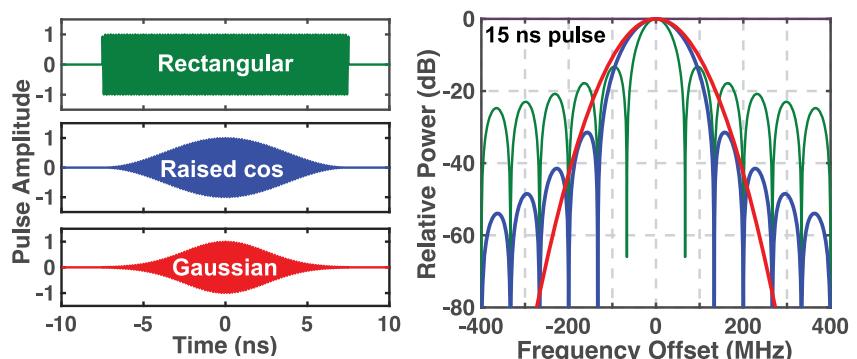
**Z gates:** DC flux lines are also used to create Z gates, or phase gates. They are controlled with microwaves in IBM's superconducting qubits. Using DC flux lines is reducing the phase error observed with these gates.



**Qubit readouts:** is done with only a few microwave photons sent to the qubits. The result is amplified by 100 db in several steps, one at the 15 mK processor stage and another at the 3K stage. The resulting amplified microwaves are converted digitally by an ADC and analyzed by a FPGA to detect their phase. The system multiplexes in the frequency domain the readout microwaves of 6 qubits groups conveyed by a single cable, between 5 and 7 GHz.

**Cryo-CMOS:** to scale up micro-waves generation and put it inside the cryostat, Google is working on the creation of some CMOS chipsets operating at 3K<sup>480</sup>. These chipsets use very simple waveform generators consuming a minimum of energy. It has however not yet been deployed.

Google uses microwaves of cosinusoidal shape with the interest of creating spectral "holes" corresponding to the qubits frequencies harmonics of the state  $|1\rangle$  to the state  $|2\rangle$  transition, that must be avoided<sup>481</sup>. It corresponds to the wavelength known as  $\omega_{12}$  as seen in the illustration from page 255.



**Raised cosine: good compromise between sidelobes and pulse duration**

<sup>480</sup> See [Control of transmon qubits using a cryogenic CMOS integrated circuit](#) by Joseph Bardin, March 2020 (35 minutes) and [A 28nm Bulk-CMOS 4-to-8GHz <2mW Cryogenic Pulse Modulator for Scalable Quantum Computing](#), February 2019 (13 pages).

<sup>481</sup> Illustration source: [XY Controls of Transmon Qubits](#) by Joseph Bardin, June 2019 (36 slides).

**Energetic advantage:** Sycamore showcases some energy consumption advantage, with a ratio of about one to a million. Its power consumption is about 25 kW and IBM Summit is at 12 MW at full charge, and the computing time ratio is 2.5 minutes vs. 2.5 days (1/1440) in the most favorable IBM Summit case. But we are probably comparing apples and oranges.

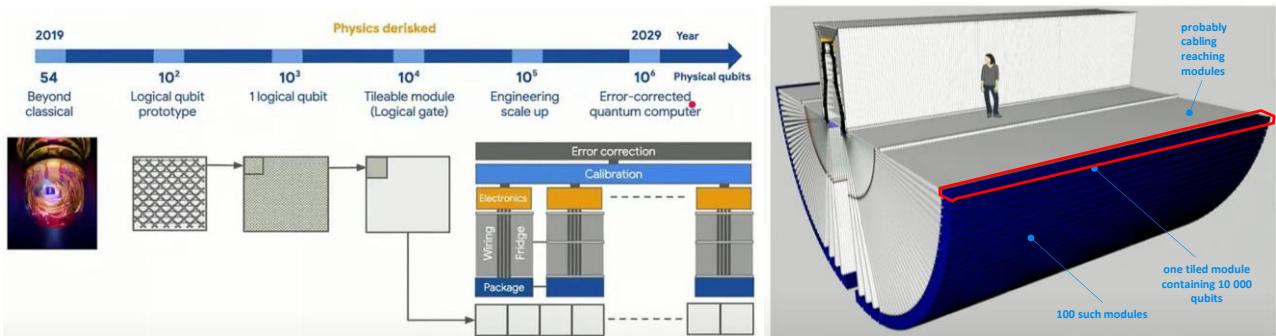
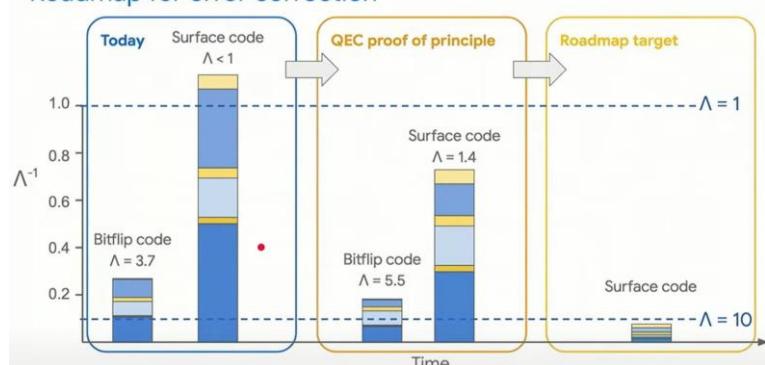
**Useful applications:** Google's teams published two papers in April 2020, one on solving combinatorial problems and the other on the chemical simulation of a molecule of four atoms.

This time, without mentioning the notion of supremacy<sup>482</sup>! Which makes sense given they didn't use more than 15 qubits to solve these small-scale problems. Other same scale algorithms were published in 2020<sup>483</sup>. Several Google teams are working on quantum software, including those working on Cirq, on TensorFlow Quantum and another Google X team working on applications, under the leadership of Jack Hidary<sup>484</sup>.

**Resignation:** John Martinis left Google in April 2020<sup>485</sup>. He explained this in an exit interview. We discover there the role of wiring in the cryostat, a member of the hardware team wanting to follow up on a lead he found unproductive but which was nevertheless approved by Hartmut Neven<sup>486</sup>.

**Next steps:** Google wants to reduce qubits error rates and scale up to a hundred logical qubits<sup>487</sup>. In a July 2020 conference, Hartmut Neven announced his 10-year plan to achieve this result, showing impressive mockups of a giant quantum computer containing 100 modules with 10 000 physical qubits each. It would be a giant installation.

Roadmap for error correction



<sup>482</sup> See [Quantum Approximate Optimization of Non-Planar Graph Problems on a Planar Superconducting Processor](#) by Google AI Quantum and Collaborators, April 2020 (17 pages) which deals with three families of combinatorial problems with the QAOA algorithm and [Hartree-Fock on a superconducting qubit quantum computer](#) by Google AI Quantum and Collaborators, April 2020 (27 pages) with a diimide  $(\text{NH})_2$  molecular simulation algorithm.

<sup>483</sup> See this theoretical paper on the use of quantum computing, not necessarily with Google qubits, to study black holes. See [Google Scientists Are Using Computers to Study Wormholes](#) by Ryan F. Mandelbaum, November 2019 which refers to [Quantum Gravity in the Lab: Teleportation by Size and Traversable Wormholes](#) by Adam R. Brown et al, November 2019 (20 pages).

<sup>484</sup> See [Alphabet Has a Second, Secretive Quantum Computing Team](#) by Tom Simonite, January 2020. No secret anymore buddy!

<sup>485</sup> See [Google's Head of Quantum Computing Hardware Resigns](#) by Tom Simonite, April 2020. He resigned from Google in April 2020 after being demoted to a scientific advisory role mid-2019.

<sup>486</sup> John Martinis explains in detail his reasons for leaving Google in an interview for Forbes: [Google's Top Quantum Scientist Explains In Detail Why He Resigned](#) by Paul Smith-Goodson, 2020.

<sup>487</sup> Source of illustrations: [Day 1 opening keynote by Hartmut Neven \(Quantum Summer Symposium 2020\)](#), July 2020 (30 mn) and the [whole symposium](#).



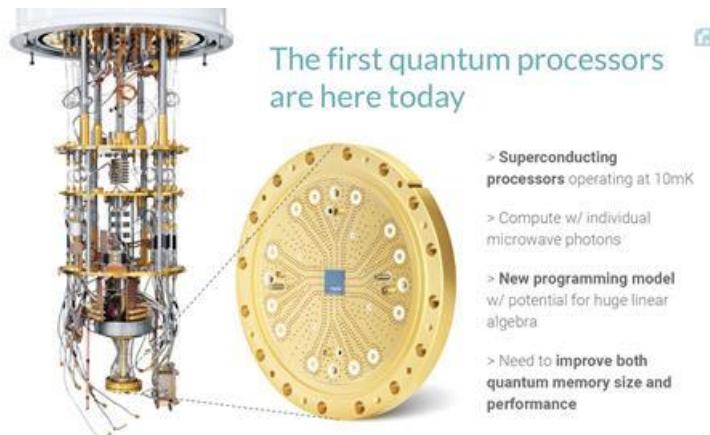
**Rigetti** (2013, USA, \$656M) is another commercial superconductor vendor. Together with D-Wave and PsiQuantum, it is the third best funded startup in the industry. It was launched by Chad Rigetti, who received his PhD from Yale University on superconducting qubits in 2009<sup>488</sup>.

Their last generation is Aspen-9 with 31 qubits, being deployed at Amazon Braket. They announced a 128 qubits test version in August 2018 but it was never used or benchmarked.

Their fidelities are not as good as with IBM and Google, which is bad omen. They have their own small manufacturing unit producing their semiconducting chipsets. The required equipment costs about \$10M, which is reasonable even for a startup. The creation of superconducting qubit circuits is done with a very low-level of integration.

We are far from the \$20B 5nm fabs from TSMC. In the case of silicon qubits, on the other hand, it is necessary to have an equipment of about \$1B<sup>489</sup>!

Aspen-9		Median Time Duration (μs)	Median Fidelity (per op.)
Deployed	07.02.21	T1 Lifetime	27
Qubits	31	T2 Lifetime	19
			Two-qubit gates (XY) 95.4%



**Coupling qubits:** their flux qubits are entangled by dynamically configurable couplers, which reminds us of Google Sycamore. It brings more flexibility for managing two qubit gates<sup>490</sup>. These are adjustable transmon qubits using asymmetric SQUIDs (magnetometers).

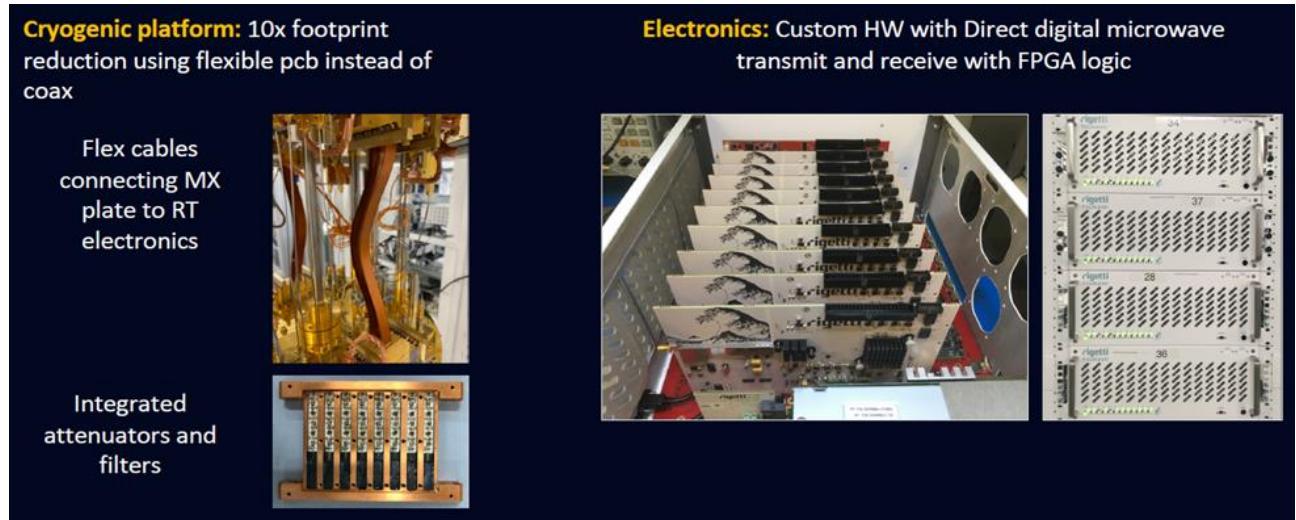
**Electronics optimization:** Rigetti made efforts to optimize the physical and electrical components of its accelerators.

<sup>488</sup> See [Quantum Gates for Superconducting Qubits](#), 2009 (248 pages).

<sup>489</sup> See [Quantum Cloud Computing Rigetti](#) by Johannes Otterbach, 2018 (105 slides) and the [corresponding video](#).

<sup>490</sup> This is explained in [Demonstration of Universal Parametric Entangling Gates on a Multi-Qubit Lattice](#) by M. Reagor et al, 2018 (17 pages).

First, by integrating the control and measurement wiring of the qubits in compact sheets that they patented<sup>491</sup>. They developed their own microwave generation electronics. They also found a way to limit crosstalk between qubits<sup>492</sup>. The coherence time of qubits is 200  $\mu$ s, which is a best-in-class with commercial superconducting qubits. They also work on merging microwave and DC flux lines into the same wires used for respectively XY and Z single qubit gates, between the 10 mK cold plate and the qubit chipset<sup>493</sup>.



**Modular chipsets.** Rigetti is working on splitting qubits in multiple semiconductors dies connected with each other with indium-based flip-chip bonded on a single larger carrier die. This reduces qubits crosstalk between modules, at the expense of a smaller fidelity. With 4 chips containing each 4 aluminum and niobium-based SQUIDs qubits and 4 tunable couplers, their fidelities are  $99.1 \pm 0.5\%$  and  $98.3 \pm 0.3\%$  for iSWAP and CZ gates<sup>494</sup>.

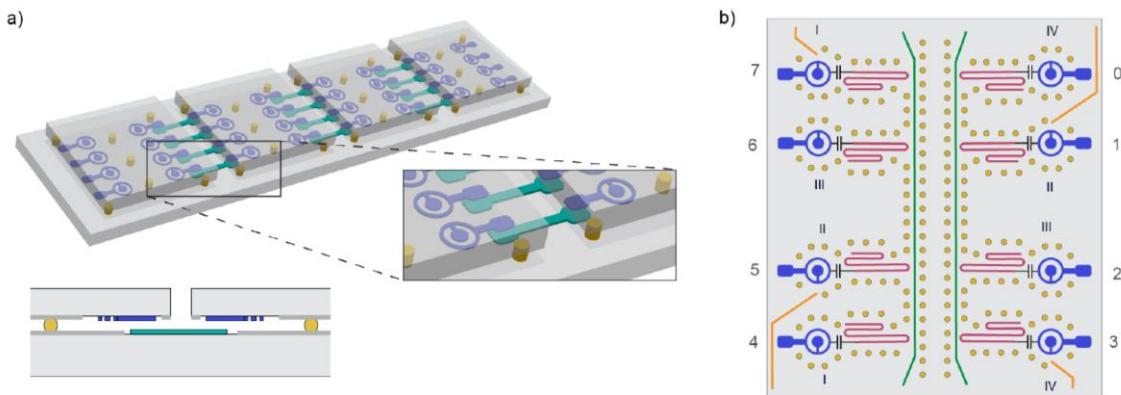


FIG. 1. (a) Isometric view of the device assembly. The qubits (blue circular structures) are fabricated on the QuIC die and have one arm with a paddle-shaped coupler extending to the edge of the chip. The chips are flip-chip bonded onto the carrier chip using indium bump bonds (yellow) and the qubit couplers are aligned above couplers on the carrier chip (teal) as shown in the inset as well as the cross-sectional view. (b) False-colored image of a single QuIC including readout resonators and readout lines (magenta and green), indium bumps (yellow), flux bias lines (orange) and the qubits and paddles of the inter-chip couplers (blue). The physical qubits are labelled 0-7 while Roman numerals correspond to the design specification for the qubit (see Methods).

<sup>491</sup> See Connecting Electrical Circuitry in a Quantum Computing System, [USPTO 20190027800](#).

<sup>492</sup> See [Methods for Measuring Magnetic Flux Crosstalk Between Tunable Transmons](#) by Deanna M. Abrams et al, August 2019 (12 pages).

<sup>493</sup> See [Full control of superconducting qubits with combined on-chip microwave and flux lines](#) by Riccardo Manenti et al, July 2021 (8 pages).

<sup>494</sup> See [Entanglement Across Separate Silicon Dies in a Modular Superconducting Qubit Device](#) by Alysson Gold, 2021 (9 pages).

**Full-stack software development:** includes pyQuil for scripting and Quil for quantum gate management. These are both open-source and published on Github. Quil allows to synchronize tasks between quantum and classical computing ([documentation](#)). In 2018, they demonstrated the use of their quantum computer for a machine learning algorithm that does not require a hybrid algorithm<sup>495</sup>.

**Acquisition:** Rigetti acquired QxBranch in July 2019 to complete its software offering. It was established in the USA, UK and especially in Australia. In September 2020, their UK-based subsidiary announced the launch of a collaborative project to accelerate the commercialization of quantum computers, funded with £10M private/public money. To do so, they will use a latest-generation Proteox cryostat from Oxford Instruments.

**Cloud:** Rigetti offers access to its quantum computers via the cloud, like IBM and D-Wave do with their Quantum Cloud Services. It started running in beta in January 2019. Since early 2020, they are also distributed in the cloud by Amazon in its Braket service.



**IQM** (2018, Finland, €70.8M) was initially developing an on-chip refrigeration system technology for superconducting and silicon chip-sets based on electron transfer using an electron tunnel-effect<sup>496</sup>.

IQM is a spin-off from the Quantum Computing and Devices group of the Aalto University and from the VTT research center. They opened a research lab in Germany in March 2020. In 2020, the Finland government granted VTT with a 20,7M€ funding to acquire an IQM system. It should reach 50-qubit by 2024. They had 5 operational qubits as of November 2021. The company had over 120 people as of August 2021.

The company states that their qubits are operable with a faster clock speed than competing superconducting qubits thanks to optimizations applied to qubits reset, gates and readout. They use tunable couplers for qubits entanglement. After relying on VTT Micronova 2600 m<sup>2</sup> clean-room fab, they inaugurated their own Espoo 560 m<sup>2</sup> and 20M€ fab in November 2021 to manufacture their chipsets, a self-sufficiency strategy also seen with Rigetti.

They have a business model based on selling quantum computing system to research and supercomputing centers as well as proposing customized hybrid analog/digital "Co-Design QC" quantum processors. The latter could be classified as "quantum ASICs", based on superconducting qubits<sup>497</sup>. These systems are adapted to the execution of hybrid algorithms such as VQE (Variational Quantum Eigensolvers) and QAOA (Quantum Approximate Optimization Algorithm). IQM will also implement a digital-analog quantum processor together with other partners like Infineon at the LRZ supercomputing center in Garching, near Munich in Germany<sup>498</sup>.

In June 2020, IQM received 15M€ capital funding from the European Commission's EIC Accelerator, supplemented by a 2.5M€ grant. They also announced a partnership with Atos together with the Finnish supercomputing center CSC which bought a classical QLM emulator for their services. This machine is used both to simulate the operation of IQM's quantum accelerator qubits and to drive it<sup>499</sup>. The partnership also involves the Finnish computing center CSC, which provides scientific computing resources to the country's researchers, much like GENCI does in France.

---

<sup>495</sup> In [Quantum Kitchen Sinks: An algorithm for machine learning on near-term quantum computers](#), July 2018 (8 pages).

<sup>496</sup> See [Quantum-circuit refrigerator](#) by Kuan Yen Tan et al, 2017 (8 pages). And [video](#).

<sup>497</sup> Their method is described in [Approximating the Quantum Approximate Optimization Algorithm](#) by David Headley et al, February 2020 (14 pages) and [Improving the Performance of Deep Quantum Optimization Algorithms with Continuous Gate Sets](#) by Nathan Lacroix, Alexandre Blais, Andreas Wallraff et al, May 2020 (14 pages).

<sup>498</sup> See [New EU Consortium shaping the future of Quantum Computing](#), IQM, February 2021.

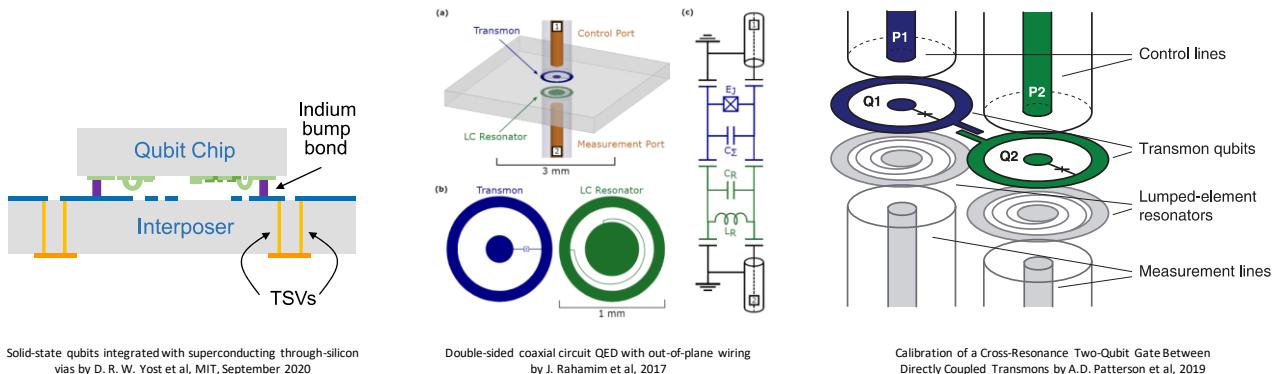
<sup>499</sup> See [Atos, CSC and IQM join forces to accelerate the commercialization of European quantum technologies](#), June 2020.

Atos has also announced its interest to distribute an IQM quantum accelerator, among other market solutions, including the Pasqal simulator.



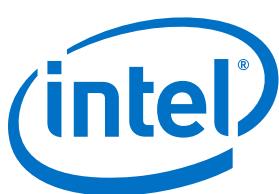
**Oxford Quantum Circuits** (2017, UK, \$18M) was launched by Peter Leek from Clarendon Laboratory Oxford. The startup is run by Ilana Wisby and had a team of 26 people as of May 2021. The company wants to remove the identified barriers that prevent superconducting qubits from scaling.

OQC's technology is based on their "coaxmon" superconducting qubits that are composed of highly coherent planar qubits<sup>500</sup> and using a 3D structure connecting the qubit chipset with an interposer and using a layer for controlling the qubits on top of the chipset and another one below for qubit readouts<sup>501</sup>. It's based on various works from MIT and the University of Oxford<sup>502</sup>.



They are partnering with Cambridge Quantum Computing (CQC) which is developing a quantum compiler dedicated to their qubits. In April 2020, OQC obtained collaborative project funding from the British government of £7M. As part of this project, they are associated with SeeQC UK, Oxford Instruments, Kelvin Nanotechnology, the University of Glasgow and the Royal Holloway University of London.

In July, OQC announced that they were making their first system available only as a QCaaS solution, in private beta (quantum cloud as a service). They then announced that an 8 qubit version of their processor would be made available on Amazon Braket by the beginning of 2022.



**Intel** is another player in the superconducting qubits field. With no commercial solution so far as it's only a research field at this stage, completed by to the more natural avenue of electron spin silicon qubits they are also pursuing. At CES 2018, Intel's CEO proudly showcased a 49-qubit superconducting chipset during his keynote, stuck between a passenger drone demonstration and a broad talk on artificial intelligence.

Named Tangle Lake, it was tested at **Qutech** in the Netherlands. They were at 7 qubits at the end of 2016, 17 qubits at the end of 2017 and 49 (uncharacterized) qubits in January 2017. Since then, no news. It seems that Intel is now entirely focused on electron spin qubits, along with their partner Qutech in The Netherlands, where they invested \$50M back in 2015.

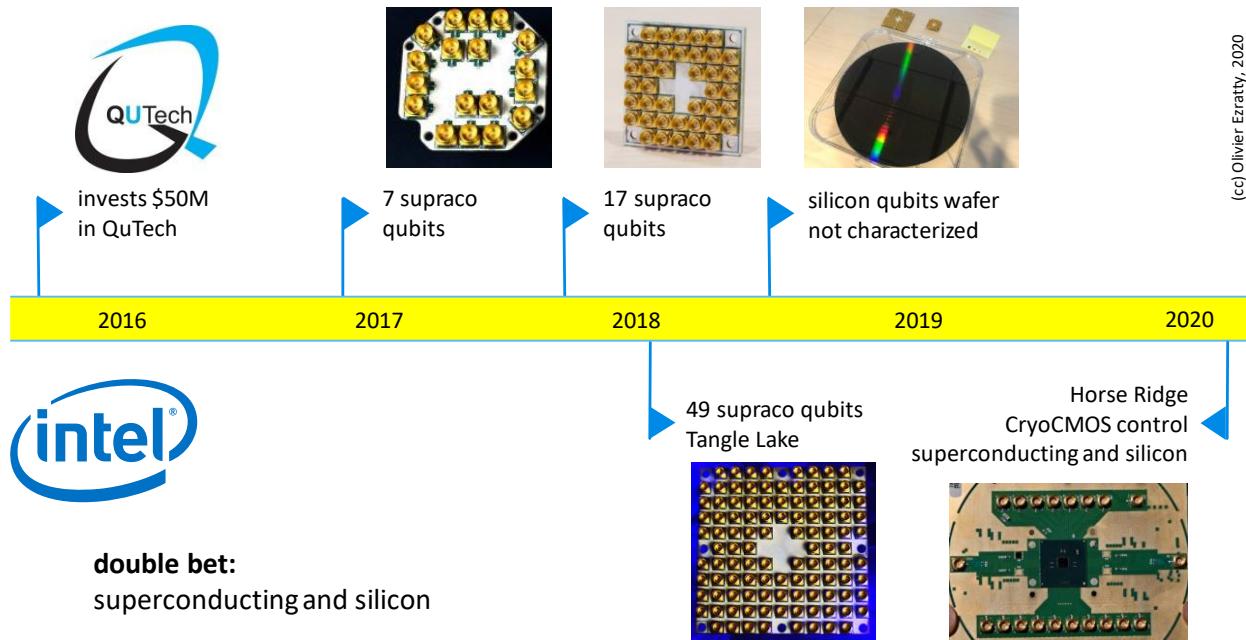
<sup>500</sup> See [Surface acoustic wave resonators in the quantum regime](#), 2016 (40 slides).

<sup>501</sup> The 3D layering and TSV structure is inspired from [Solid-state qubits integrated with superconducting through-silicon vias](#) by D. R. W. Yost et al, MIT, September 2020 (9 pages). This project was funded by IARPA.

<sup>502</sup> See [Double-sided coaxial circuit QED with out-of-plane wiring by J. Rahamim](#) et al, 2017 (4 pages) and [Calibration of a Cross-Resonance Two-Qubit Gate Between Directly Coupled Transmons](#) by A.D. Patterson et al, 2019 (8 pages).

In February 2020, Intel announced its Horse Ridge cryogenic component, used to drive superconducting and silicon qubits inside the cryostat. It creates microwaves in the 6 to 7 GHz (for superconducting qubits) and 14 to 20 GHz (for silicon qubits) frequency bands. They are specified to cover a range from 2 to 20 GHz. It is a cryo-CMOS component integrating SRAM memory realized in Low Power FinFET in 22 nm integration, on 4 mm<sup>2</sup>. It can control up to 128 qubits and operates at 3K<sup>503</sup>. It consumes 1.7 mW per qubit and a total of 330 mW.

This is within the cooling power envelope of a current cryostat 4K stage, which is typically about 1W. The component is being tested by QuTech in the Netherlands.



**Anyon Systems** (2014, Canada) is the kind of startup whose communication seems to be designed to thwart any attempt to understand exactly what they are doing.

They are developing gates-based superconducting qubits quantum computers implementing some sort of topological error correction codes. In December 2020, they announced that they would provide such a system to the Canadian Department of Defense using their Yukon processor. But there's no open way to have some clues on the number, geometry and fidelity of their qubits. They also developed Quantum Device Simulator (QDS), a software tool used in quantum computer design and simulation that can run on supercomputers.

It was used by John Martinis' Google team in 2017 for their design of a superconducting 6- and then 20-qubit qubit processor<sup>504</sup>. Their software was mainly used to predict the level of adjacent qubits cross-talks.



**Bleximo** (2017, USA, \$1.5M) develops the qASICs qubits, based on superconducting Josephson effect. It wants to develop quantum coprocessors adapted to different markets including biotechs.

<sup>503</sup> See [Intel and QuTech Unveil Details of First Cryogenic Quantum Computing Control Chip, 'Horse Ridge'](#), February 2020 and their [HorseRidge](#) flyer.

<sup>504</sup> See [Google's 'supreme' 20-qubit quantum computer](#) by Tushna Commissariat, 2017.

The startup was founded by Alexei Marchenkova and Richard Maydra, two former Rigetti employees. They are partnering with Q-CTRL which develops error correction codes quantum software. But their nearly empty landing page doesn't bode well for this kind of venture. However, in their team, Anastasia Marchenkova is a researcher producing a lot of [educational video content](#).



**Quantware** (2020, Netherlands, \$1M) is a designer and manufacturer of a superconducting qubits processor, the Soprano with 5 qubits and a customizable topography, with Purcell filters, AirBridges and a proprietary TSV configuration (through-silicon via). It seems to be very classical transmon superconducting qubits. They don't build full-fledged quantum computers.

Their QPU  $T_1$  is modest with 10  $\mu\text{s}$  and a single-qubit gate fidelity of 99,99%. They don't provide data on the most important figures of merit: dual-qubits gates fidelity and readout fidelity.

Who could use these QPUs? Seemingly, research labs and vendors developing enabling technologies for superconducting qubits, like their colleagues from Qblox and Delft Circuits. Similarly to IBM, they plan to double the number of qubits in their QPUs each and every year. All these claims are to be taken with a grain of salt.



In April 2021, the Japanese research center **RIKEN** and **Fujitsu** created the RIKEN RQC-Fujitsu Collaboration Center to do joint research and create a superconducting qubit computer, with a goal of reaching 1000 physical qubits and develop an associated software platform.

It will leverage RIKEN's existing work on superconducting qubits and Fujitsu's computing know-how. The research plan is quite classical: improving qubit manufacturing, reducing the size and noise of driving electronics components and wiring and improve error correcting codes.



Alibaba is active in using the resources of its datacenters to simulate quantum algorithms exceeding 50 qubits. China's leading e-commerce company is also partnering with the **University of Science and Technology of China** (USTC) of the Chinese Academy of Sciences (CAS) to create superconducting quantum computers with superconducting qubits.

They offer cloud access to 11 qubits since early 2018, on a technology platform developed with USTC. They even announced in 2018 that they were creating a subsidiary, **Ping-Tou-Ge**, which develops NPUs (neuromorphic processors for AI) and, eventually, superconducting quantum chipsets<sup>505</sup>. They work on superconducting qubits, using the fluxonium variation, which could bring some coherence advantage. They announce qubit lifetimes  $T_1$  and  $T_2$  over 100  $\mu\text{s}$  and a 99,5% iSWAP gate fidelity.

At last, in 2021, a China research team led by Jian-Wei Pan created a 66 superconducting qubits system and claimed having reached another quantum advantage. In their Zuchongzhi system, they reproduced the Google supremacy experiment with a 2D array of qubits with 13 additional qubits, using the same coupling technology, with 110 couplers<sup>506</sup>. Their fidelities were not best-in-class with 99,86% for single qubit gates, 99,24% for two-qubit gates and 95,23% for qubits readout, on top of a rather low  $T_1$  of 30.6  $\mu\text{s}$ . In their experiment, though, they did use only 56 of their 66 qubits, showing that qubits fidelities are probably not that good when all qubits are activated. In September 2021, they used 60 qubits on 24 cycles with an improved readout fidelity of 97.74%<sup>507</sup>.

<sup>505</sup> See [Alibaba Launches Chip Company "Ping-Tou-Ge"; Pledges Quantum Chip](#), September 2018.

<sup>506</sup> See [Strong quantum computational advantage using a superconducting quantum processor](#) by Yulin Wu, Jian-Wei Pan et al, June 2021 (22 pages).

<sup>507</sup> See [Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling](#) by Qingling Zhu, Jian-Wei Pan et al, September 2021 (15 pages).

Now, on to cat-qubit vendors...



ALICE & BOB

**Alice&Bob** (2020, France, €3M) was created by Théau Peronnin (ENS Lyon) and Raphaël Lescanne (ENS Paris). They are designing a fault-tolerant gate-based quantum computer associating superconducting technology and stabilized photon-based (in the microwave regime) cat-qubits. Their technology main benefit is its capability to implement a complete universal fault-tolerant quantum computer with a much lower ratio of physical per logical qubits than traditional transmon based superconducting qubits. It saves at least two orders of magnitude, moving from 10000 to 1 down to 100 to 1!

Alice&Bob's technology is based on the PhD thesis from the startup founders and the associated work of the **Mazyar Mirrahimi**'s Quantic team from Inria where Raphaël Lescanne was a doctoral student and where **Zaki Leghtas** as well as **Jérémie Guillaud** also work or worked<sup>508</sup>, the CNRS and ENS Lyon and ENS Paris. We'll see how all these works were influential, up to inspire Amazon in its own cat-qubits engineering efforts, documented later.

Cat-qubits encode the state of a qubit with superposing opposite quantum states in micro-wave photon cavities, precisely, in the two-dimensional Hilbert space spanned by two coherent states of microwaves of same amplitude and opposite phase<sup>509</sup>. These cat-qubits have a very low bit-flip error rate given it decreases exponentially with the average number of microwave photons used in the cat qubit cavity. Phase-flip errors can be corrected with repetition error codes having a rather low overhead<sup>510</sup>.

In conventional superconducting qubits, non-Clifford gates are corrected with “magic state distillation”, a QEC that adds a 100x overhead in physical qubits. That's why 10,000 to 100,000 physical qubits per logical qubits are frequently mentioned. Cat-qubits supports a native implementation of 3-qubits Toffoli gates which, combined with Clifford gates, can form a universal set of quantum gates. The implementation of such a universal gate set is a prerequisite to run quantum algorithms with a proven exponential speed-up. The Toffoli gate is an alternative to the usual (non-Clifford) T gate used in QFT-based algorithms. This gate can be corrected efficiently with avoiding magic state distillation, enabling fault-tolerance and limiting error propagation between ancilla qubits<sup>511</sup>.

These qubits are more complex to design and operate but it would only take between 10 and 100 of them to create a well-corrected logical qubit, which would make it possible to create a better scalable architecture whereas with the current technologies of IBM, Google and Rigetti, about 10,000 physical qubits are required to create a functional logical qubit given their expected fidelities. These corrected qubits could also play the role of quantum memory. Moreover, their system avoids microwave radiations leaks between adjacent qubits.

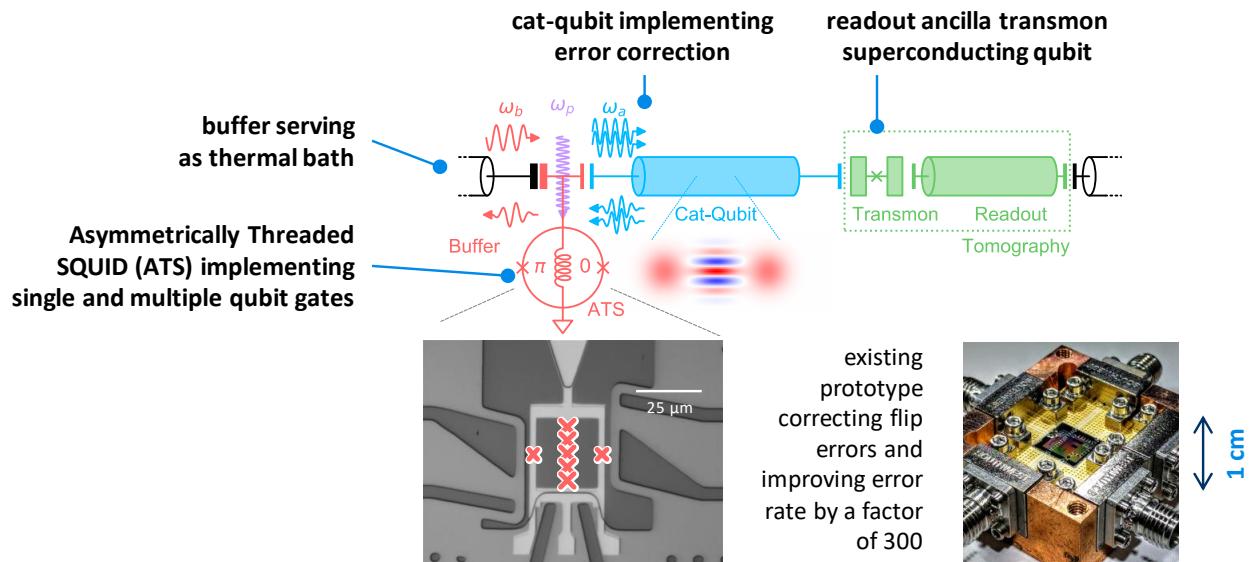
---

<sup>508</sup> Mazyar Mirrahimi did work in Michel Devoret's team at Yale around 2012. See [Dynamically protected cat-qubits: a new paradigm for universal quantum computation](#) by Mazyar Mirrahimi, Zaki Leghtas and Michel Devoret, 2013 (28 pages). Jérémie Guillaud is now Chief of Theory at Alice&Bob.

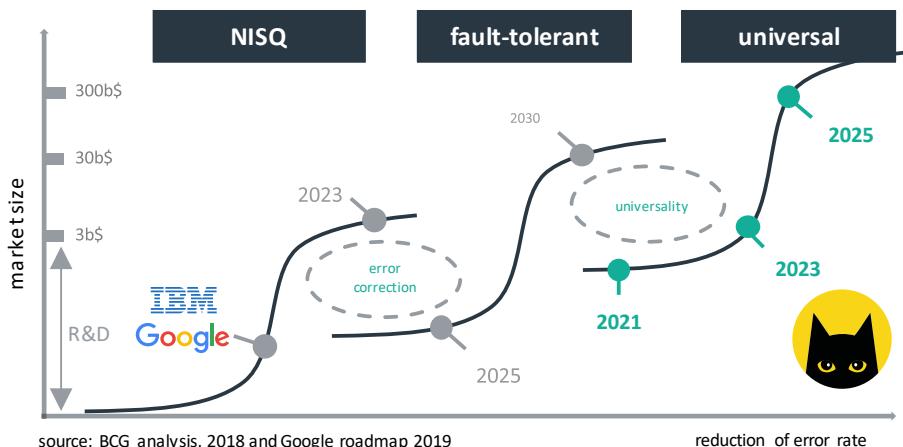
<sup>509</sup> See [Exponential suppression of bit-flips in a qubit encoded in an oscillator](#) by Raphaël Lescanne et al, July 2019 (18 pages) and [Repetition Cat Qubits for Fault-Tolerant Quantum Computation](#) by Jérémie Guillaud and Mazyar Mirrahimi, July 2019 (23 pages).

<sup>510</sup> See [Error Rates and Resource Overheads of Repetition Cat Qubits](#) by Jérémie Guillaud and Mazyar Mirrahimi, March 2021 (17 pages). Based on numerical simulation, it estimates that a fault-tolerant cat-qubits computer with a logical error probability of  $10^{-10}$  can be realized using 140 physical cat-qubits for Clifford gates and an average number of 15 photons per mode. A Toffoli gate could be implemented with only 180 physical cat-qubits including all required ancilla qubits.

<sup>511</sup> They propose a ‘pieceable fault-tolerant’ implementation of the Toffoli gate, following the method introduced in [Universal Fault-Tolerant Gates on Concatenated Stabilizer Codes](#) by Theodore J. Yoder, Ryuji Takagi and Isaac L. Chuang, September 2016 (23 pages). This is a substitute to the transversal gates technique.



The gates they implement on top of a Toffoli gate are a CNOT and a Hadamard gate. SWAP gates are built with three CNOTs in a classical fashion. These are heavily used to circumvent the absence of many to many qubits connectivity in most 2D qubits layouts. All this will require a specific compiler, to be done later in the startup product lifecycle.



**Amazon** (USA) started first to announce late 2019 its Amazon Braket cloud offering, based on using third-party quantum computers from D-Wave, Rigetti and IonQ, covered in the cloud section of this ebook, page 523.

In December 2020, they went out of the woods with announcing their detailed plan to build their own quantum computers, using cat-qubits, in a thorough 118 pages paper<sup>512</sup>.

This work is getting the help from Caltech, including John Preskill, in connection with Yale where some Caltech students did their PhDs in the teams of Rob Schoelkopf and Michel Devoret. The Amazon effort is led by **Simone Severini** (Director of Quantum Computing at AWS), **Oskar Painter** (Head of Quantum Hardware at AWS), **Fernando G.S.L. Brandão** (Head of Quantum Algorithms at AWS and also researcher at Caltech) and **Richard Moulds** (GM Amazon Braket).

<sup>512</sup> See [Building a fault-tolerant quantum computer using concatenated cat codes](#) by Christopher Chamberland, John Preskill, Oskar Painter, Fernando G.S.L. Brandão et al, 2020 (118 pages). It is summarized in [Designing a fault-tolerant quantum computer based on Schrödinger-cat qubits](#) by Patricio Arrangoiz-Arriola and Earl Campbell, April 2021. See also [Fault-tolerant quantum computing with biased-noise hardware](#) by Earl Campbell, November 2020 (40 mn).

The bulk of Amazon's quantum team are based in the new 21,000-sqrt-ft AWS Center for Quantum Computing building next to Caltech in Pasadena, North of Los Angeles. It was inaugurated in October 2021.

The Amazon proposed architecture is largely inspired by what the French teams of Inria have done and investigated since 2013 with Mazyar Mirrahimi et al, including the founders of Alice&Bob<sup>513</sup>. They want to create a FTQC.

Amazon is using an electro-acoustic resonator to host the cat qubits while the circuit element, the Asymmetrically Threaded SQUID (ATS) invented by Raphaël Lescanne and Zaki Leghtas, used by Alice&Bob to stabilize the cat-qubit is superconducting. While Alice&Bob QEC is based on dissipating excess qubit energy to maintain it in low-energy states with encoding it in a linear oscillator driven by 10 GHz microwaves, Amazon chose a variant that uses linear harmonic oscillators-based cat-qubits using very compact piezoelectric nanostructures and phonons. Like with Alice&Bob, these cat-qubits self-corrects flip errors at the hardware level while phase errors are being handled by some QEC.

Cat-qubits encode information with microwaves put in coherent states with opposite phases,  $|+\rangle$  and  $|-\rangle$ . The qubit computational basis states are defined as even and odds coherent states cats, meaning using positive and negative sign superpositions for these two cat-states.

Like Alice&Bob, they will implement a universal gates set comprising X, Z, CNOT and Toffoli gates. They use two new ideas for implementing fault-tolerant Toffoli gates: an extremely small chip layout ("bottom-up Toffoli") and a technique to lower the bit-flip error rate ("top-down Toffoli").

They also avoid crosstalk between cat-qubits with using four cat-qubits connected to a single dissipating reservoir. This compact layout is compatible with a scalable architecture but may generate significant crosstalk errors, which could be mitigated with a well-chosen filter design cutting the frequencies to remove crosstalk errors.

They plan to implement a 9 data-qubits QEC to obtain a logical error rate of  $2.7 \times 10^{-8}$ . As a result, they expect to use 2000 superconducting components to create a 100 logical qubits system. If this works, as with Alice&Bob, it will make a significant difference with IBM and Google who plan to obtain the same number of logical qubits with one million physical qubits. The scalability constraints are much different in both cases, whether it deals with cryogenics, microwave generations and readouts, or cabling.

Still, with 2000 qubits, microwave generation and readout will somewhat need to be implemented inside the cryostat and at this point, Amazon has not mentioned anything about it. Pragmatism could lead them to investigate the use of SeeQC superconducting electronic components (*aka* SFQs).

In April 2021, University of Sydney science undergraduate Pablo Bonilla Ataides published in Nature Communications a paper on its ZXXZ surface code that would reduce the number of required physical qubits to create a logical qubit thanks to a lower error threshold. It brought the attention of Amazon researchers<sup>514</sup>. This surface code could be used by Amazon who made a choice to use a relatively low number of photons per cat qubit (8 to 10), still requiring some first level bit-flip error correction on top of phase-flip correction. That's where a ZXXZ surface code QEC could come into play. ZXXZ QEC codes are indeed mentioned as an option QEC technique in Amazon's technical paper from December 2020.

---

<sup>513</sup> On top of France's founding work on cat-qubits, Amazon is also relying on many US Universities research like Caltech, Stanford, Chicago University and Yale.

<sup>514</sup> See [Student's physics homework picked up by Amazon quantum researchers](#) by Marcus Strom, University of Sydney, April 2021, [Sydney student helps solve quantum computing problem with simple modification](#) by James Carmody April 2021 and [The XZZX surface code](#) by J. Pablo Bonilla Ataides et al, April 2021, Nature Communications (12 pages).



**QCI** (2015, USA, \$18M) or Quantum Circuits Inc is a spin-off from Yale University co-founded by Rob Schoelkopf, Luigi Frunzio and Michel Devoret. Michel left them in 2019, preferring to be a full-time researcher at Yale University.

Their technology is also based on cat-qubits that solve noise and coherence problems, using Rob Schoelkopf's team work at Yale. They have a long track-record in that space although they are not very talkative. As announced back in 2019, their system should be available some day on Microsoft Azure Quantum cloud.

They are also at the origin of the **qbsolv** framework that is part of their **Mukai** middleware and development platform launched in January 2020<sup>515</sup>. It supports D-Wave computers, Fujitsu digital-annealed computers and Rigetti superconducting qubits.

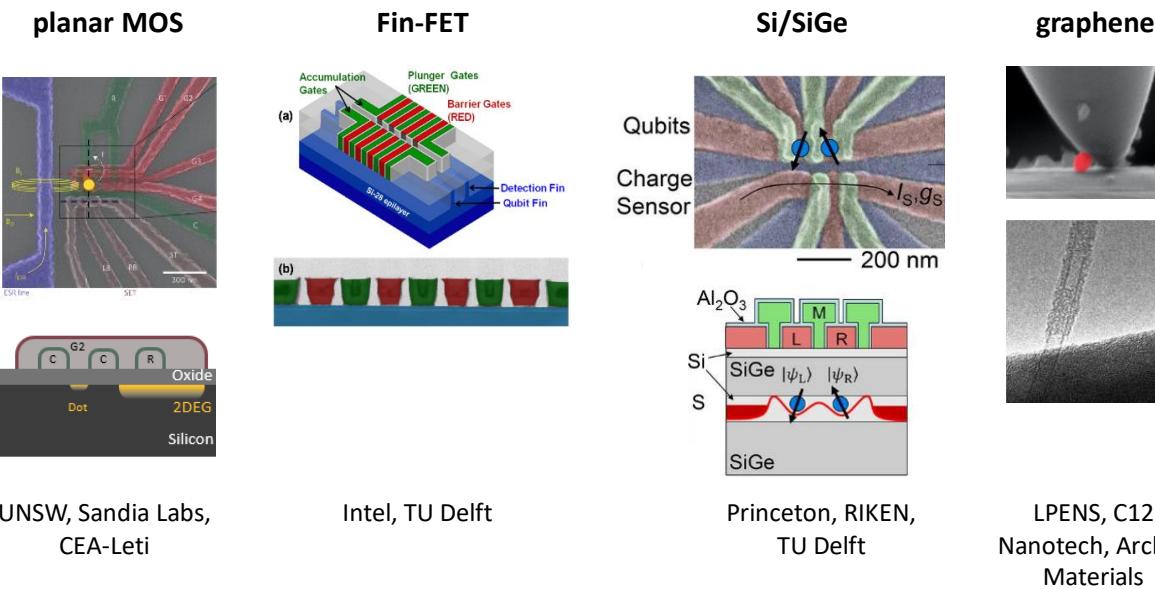


**Nord Quantique** (2019, Canada) is a startup from the Institut Quantique from the University of Sherbrooke that is working on creating a superconducting quantum computer using more efficient error correction, using another variation of bosonic codes. Quantonation is one of their investors.

## Electron spins qubits

Electron spins qubits are a new promising qubit technology with a lot of variations. Its related research started later than superconducting qubits. Its potential benefits are miniaturization and scalability. It could leverage existing manufacturing processes for standard CMOS semiconductors<sup>516</sup>.

This is the path chosen by some research laboratories around the world and by some commercial companies such **RIKEN** in Tokyo and **NTT Basic Research Laboratories** in Japan, **TU Delft** in the Netherlands, **University of Aachen** in Germany, **NBI** in Denmark, **Oxford University**, **Cambridge University** and **UCL** in the UK, **UNSW** in Australia, **Princeton**, **Purdue** and **Wisconsin-Madison Universities**, **HRL Malibu** and **Intel** in the USA. In France, it is a key project led by **CEA-Leti**, teaming up with **CEA-IRIG**, **UGA** and the **CNRS Institut Néel** in Grenoble.



Inspired from: MaudVinet JEDM tutorial, 2020

<sup>515</sup> See [QCI Obsolv Delivers Strong Classical Performance for Quantum-Ready Formulation](#) by Michael Booth et al, May 2020 (7 pages).

<sup>516</sup> CMOS ("Complementary Metal Oxide Semiconductor") is the dominant technology used to produce microprocessors, for CPUs (Intel, AMD), GPUs (Nvidia, AMD), chipsets for smartphones (Qualcomm, Samsung, Mediatek, HiSilicon, etc.) and in a whole host of specialized sectors (microcontrollers, radio components, etc.).

Electron spin qubits quantum state is generally the spin orientation of an electron trapped in a potential well or of an electron hole, i.e. a missing electron and its virtual inverse impact on structural spin. Its coherence times have been tested beyond the second threshold. There are many implementation variations, namely with AsGa (gallium arsenide, first tested in 2005, but with very short coherence times due to spin interferences from gallium and arsenic atoms nuclei), silicon (starting in 2012 and progressing), germanium on silicon (with a record 4 entangled qubits at QuTech), atom ions implanted on silicon (SQC in Australia) and also, with graphene structures trapping single electrons (nanotubes from C12 in France or spheres from Archer in Australia).

Germanium is used with silicon for the stability of its spin holes and large band gaps, with its qubits entanglement capacity, but is more difficult to manufacture and scale, with gates that are far from the qubits<sup>517</sup>.

Graphene structures have the benefit of better protecting the spin of a trapped electron, at the expense of more complicated interfaces and controls. Silicon qubits are more generic and easier to manufacture. They are built with planar MOS and gates that are closer to qubits as well as with FinFET that is inspired from the latest CMOS manufacturing technologies. Many techniques are based on FD-SOI which make it easier to create and isolate the quantum dots.

In 2020, demonstrated silicon-based qubits (silicon or silicon+germanium) reached a fidelity of more than 98% for all operations with readout times of 5µs. Spin qubits have a size of about 100x100 nm, leading to potential high densities when it will scale. A record breaking 4 entangled qubits was announced late 2020 by TU Delft, based on germanium.

## electron spins qubits

- **good scalability potential** to reach millions of qubits, thanks to their size of 100x100 nm.
- **works at around 1K** => larger control electronics energy budget.
- adapted to **2D architectures** usable with surface codes or color codes QEC.
- can leverage existing semiconductor **fabs**.
- good quantum **gates speed**.

- **so far, only four entangled qubits** (UNSW, QuTech, Princeton, UTokyo).
- **average qubits fidelity** with 98% for two qubits gates.
- **qubits variability** to confirm.
- **high fabs costs** and quality manufacturing constraints.

It is both this dimension, the intrinsic potential of silicon with  $10^{-7}$  error rates demonstrated in massive silicon samples and the possibility to integrate control electronics in or around the qubit chipset that makes it an interesting candidate for large-scale quantum computing<sup>518</sup>.

<sup>517</sup> See this excellent germanium review paper: [The germanium quantum information route](#) by Giordano Scappucci, Silvano De Franceschi et al, 2020 (18 pages).

<sup>518</sup> A good up-to-date overview of silicon qubits can be found in [Scaling silicon-based quantum computing using CMOS technology: Challenges and Perspectives](#) by Fernando Gonzalez-Zalba, Silvano de Franceschi, Tristan Meunier, Maud Vinet, Andrew Dzurak et al, 2020 (16 pages).

The general principle used to create qubits of this type is the following<sup>519</sup>:

- **Qubit quantum state** is generally the spin of a trapped individual electron in a semiconductor structure potential well.
- **Single-qubit quantum gates** use the principle of electron spin resonance (ESR). As with superconducting qubits, these gates rely on the emission of microwaves sent by conduction to the qubits, either using electromagnetic cavities, or with radio-frequency lines in which an alternating current creates a magnetic field, or finally, using micro-magnets. The related microwaves use frequencies between 12 and 20 GHz. These gates are usually R<sub>x</sub> and R<sub>y</sub> gates with the microwave pulse phase driving the gate rotation around axis X or Y and their amplitude and duration driving the rotation angle.
- **Two-qubit quantum gates** are created by controlling a tunneling interaction between two neighboring qubits with a significant number of electrodes. These interact with each other by modifying the potential barrier that separates the two qubits. The manipulations, as in single-qubit gates, are performed by applying square pulse currents to qubit barrier and plunger gates. Common low-level gates of this type are the square root of a SWAP gate and a phase controlled gate.
- **Qubit readout** uses the conversion of the electron spin into electrical charge ("spin to charge") which is then exploitable by traditional electronics. It's frequently using a second electron-spin positioned next to each and every computing qubit. It's based on a microwave pulse sent on the qubit and a reflected signal phase/amplitude analysis, *aka* gate reflectometry<sup>520</sup>.

This technique allows the integration of a large number of qubits in a circuit, with potentially up to billions of qubits on a single chipset. It seems to be the only technology that can achieve this level of integration. These qubits would have a rather long coherence time and an error rate at least as low as with superconducting qubits<sup>521</sup>.

The control microwaves used have a higher energy level which explains why silicon qubits can theoretically operate around 1K instead of 15 mK for superconducting qubits. This level corresponds to microwaves with a frequency higher than 20 GHz, compared to the 4 to 8 GHz control microwaves of superconducting qubits. This higher temperature makes it possible to place denser control electronics around the qubits without heating up the circuit too much.

The reference data are as follows: only one milliwatt of energy can be consumed at 100 mK<sup>522</sup>. This limits the control electronics to about 10,000 transistors in CMOS technology<sup>523</sup>. It should be noted that once developed, silicon qubits will require the use of massive error correction codes, such as surface codes or color codes.

---

<sup>519</sup> See [Silicon Qubits](#) by Thaddeus D. Ladd 2018 (19 pages) which describes various methods other than the one discussed here.

<sup>520</sup> See an implementation with [Gate-reflectometry dispersive readout and coherent control of a spin qubit in silicon](#) by Alessandro Crippa, Silvano De Franceschi, Maud Vinet, Tristan Meunier et al, July 2019 (6 pages).

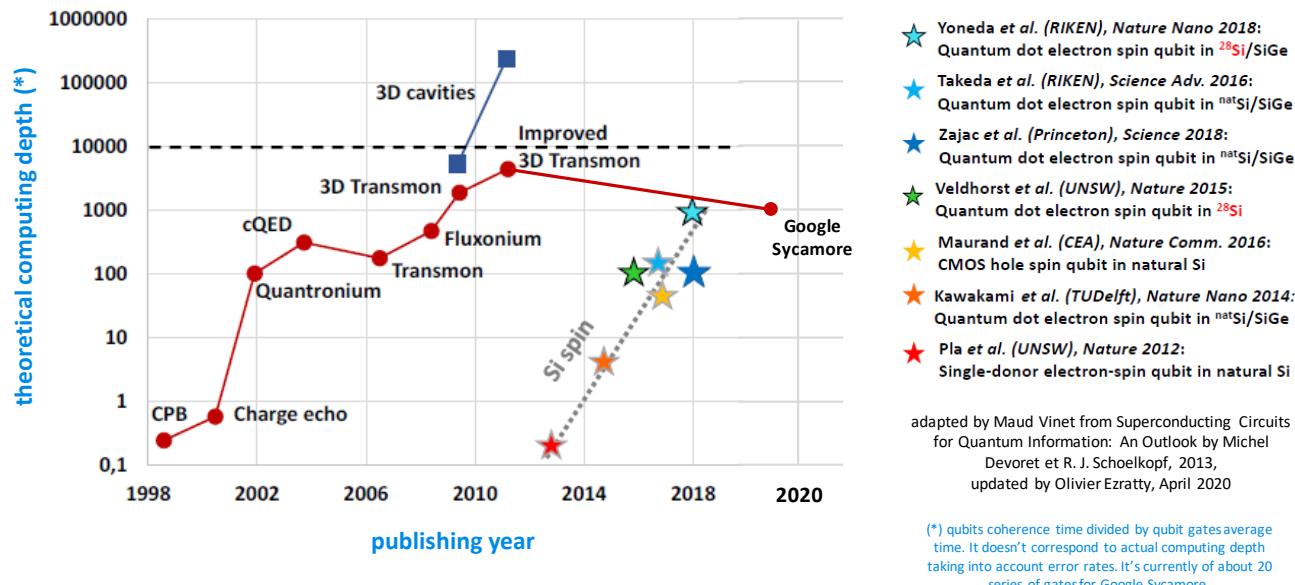
<sup>521</sup> A record silicon qubit coherence time was broken in 2020 by a team from the University of Chicago, reaching 22 ms (T2). This is 10,000 times longer than the usual coherence times around 100μs found in superconducting qubits. These qubits use double gaps in silicon carbide structures. See [Universal coherence protection in a solid-state spin qubit](#) by Kevin C. Miao, David D. Awschalom et al, August 2020 (12 pages). University of Chicago.

<sup>522</sup> A milli-Watt of cooling power can be achieved with a double pulsed tube cryostat such as the BlueFors XLD1000 or the Oxford Instruments TritonXL.

<sup>523</sup> This is explained in [28nm Fully-Depleted SOI Technology Cryogenic Control Electronics for Quantum Computing](#), 2018 (2 pages), from CEA-Leti and STMicroelectronics. It discusses the good performance of CMOS components manufactured in FD-SOI technology and operating at 4K, where the available cooling budget is even higher than at 100 mK. A 4K, the cooling power is in the order of a quarter of a Watt to a Watt.

Advances in spin qubits are more recent in a race against superconducting qubits. The diagram below illustrates this evolution over time between 2013 and 2020<sup>524</sup>, and would require some updating. They use a single parameter of comparison, the number of quantum gates that can be executed before reaching qubit decoherence time T2.

At the state-of-the-art level, the Australians, Dutch researchers from QuTech<sup>525</sup> and Jason Petta at Princeton have demonstrated two-qubit gates in different geometries. To get to the next step, the challenge is to control the electrostatic potential between the quantum wells where the electrons are stored - and thus their spin - with a number of grids that allow the qubits to be arranged not too far apart, typically on the order of a few tens of nanometers.



Note that these qubits can be associated with photonics for long range connectivity. The states of these qubits can be transmitted via photons, which would enable distributed quantum computing architectures<sup>526</sup>.

Here are now the main research laboratories and businesses that are exploring the silicon spin path, very often in multi-laboratory and multi-country partnership ventures.



**QuTech and TU Delft University** in collaboration with Intel are working on a silicon qubit architecture using two-dimensional electron gases based on Si/SiGe built on a SOI substrate<sup>527</sup>.

<sup>524</sup> This diagram is by Maud Vinet and is inspired by [Superconducting Circuits for Quantum Information: An Outlook](#) by Michel Devoret and Robert Schoelkopf, 2013 (7 pages). Being quite old, it does not indicate the progress made since then in superconducting qubits as well as on spin qubits. "Operations per error" is proportional to the ratio between the lifetime of the qubits and the speed of the quantum gates on these qubits. It does not take into account the impact of the qubit error rate, which generally occurs well before reaching the limit of the number of theoretically executable gates.

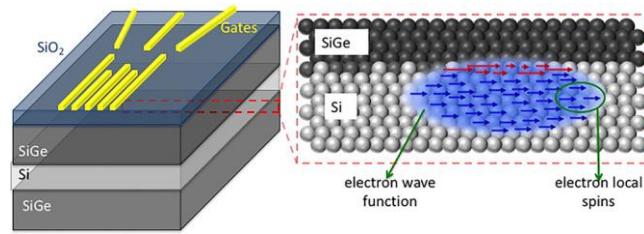
<sup>525</sup> See [A Crossbar Network for Silicon Quantum Dot Qubits](#) by R Li et al, 2017 (24 pages).

<sup>526</sup> See [Coherent shuttle of electron-spin states](#) by Lieven Vandersypen et al, 2017 (21 pages).

<sup>527</sup> QuTech's Menno Veldhorst team published [Reliable and extremely fast quantum calculations with germanium transistors](#) in January 2020. The goal was to demonstrate the feasibility of germanium qubits with two interleaved qubits. Fidelities were respectively of 99.9% and 98% for one and two qubit gates. On the other hand, these qubits coherence time is very low, at <1μs. See [Fast two-qubit logic with holes in germanium](#) by Menno Veldhorst et al, January 2020 in Nature et on Arxiv in April 2019 (6 pages).

Qutech also works on Majorana fermions and cryo-CMOS. Qutech is indeed the testing arm of Intel with its Horseridge system. All this create some synergies with their electron spin research efforts.

Germanium allows the creation of very fast quantum gates ranging from 0.5 to 5 ns<sup>528</sup>. The SOI for "silicon on insulator" is a technology from the French CEA-Leti and SOITEC. It adds a layer of silicon oxide insulator ( $\text{SiO}_2$  or "BOX" for "buried oxide") over the silicon wafers and on which are then etched transistors and other circuits conductors.



In 2020, QuTech announced that it would develop "hot" silicon qubits that could operate at around 1K. More precisely at 1.1K<sup>529</sup>. At the same time, UNSW was operating such qubits at 1.5K<sup>530</sup>.

TU Delft collaborates on germanium qubits with **Purdue University** in Indiana and **Wisconsin-Madison University**. Their ambition is to integrate millions of qubits into SiGe circuits<sup>531</sup>. In September 2020, they announced that they had created a four-qubit germanium-based silicon-quantum dots processor with bi-directional coupling (meaning... two qubit gates and entanglement), paving the way for scalability<sup>532</sup>.



**UNSW**  
SYDNEY

Australians are among the most active around silicon qubits, whether in the **CQC2T** teams at UNSW (University of New South Wales), in Michelle Simmons' **SQC** startup that grew out of it, or in other laboratories. Australian Universities are teaming up a lot with Microsoft Research.

UNSW's **CQC2T** (Center for Quantum Computing & Communication Technology) laboratory is led by Michelle Simmons. She also runs SQC, a silicon qubit startup.



UNSW is advancing CMOS qubit fidelity, quantifying the variability of qubits and their fidelity as a function of temperature. In 2019, they obtained a 2% error rate for two-qubit quantum gates and a 99.96% fidelity for one-qubit gates<sup>533</sup>.

UNSW and Purdue University in Indiana, USA (funded by Microsoft) experimented a system of phosphorus atoms integrated in a silicon substrate, the qubit states being the electron spin of the phosphorus atoms. Qubits coupling is based on connecting electric dipoles. They plan to reach 10 qubits by 2022<sup>534</sup>. UNSW received funding of \$53M from the telecom operator Telstra, the Commonwealth Bank and the governments of Australia and the New South Wales region.

<sup>528</sup> See also [Quantum control and process tomography of a semiconductor quantum dot hybrid qubit](#), 2014 (12 pages).

<sup>529</sup> See [Hot, dense and coherent: scalable quantum bits operate under practical conditions](#) by QuTech, April 2020 which refers to [Universal quantum logic in hot silicon qubits](#) by L. Petit et al, April 2020 in Nature and October 2019 in pre-print (10 pages).

<sup>530</sup> See [Hot qubits made in Sydney break one of the biggest constraints to practical quantum computers](#) by UNSW, April 2020.

<sup>531</sup> In [Silicon provides means to control quantum bits for faster algorithms](#), June 2018.

<sup>532</sup> See [A four-qubit germanium quantum processor](#) by N.W. Hendrickx et al, September 2020 (8 pages).

<sup>533</sup> See [Quantum World-First: Researchers Reveal Accuracy Of Two-Qubit Calculations In Silicon](#), May 2019.

<sup>534</sup> This is documented in [Silicon quantum processor with robust long-distance qubit couplings](#), 2017 (17 pages). This is based on the "Kane quantum computer", proposed by Bruce Kane in 1998 at UNSW.

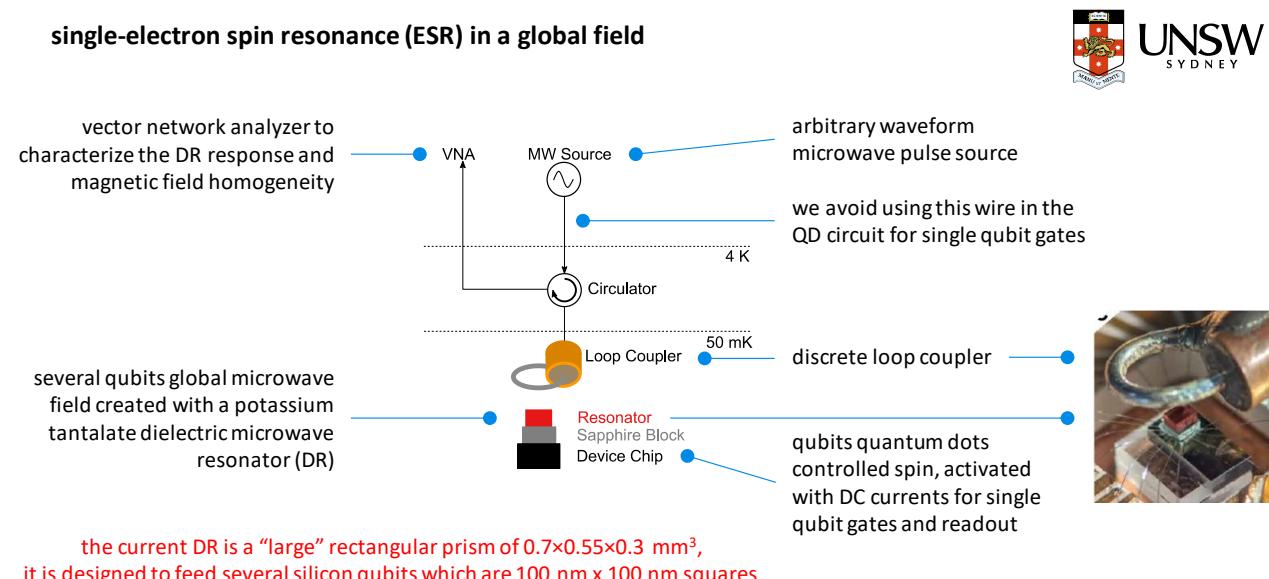
In 2020, a team from the **University of Melbourne** showed how machine learning could help calibrate the placement of phosphorus atoms in a 2D structure of qubits on a silicon substrate<sup>535</sup>.

An UNSW team proved in 2018 the feasibility of creating qubits in CMOS structures and developed protocols for reading the state of the spins of these qubits without the need for averaging via a process called "Pauli spin blockade", paving the way for error correction codes implementation and the creation of large-scale quantum computers<sup>536</sup>.

Andrea Morello's team at **CQC2T** at UNSW is studying the remote coupling of electron spins via photons in the visible or in radio waves spectrum. His team created silicon qubits exploiting the control of electron spin of intermediate layers of silicon atoms, increasing stability and reducing flip (or charge) errors<sup>537</sup>.

It also managed, by chance, to control the spin of antimony atomic nuclei with an oscillating electric field<sup>538</sup>.

A team from **UNSW** led by Andrew Dzurak found in 2021 a way to improve the scalability of spin qubits with removing some the microwave circuits within the qubit chipset and providing these microwaves to the qubits quantum dots with a dielectric microwave resonator (DR) made in potassium tantalate and activated by a discrete loop coupler, made of a simple wire<sup>539</sup>. It drives the ESR (Electron Spin Resonance) magnetic field that enables spin rotations and single qubit gates as well as spin state readout. All this saves at least two microwaves circuits in the quantum dots chipset, reducing heating and simplifying the chipset design and, potentially, qubits topology.



<sup>535</sup> See [Machine learning to scale up the quantum computer](#) by Muhammad Usman and Lloyd Hollenberg, University of Melbourne, March 2020. Also seen in [To Tune Up Your Quantum Computer, Better Call an AI Mechanic](#) by NIST associated with UNSW, March 2020.

<sup>536</sup> See [Tests show integrated quantum chip operations possible](#), October 2018.

<sup>537</sup> See [UNSW use flat electron shells from artificial atoms as qubits](#) by Chris Duckett, February 2020 and [Engineers Just Built an Impressively Stable Quantum Silicon Chip From Artificial Atoms](#) by Michelle Starr, February 2020 which refers to [Coherent spin control of s-, p-, d- and f-electrons in a silicon quantum dot](#) by Andrea Morello et al, 2020 (7 pages).

<sup>538</sup> See [Engineers crack 58-year-old puzzle on way to quantum breakthrough](#) by UNSW, March 2020 and [Chance discovery brings quantum computing using standard microchips a step closer](#) by Adrian Cho, March 2020.

<sup>539</sup> See [Single-electron spin resonance in a nanoelectronic device using a global field](#) by Ensar Vahapoglu, Andrew S. Dzurak et al, August 2021 (7 pages) and [Supplemental Materials](#) (12 pages).

The global magnetic field generated by this system comes from a dielectric microwave resonator of  $0.7 \times 0.55 \times 0.3$  mm and the discrete loop coupler is even larger, while quantum spin qubits can scale down as low as 100 nm  $\times$  100 nm. The team communicates on this technology as one that could enable scaling quantum dots to million qubits. So how are individual qubits controlled? Individual spin control and readout is activated by some classical direct current tension sent to each quantum dots in the qubit chipset, replacing the usual microwave signals sent and reflected in the chipset. The next step is to implement the qubit circuit on isotopically purified  $^{28}\text{Si}$  and check qubits coherence.

While the solution simplifies the qubit chipset wiring for some of the microwave lines, the prototype is based on using external microwave generators and readout systems, which doesn't scale at all. It circles back to a cryo-CMOS component that was developed by another Australian team and with Microsoft, which we describe in the [cryo-CMOS section](#), page 385.



**Silicon Quantum Computing** or SQC (2017, Australia, \$66M) is a spin-off from UNSW and CQC2T launched by Michelle Simmons. It wants to produce a 10-qubit demonstrator by 2022. The company recruited John Martinis from Google at the end of September 2020.

However, it doesn't seem John Martinis considered this as a long-term assignment.

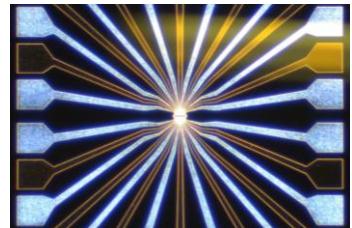
They trap phosphorus atoms on a silicon substrate. Their qubit is made with controlling the spin of the phosphorus atom qubit. They create two-qubit gates with two phosphorus atoms that are a few nanometers apart, using quantum tunneling. They also achieve a very good fidelity, of about 99.99% and two-qubit gates speed of less than one nanosecond<sup>540</sup>.

Other Australian teams are working on spin qubits operating at room temperature, an interesting Holy Grail to pursue as long as all the components actually work at room temperature.



**Archer** (Australia) made headlines in April 2020 by suspending its stock market listing at the time of the announcement of a new manufacturing deal for their component called  $^{12}\text{CQ}$ .

It is based on carbon nanospheres and can operate at room temperature<sup>541</sup>. The 12 does not correspond to the number of qubits of the chipset (which is not specified) but to the isotopic weight of the zero spin carbon used to create these nanospheres.  $^{12}\text{CQ}$  has been invented by Mohammad Choucair. Archer's Quantum Technology Manager Martin Fuechsle has contributed to the development of the single electron transistor and worked at UNSW with Michelle Simmons.



The company seems to be overselling the state of progress of its component which is not really characterized, especially on a large scale. They talk about room temperature operation for qubits with a relaxation time (= coherence time) of 175 ns at 300K. This doesn't seem suited to the execution of a significant number of quantum gates to say the least! In April 2021, Archer Materials announced it would sell off all its mineral traditional business to iTech Minerals, to focus on quantum technologies. So a least, they are betting the farm on quantum computing.

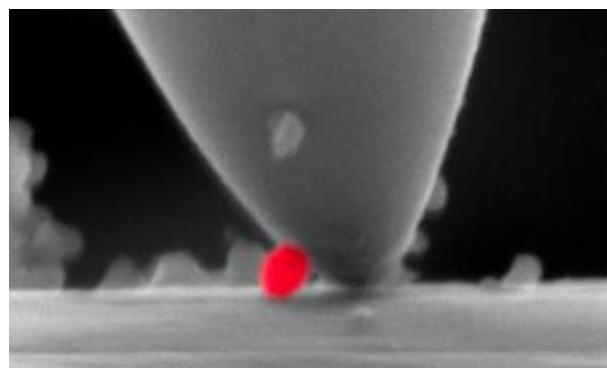
---

<sup>540</sup> See [Exploiting a Single-Crystal Environment to Minimize the Charge Noise on Qubits in Silicon](#) by Ludwik Kranz, Michelle Simmons et al, 2020 and [A two-qubit gate between phosphorus donor electrons in silicon](#) by Y. He, Michelle Simmons et al, 2019.

<sup>541</sup> See [Archer Materials granted trading halt ahead of quantum computing chip agreement](#) by Quantum Analyst, 2020 and [Room temperature manipulation of long lifetime spins in metallic-like carbon nanospheres](#) by Bálint Náfrádi, 2016 (32 pages) which describes in detail this technique of electron spin trapping in a carbon nanosphere. It reminds us of the nanotubes of the French startup C12. Archer says it's partnering with IBM. Since IBM is not ready to give up on superconducting qubits, it seems interested in having Archer adopt its Qiskit software platform, a bit like what IonQ has also announced in 2021.

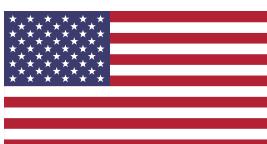
In July 2021, they announced that they were embedding some parts of their qubits control electronics in the qubit chipset, that records the Continuous Wave Electron Spin Resonance (cwESR) signals generated by a superconducting on-chip resonator.

In February 2021, Archer announced that they had achieved electronic transport in a single qubit at room temperature in its  $^{12}\text{C}$  quantum computing qubit processor chip (in red, in the picture, the large device being an electric probe). It however does not mean that this is a fully functional qubits that can be operated with quantum gates.



In December 2020, Archer also launched a partnership with **Max Kelsen**, another Australian company, specialized in QML software development.

Max Kelsen and Archer will develop QML algorithms based on Qiskit, eying a future execution on Archer's processor.



In the USA, on top of Intel, several research labs are working on electron spin qubits. Let's factor in **Sandia Labs**, a research laboratory of the US Department of Energy (DoE) with sites in New Mexico and California.

They work on the physics of silicon qubits and their error correction codes.

They are targeting an operating temperature of 100 mK.

*Opposite*, their qubit architecture based on a commonplace double silicon quantum dots ([source](#)).

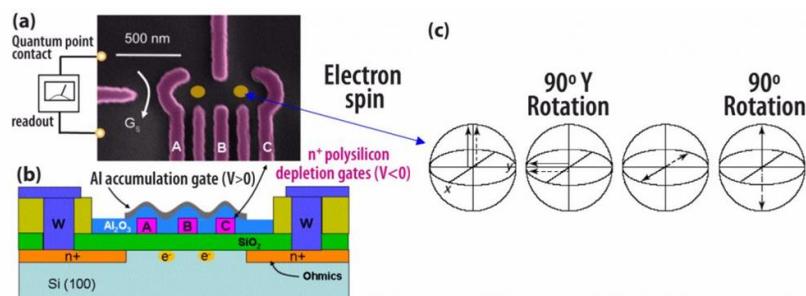


Figure 1: (a) scanning electron microscope image of Sandia's dual quantum dot structure fabricated in silicon (the dots suggest the approximate location of the electron position); (b) schematic cross section of the quantum dot structure showing the position of the single electron locations; and (c) schematic representation of spin manipulation using rotation and precession of two different spins.

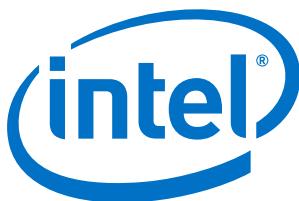
**Princeton University** and Jason Petta's team are working on the realization of a two-qubit silicon CNOT gate with a very high level of reliability and low operating time, respectively 200ns and 99%<sup>542</sup>. These are also double quantum dots qubits using silicon and germanium. In October 2018, this Princeton team had succeeded in monitoring the state of its CMOS qubits with light and exploiting a microwave field to exchange a quantum between an electron and a photon<sup>543</sup>.

Laboratories at **HRL Malibu**, a joint research subsidiary of Boeing and General Motors, located in California, and **Nokia Bell Labs** are working on gallium arsenide qubits that require cooling to less than 1K. These would be qubits with long coherence times.

<sup>542</sup> Seen in [Quantum CNOT Gate for Spins in Silicon](#), 2017 (27 pages).

<sup>543</sup> See [How old-school silicon could bring quantum computers to the masses](#), October 2018 and [In leap for quantum computing, silicon quantum bits establish a long-distance relationship](#) by University of Princeton, December 2019.

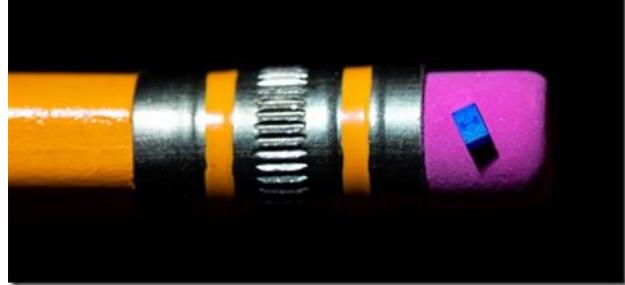
A team of researchers from Hungary, Sweden, Russia and the DoE **Argonne National Laboratory** published in 2019 work on the creation of qubits operating at room temperature and based on defects in silicon carbide (SiC) that are somewhat reminiscent of NV Centers<sup>544</sup>.



In addition to superconducting qubits, **Intel** is mostly working on silicon qubits. They produced a wafer with 26 qubit chipsets in 2017 and made some progress since they, although it is hard to evaluate.

Intel's quantum work is managed under the direction of **Anne Matsuura**<sup>545</sup> and **James Clark** for hardware.

In June 2018, Intel made another announcement with a highly integrated chip using this CMOS technology, which is supposed to be able to count up to 1500 qubits (*opposite*). It is fabricated in the D1D fab located in Portland, Oregon, with an etch density of 50 nm, six times greater than the early 2018 generation. But it was no characterized.



QuTech and Intel work well together on these qubits. QuTech got a \$50M investment from Intel in 2015 to explore it.

Intel announced in 2018 that it had succeeded in controlling a two-qubit CMOS processor with single and double interleaved quantum gate management running Deutsch-Jozsa and Grover algorithms on a very small scale. These silicon and germanium qubits manufactured by Intel were tested by the Vandersypen Laboratory at the University of Delft, part of QuTech<sup>546</sup>. Since 2018, Intel has kept a rather low profile on its silicon qubit advances<sup>547</sup>.

At the beginning of 2020, Intel announced that it had developed with QuTech the **Horse Ridge** cryo-component. It is a CMOS component operating at 4K that is used to generate the microwaves used to drive both superconducting and silicon qubits. A second version was announced in 2021.



**equal1.labs** (2017, Ireland/USA, 6M€) is creating a charge electron spin qubits chipset manufactured in 22 nm FD-SOI technology at Global Foundries in Dresden, Germany.

They announced in 2021 a 422 qubits test chipset embedded in a full-rack system with its cryogeny, Alice mk1. At this stage, they are just able to inject single electrons in their quantum dots and simulate numerically some one- and two-qubit quantum gates, but not much more<sup>548</sup>. Their next generation Aquarius is to fit in a desktop packaging, planned for 2022, and is to house one million qubits. They position their systems to run quantum neural networks for imaging applications.

<sup>544</sup> See [Scientists Find Yet Another Way to Get Qubits Working at Room Temperature](#) by David Nield, March 2020 and [Novel Qubit Design Could Lead to Quantum Computers That Work at Room Temperature](#) by Matt Swayne, March 2020 which references [Quantum well stabilized point defect spin qubits](#) by Viktor Ivády et al, May 2019 (20 pages).

<sup>545</sup> See [Intel's quantum efforts tied to next-gen materials applications](#), January 2019 and [Intel's spin on qubits and quantum manufacturability](#), both from Nicole Hemsoth, November 2018 and [Leading the evolution of compute](#), Anne Matsuura, June 2018 (26 slides).

<sup>546</sup> See [A programmable two-qubit quantum processor in silicon](#) by T F Watson et al, TU Delft, May 2018 (22 pages).

<sup>547</sup> See, however, [What Intel Is Planning for The Future of Quantum Computing: Hot Qubits, Cold Control Chips, and Rapid Testing](#) by Samuel Moore, August 2020, which provides a rather pedagogical overview of Intel's approach to silicon qubits.

<sup>548</sup> See [A Single-Electron Injection Device for CMOS Charge Qubits Implemented in 22-nm FD-SOI](#) by Imran Bashir, Elena Blokhina et al, 2020 (4 pages).

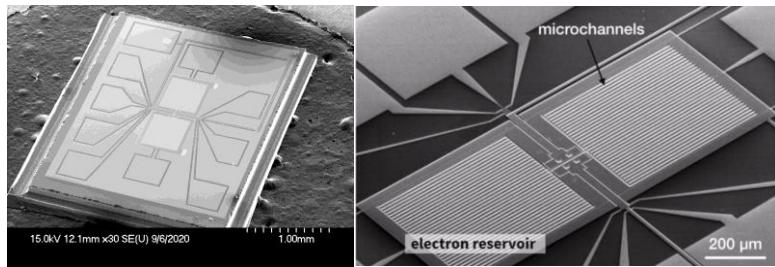
In May 2021, equal1 uncovered a prototype chipset operating at 3.7K and including 10 million transistors handling qubits controls and readout with arbitrary waves generation (AWGs), all coupled to an external FPGA, as well as some classical cryogenic memory. There's a caveat with their coherence time being only 150 ns. Equal1 also designs its own cryogenic system.

The company was created by Dirk Leipold, Mike Asker and Bogdan Staszewski from the University of Dublin. Elena Blokhina is their CTO and expect to raise \$50M by 2022.



**EeroQ** (2016, USA) develops an exotic quantum processor using trapped (and more or less flying/moving) electrons on superfluid helium. The startup was created by [Johannes Pollanen](#) from the University of Michigan, Nick Farina and Faye Wattleton.

In May 2021, they appointed Princeton University Professor Steve Lyon as CTO. It has benefited from US public (NSF) and private funding. Johannes Pollanen's bio indicates that he conducted research in superconducting and two-dimensional qubits (silicon, graphene)<sup>549</sup>.



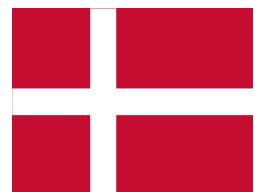
They want to associate the long coherence and high connectivity of trapped ions and the fast gates of electron spin and superconducting qubits. The chipset is built using CMOS technology.



In **China**, all the technological avenues of quantum computers are being explored in parallel, and silicon qubits are no exception. However, their work is difficult to evaluate and they don't publish much on this type of qubits compared to photon-based qubits, boson sampling and superconducting qubits<sup>550</sup>.



In Japan, a **RIKEN** team was able to measure the state of silicon qubits without altering it. This non-destructive measurement uses an Ising interaction model based on ferromagnetism that evaluates the spin of atoms neighboring the atom containing the qubit spin electron<sup>551</sup>. Sounds interesting but surely has some limitations yet to be discovered.



**Niels Bohr Institute** and **CEA-Leti** collaborated to build a 2x2 matrix silicon qubits using single electrons quantum dots. These were fabricated on a classical 300 mm SOI wafer coming out of the CEA-Leti fab in Grenoble. While not being operational qubits, these quantum dots electrons were controllable with voltage pulses bases gates. They also implemented electron swaps, that could be useful in optimizing SWAP gates in future systems<sup>552</sup>.

<sup>549</sup> See [Integrating superfluids with superconducting qubit systems](#) by Johannes Pollanen et al, 2019 (11 pages).

<sup>550</sup> See [Semiconductor quantum computation](#) by Xin Zhang Hai-Ou Li et al, December 2018 (23 pages). The document provides an overview of CMOS quantum technology but does not specify the specific contribution of Chinese research laboratories.

<sup>551</sup> See [Scientists succeed in measuring electron spin qubit without demolishing it](#), RIKEN, March 2020, mentioning [Quantum non-demolition readout of an electron spin in silicon](#) by J. Yoneda et al, 2020 (7 pages).

<sup>552</sup> See [Single-electron operations in a foundry-fabricated array of quantum dots](#) by Fabio Ansaloni, Benoit Bertrand, Louis Hutin, Maud Vinet et al, December 2020 (7 pages).



In Germany, at the **University of Aachen**, researchers created double quantum dots of silicon with graphene<sup>553</sup>.



The **UK** is another active country on silicon qubits, particularly in **Oxford University, Cambridge University and UCL**.



**QUANTUM MOTION**

**Quantum Motion Technologies** (2017, UK, \$9.7M) is an Oxford University spin-off that wants to create high-density silicon quantum computers. They have received unspecified seed funding from the UK fund Parkwalk Advisors in 2017.

The startup co-founded by John Morton (UCL) and Simon Benjamin (Oxford University) wants to industrialize a process created by Joe O'Gorman's team at Oxford University, which consists of clearly separating silicon qubits and their measurement.

Measurement was supposed to be carried out with a magnetic probe mechanically moved on the surface and making "square" movements, guided by a MEMS (micro-electro-mechanical device). This probe system was designed to avoid the use of control electronics and allow a better separation between the qubits<sup>554</sup>.

A data rate separation process with intermediate mediation rates was limiting leakage effects<sup>555</sup>. This process protected by one validated US patent and four patents pending. But it seems that this technology is finally not the one they will implement!

In January 2021, Quantum Motion presented with Hitachi Cambridge, University of Cambridge and EPFL a 50 mK cryo-CMOS including quantum dots qubit arrays, row-column control electronics lines and analog LC resonators for multiplexed readout, using 6-8 GHz microwave resonators. This was a first step to implement time- and frequency-domain multiplexing scalable qubits readout<sup>556</sup>.

In March 2021, Quantum Motion announced a record of stability of 9 seconds for an isolated silicon qubit. The chipsets were manufactured by CEA-Leti in Grenoble and the French team led by Maud Vinet coauthored the paper associated with this performance<sup>557</sup>. Quantum Motion and UCL are part of the Quantum Flagship QLSI on silicon qubit that is led by Maud Vinet. So, this explains that.

Their roadmap consists of producing 5 qubit "small cells" by 2022 in a structure that could then be reproduced in matrix patterns. They believe they can create a quantum computer with 100 logical qubits by 2029, a classical milestone for most quantum computer vendors.

---

<sup>553</sup> See [Bilayer graphene double quantum dots tune in for single-electron control](#) by Anna Demming, March 2020.

<sup>554</sup> See [A silicon-based surface code quantum computer](#) by Joe O'Gorman et al, 2015 (14 pages). The paper is co-authored by John Motin and Simon Benjamin who are two co-founders of the startup Quantum Motion Technologies.

<sup>555</sup> See [A Silicon Surface Code Architecture Resilient Against Leakage Errors](#) by Zhenyu Cai (Quantum Motion Technologies) et al, April 2018 (19 pages).

<sup>556</sup> See [Integrated multiplexed microwave readout of silicon quantum dots in a cryogenic CMOS chip](#) by A. Ruffino, January 2021 (14 pages).

<sup>557</sup> See [Spin Readout of a CMOS Quantum Dot by Gate Reflectometry and Spin-Dependent Tunneling](#), by Virginia N. Ciriano-Tejel, Maud Vinet, John Morton et al, 2021 (18 pages). This followed [Remote capacitive sensing in two-dimensional quantum-dot arrays](#) by Jingyu Duan, Michael A. Fogarty, James Williams, Louis Hutin, Maud Vinet and John J. L. Morton, 2020 (31 pages) which described the coupling technique using silicon nanowires (SiNW) to measure qubits spins with remote capacitive charge sensing.

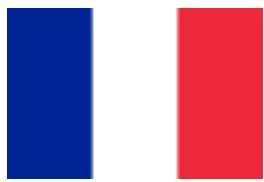
**SPIN** (Spin Qubits in Silicon) is an electron spin qubits project launched in December 2019 by the Swiss National Science Foundation with a funding of \$18M.

The end goal is to create a scalable universal quantum computer with more than a thousand logical qubits. The project led by the University of Basel also gathers researchers from ETH Zurich, EPFL and IBM Research Zurich. It looks like a “Plan B” for IBM who is so far focused on superconducting qubits.



The European collaborative project **Mos-quito** brought together European research laboratories working on silicon qubits manufactured in CMOS technology on 300 mm wafers by CEA-Leti. In addition to CEA-Leti, the United Kingdom (London UCL, Cambridge University), Switzerland (EPFL), Finland, Denmark and Italy (IMM) are also involved.

This three-year project funded by the European Union is now completed. One of the objectives was to study the performance of different types of individual qubits based on spin in silicon to provide recommendations for their large-scale implementation. It's been followed-up with the European Flagship QLSI project.



CEA-Leti in Grenoble is Europe's leading laboratory for applied research on electron spin qubits and, more importantly, their fabrication. The team is led by **Maud Vinet**. The laboratory is at the heart of a quantum research ecosystem that includes the CNRS with the Institut Néel, the IRIG of the CEA and the University Grenoble Alpes.

Their overarching objective is to create highly integrated and scalable silicon qubits. The first qubits in CMOS technology were produced in 2016.

**Multidisciplinary approach** is the motto at Grenoble, which is quite rare in research, with a nice panel of researchers. This Grenoble-based team proposes to draw on Leti's technological capabilities, IRIG's knowledge of the quantum properties of silicon nanostructures, and Néel's spin manipulation expertise to go beyond the state of the art in both the quality and number of qubits. Not to mention Néel's expertise in theoretical physics, whether in quantum thermodynamics (Alexia Auffèves) or cryogenics. On the other hand, a more upstream research on spin manipulation in molecular magnets and in III-V semiconductors allows them in parallel to accumulate fundamental knowledge on spin properties and to develop advance microwave related electronics.

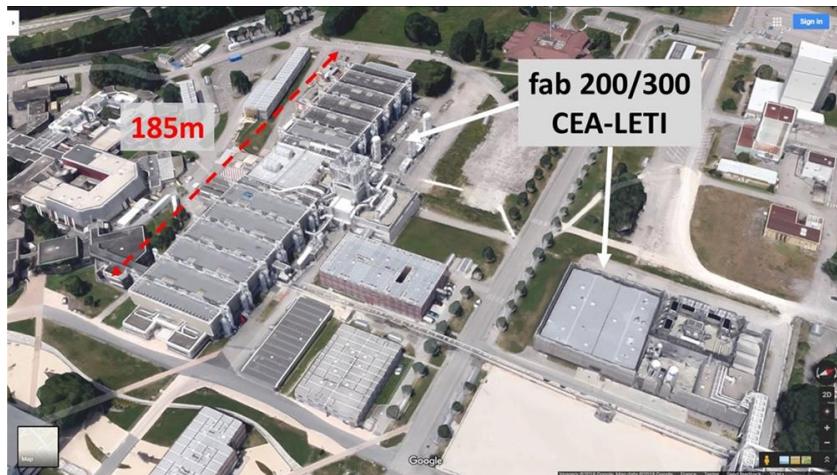
**Manufacturing capacity** with CEA-Leti being one of the few public laboratories in the world with a CMOS component test production platform. It includes all the tools required to produce 200 and 300 mm wafers. It allows the production of all kinds of components in silicon, germanium and III-V materials (photonics, gallium arsenide, gallium nitride, etc.).

The clean room includes lithography machines, notably from ASML, with a density going down to 20 nm, machines for the deposition of semiconducting and conducting materials using all techniques (plasma, CVD, MOCVD, ...) as well as for the addition of MEMS devices (micro-electro-mechanical systems). The clean rooms are spread over several buildings.

The main one is 185 m long (*below*) on 8000 m<sup>2</sup><sup>558</sup>. The use of this room requires however to have experimented the manufacturing process upstream, as the CNRS laboratories and Renatech network do.

---

<sup>558</sup> Other research clean rooms exist in France: the C2N clean room in Palaiseau, the IEF in Orsay, the Thales TRT clean room in Palaiseau, the IEMN clean room in Lille, Femto-ST clean room in Besançon and the Laas clean room in Toulouse. In production are mainly the fab 200 and 300 at STMicroelectronics in Crolles, near Grenoble. Some of these laboratories are associated in the National Network of Large Technology Plants (Renatech). They make their platforms available to companies in project and contract mode.



The CMOS qubits manufacturing process uses 300 mm SOI (silicon on insulator, with a silicon oxide insulator) wafers on which a thin layer of 99.992% purified 28-isotope silicon is deposited<sup>559</sup>.

The validated production would be transferred to volume production in commercial fabs such as those from STMicroelectronics, Global Foundries or Samsung that support the FD-SOI processes. However, in its early stages, the size of the quantum computer market will be modest. In a conventional batch of 25 wafers alone, you can produce several thousand quantum chips in a single run, enough to power a large base of quantum supercomputers. But industry-grade clean room ensure quality processes that are not necessarily found in pre-production clean rooms.

**Nanocharacterization** with a platform (PFNC or NanoCarac) that includes dozens of sensing tools over 2,500 m<sup>2</sup>. It is used to check the quality of the manufactured components. Leti's double clean room has about a billion euros worth of equipment with machines costing from a few million to 80M€! In Europe, equivalent platforms are rare. One of them is **IMEC** in Leuven, Belgium, and is a partner of CEA-Leti.

**Staging progress** with the Grenoble team expecting to progress in stages over a six-year period starting in 2019: demonstration of a two-qubit silicon-based gate, demonstration of quantum simulation in a 4x4 array based on III-V material, demonstration six qubits in silicon, development of error correction codes and adapted algorithms, and fabrication of 100 2D array qubits in silicon at the end of this journey.

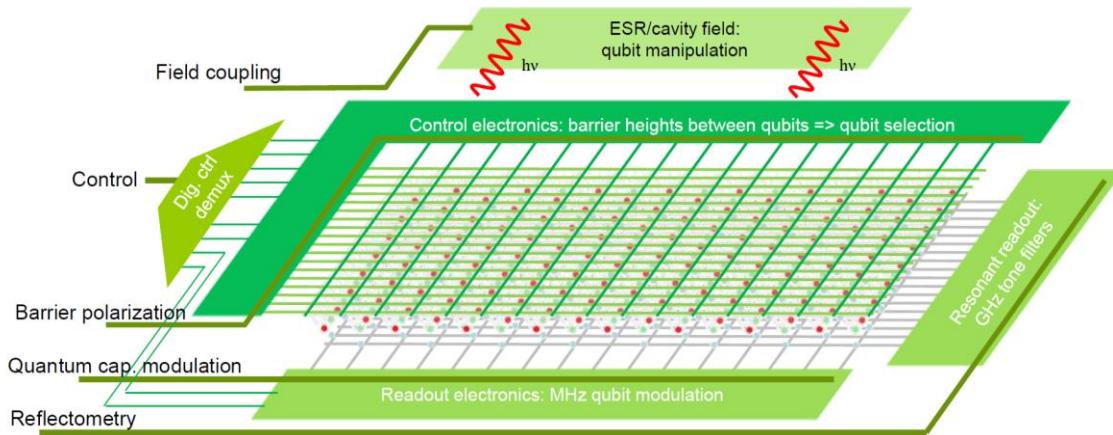
**Control electronics** with the Grenoble team creating control electronics operating at cryogenic temperature. The 2D architecture of Leti's CMOS chipsets comprises several layers with silicon qubits and then the integrated electronics for control and state measurement. The qubits are distributed in 2D, but the integration of the components is also vertical within the components. The measurement layer is located below the qubits while the layer for activating the qubits with quantum gates is above.

For  $N^2$  qubits, they would need  $2N$  control lines (horizontal, vertical) instead of  $2N^2$ , which would generate an appreciable gain in connectivity. The technique would work to generate one- and two-qubit quantum gates<sup>560</sup>.

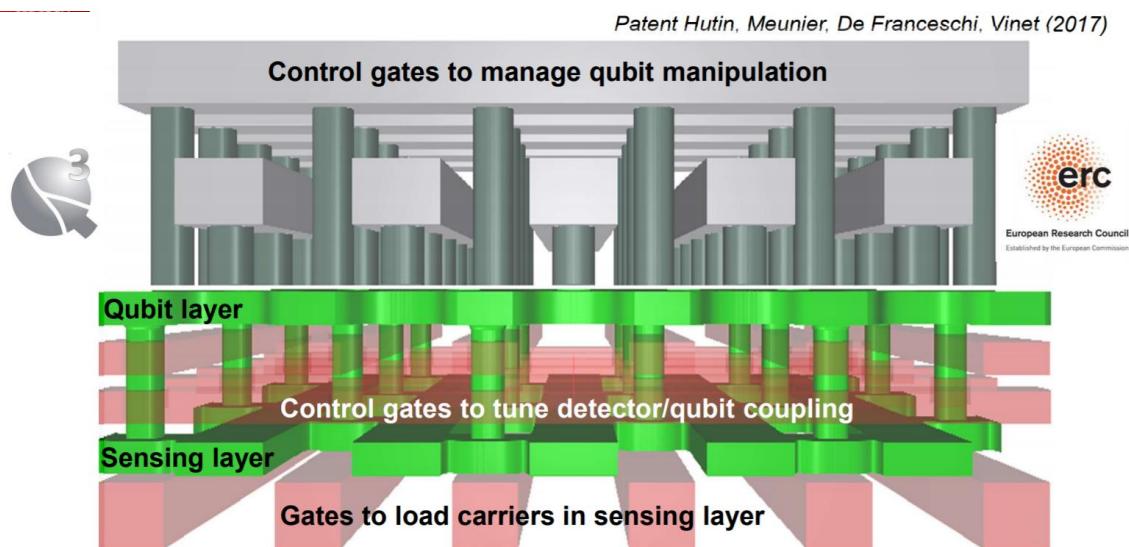
---

<sup>559</sup> The first test of spin control with isotopically purified silicon was achieved in 2011. See [Electron spin coherence exceeding seconds in purified silicon](#) by Alexei Tyryshkin, Kohei Itoh, John Morton et al, 2011 (18 pages).

<sup>560</sup> The technique is described in [Towards scalable silicon quantum computing](#) by Matias Urdampilleta, Maud Vinet, Tristan Meunier, Yvain Thonnart et al, 2020 (4 pages) as well as in the presentation [Silicon Based Quantum Computing](#), Maud Vinet 2018 (28 slides) from where the green schema comes from.



The great challenge of these architectures is their variability, i.e. the differences in behavior from one qubit to another and from one circuit to another. This leads to a need for precise calibration, qubit by qubit, of the microwaves controlling and reading the state of the qubits. As for superconducting qubits, this calibration can be done using dedicated machine learning software.



They use superconducting materials for the metal layer of these circuits, based on titanium nitride. This provides low resistance and reduces the noise of qubit state measurement.

**3D stacking** is used to arrange chipsets components in 3D ([details](#)), which can help solve various scalability problems. CEA-Leti is using it **CoolCube** technology. The reference publications of these teams on CMOS qubits are numerous<sup>561</sup>.

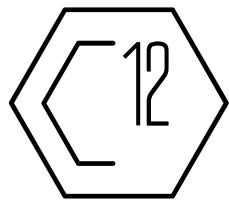
**Spin-photon coupling** could be used to create a communication link between remote qubits. At the Néel Institute, the aim is to move electron spins over long-distances ("Long-distance coherent spin shuttling"). Here, a long-distance means 5  $\mu\text{m}$ ! But it makes enough to link qubits together, so it's worth it<sup>562</sup>.

<sup>561</sup> These include [A CMOS silicon spin qubit](#), 2016 (12 pages) which defines the basis of double quantum dot CMOS qubit, [SOI technology for quantum information processing](#), 2016 which completes this description as well as [Conditional Dispersive Readout of a CMOS Single-Electron Memory Cell](#) by Simon Schaal et al, 2019 (9 pages) which describes, in the framework of a partnership with the University of London, the work on reading the state of a CMOS quantum dot. And then [Towards scalable silicon quantum computing](#) by Maud Vinet et al, 2018 (4 pages).

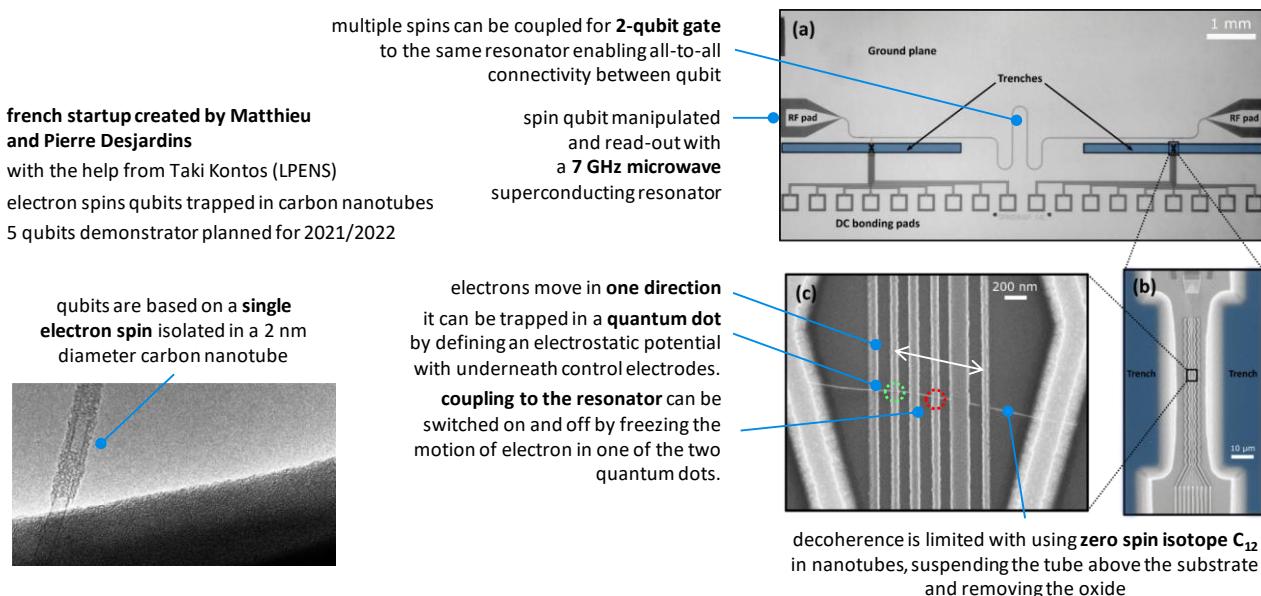
<sup>562</sup> See [Coherent long-distance displacement of individual electron spins](#), 2017 (27 pages) and [Quantum Silicon Grenoble, the project on which the Fortezza report relies for a quantum computer made in France](#) by Manuel Moragues, January 2020.

In October 2018, the Grenoble-based team of Silvano De Franceschi (INAC, CEA), Tristan Meunier (Institut Néel, CNRS) and Maud Vinet (CEA-Leti) obtained a €14M ERC Synergy Grant for their QuQube project, which is spread over 6 years to produce a 100-qubit electron spin CMOS quantum processor<sup>563</sup>.

Since March 2020, the Grenoble team is also coordinating the 4-year European Quantum Flagship project QLSI which was formally launched in February 2021<sup>564</sup>. It consolidates fundamental research in silicon qubits and brings together CEA, CNRS Institut Néel, Atos, SOITEC and STMicroelectronics for France, IMEC (Belgium), Quantum Motion and UCL (UK), Infineon, IHP, U Konstanz, Fraunhofer and RWTH Aachen (Germany), UCPH (Denmark), TU Delft, U Twente and TNO (Netherlands) and U Basel (Switzerland). With a budget of 15M€ to be shared between all these entities, the objective is to enable the manufacture and testing of 16 silicon qubits with gate fidelity of over 99%, and the preparation of a roadmap to be able to scale beyond a thousand qubits.



**C12 Quantum Electronics** (2020, France, \$10M) was launched by Matthieu Desjardins and his twin brother Pierre. It is a project originating from the LPENS at ENS Paris and 15 years of research from Takis Kontos in this lab, with contributions from Jérémie Vienot at Institut Néel Grenoble. Their goal is to use carbon nanotubes to trap electrons used in electron spin qubits and build the surrounding control circuitry on silicon substrate.



This technology can improve qubits isolation and coherence time by a factor of 100, up to one second, while keeping a strong coupling for fast qubit manipulation. The qubits are controlled by spin-photon coupling in the microwave regime, using frequency multiplexing to avoid cross-talk. Qubit readout uses spin to charge coupling with a single charge coupling with 8 qubits<sup>565</sup>. The challenges sit in materials, design, control electronics, connectivity, topology and error correction codes.

<sup>563</sup> See [An ERC Synergy Grant for Grenoble research on quantum technologies](#), October 2018 (6 pages). A European Research Council Synergy Grand funds "moonshots" in European research involving at least two research laboratories. 14M€ is the maximum funding for such projects. 10M€ of core funding and 4M€ which can fund heavy investments or access to large infrastructures.

<sup>564</sup> See [New EU Quantum Flagship consortium launches a project on silicon spin qubits as a platform for large-scale quantum computing](#), February 2021.

<sup>565</sup> A related technique is described in [Charge Detection in an Array of CMOS Quantum Dots](#) by Emmanuel Chanrion, Pierre-André Mortemousque, Louis Hulin, Silvano de Franceschi, Franck Balestro, Maud Vinet, Tristan Meunier, Matias Urdampilleta et al, Grenoble CEA-LETI, CNRS Institut Néel and UGA, August 2020 (8 pages).

The nanotubes are mechanically integrated into the circuit at the end of the manufacturing process<sup>566</sup>. The carbon nanotubes are grown by C12 using a CVD process (chemical vapor deposition). The connection between two qubits is based on microwave cavities, exploiting QEDC (Quantum Electrodynamic Cavity). Of course, there are still many challenges to develop this kind of qubits but it is worth exploring. It could even have some use cases beyond computing, in quantum sensing.

Atos works with C12 to develop its quantum compiler, to create digital simulation models of its qubits and for co-designing quantum gates.



**Qpi** (2019, India) is a QML software and hardware development company, providing the QpiAI library. They are working on creating the ASGP (AI System Generating Processor), a hybrid classical-quantum compute chip.

Practically speaking, they plan first to introduce a qubit control chip in September 2021 operating at 4K and designed in a 22 nm TSMC CMOS process<sup>567</sup>. This chipset is to control the microwaves sent to both superconducting and electron spin qubits processors. They plan later to create a one million electron spin quantum dots qubits processor. Overselling seems not to be an issue for them.

## NV centers qubits

This qubit technology is based on the control of electron spins trapped in artificial defects of crystalline carbon structures in which one carbon atom is replaced by one nitrogen atom and another carbon atom is replaced by a void, gap or cavity<sup>568</sup>.

The cavity contains a free electron that is generated by an electrical voltage applied to an n-p junction obtained by doping the diamond.

The free electron is coupled to another one from the nitrogen atom near the cavity. The cavity includes two other pairs of electrons from the nitrogen atom in the cavity, with a total zero spin.

The process involves controlling the collective spin of these two free electrons as well as the spin of the nitrogen nucleus of the cavity and possibly of the neighboring <sup>13</sup>C carbon atoms<sup>569</sup>. The cumulative spin of the two electrons of the cavity is 0, 1 or -1 because it adds two electron spins that are from  $\frac{1}{2}$  or  $-\frac{1}{2}$ . This electron spin is controlled by a combination of microwave and magnetic field. Commonly used NV centers are called NV<sup>-</sup> because of the addition of an external electron into the cavity. NV centers without this electron are not commonly used.

Here is a diagram that describes what a NV center can look like in practice considering that there are many different implementations, knowing that NV centers are used not only for computing but, in a dominant manner, in quantum sensing.

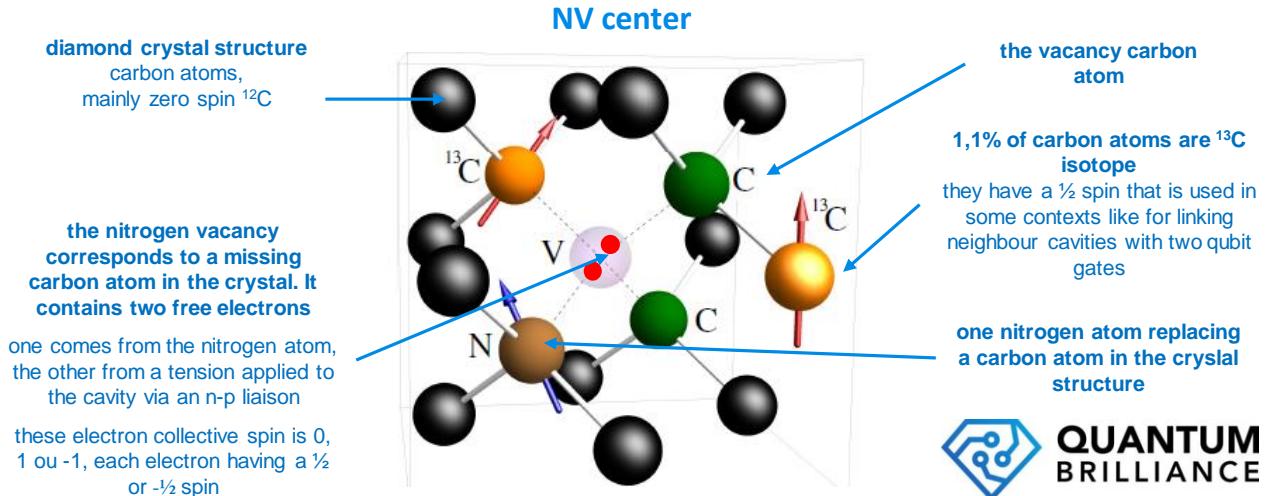
---

<sup>566</sup> It is described in [Nanoassembly technique of carbon nanotubes for hybrid circuit-QED](#) by Tino Cubaynes, Matthieu Desjardin, Audrey Cottet, Taki Kontos et al, September 2021 (6 pages).

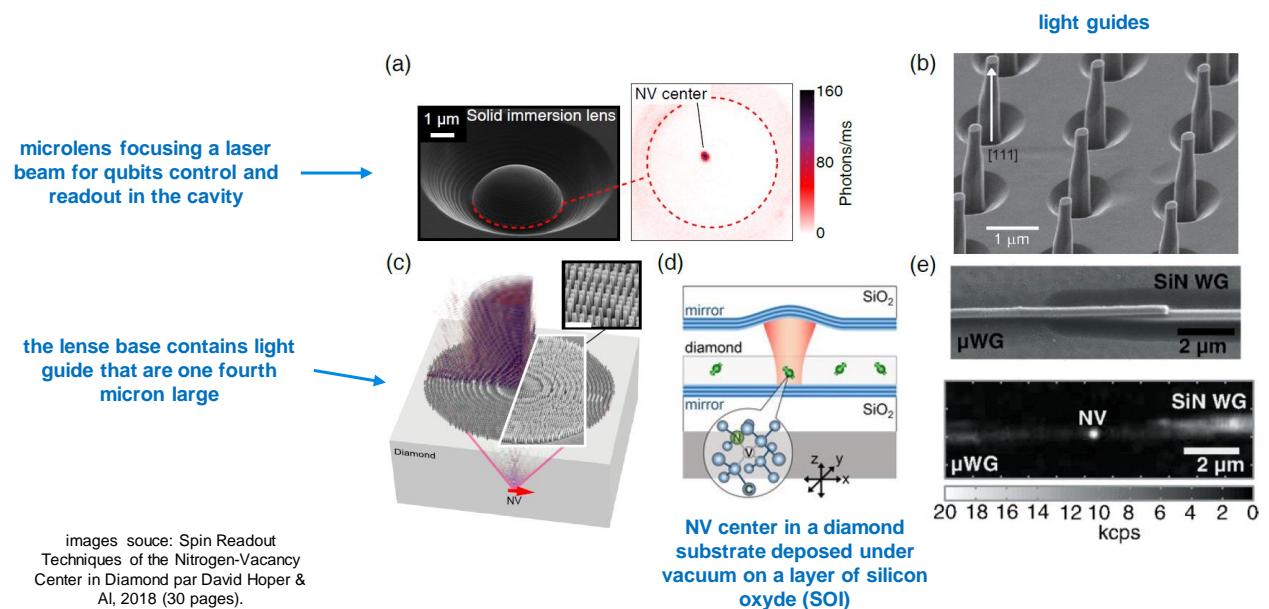
<sup>567</sup> Source: [QpiAI in Partnership With IISc Launches Joint Certification for AI and Quantum Computing to Upskill Enterprises, Schools and Colleges](#), March 2021.

<sup>568</sup> Other similar techniques are investigated with using silicon instead of carbon, and carbon instead of nitrogen. See [Single artificial atoms in silicon emitting at telecom wavelengths](#) by W. Redjem et al, 2020 (4 pages).

<sup>569</sup> Approximately 1.1% of the carbon atoms in diamond are of the <sup>13</sup>C isotope. The most common isotope is <sup>12</sup>C. <sup>14</sup>C is present in trace amounts and is used to date carbonaceous objects due to its half-life of 5730 years. See [Coherent control of an NV- center with one adjacent <sup>13</sup>C](#) by Burkhard Scharfenberger et al, 2014 (24 pages).



NV centers can be integrated in circuits fabricated on an SOI silicon wafer with a layer of  $\text{SiO}_2$  insulator. It is covered with a matrix Fresnel lens, used to focus a control and readout laser<sup>570</sup>.



Next is a diagram explaining how these rather complex qubits operate with the various energy levels and transitions of the cavity and its free electrons using microwaves and red/green photons. The vertical arrows represent useful energy transitions<sup>571</sup>.

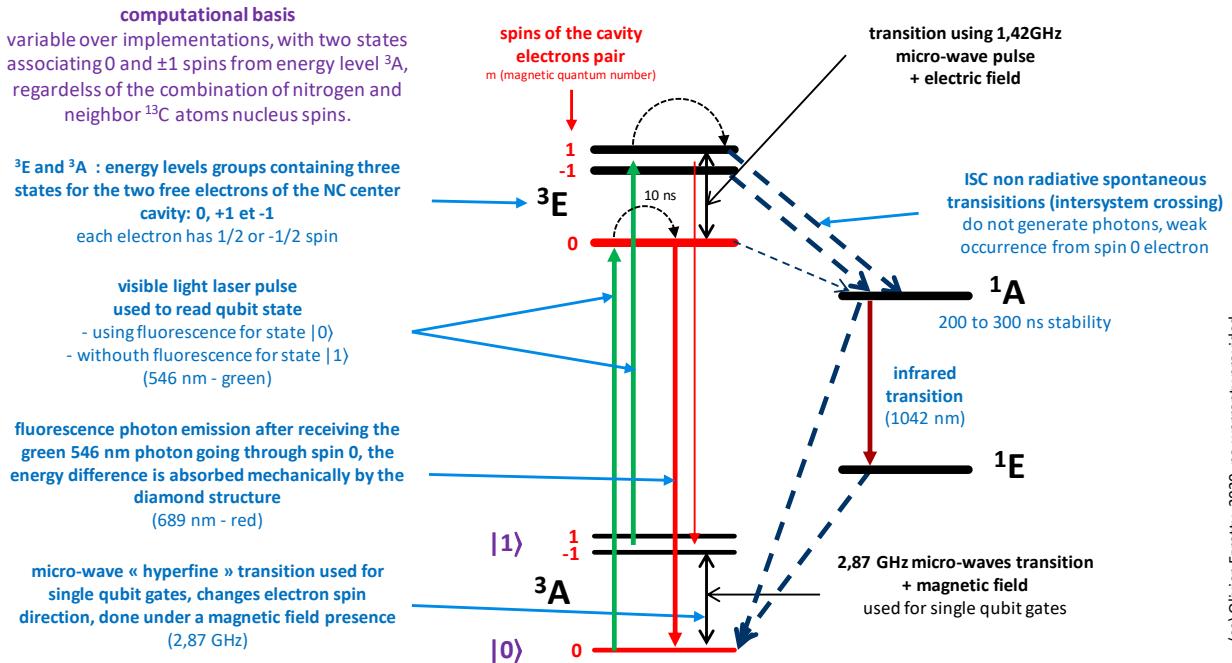
An incoming photon from a laser generates:

- Either a change of state which then degenerates via the  $^1\text{A}$  state into a spontaneous non-radiative transition which does not emit a photon but transmits some mechanical energy to the crystal structure and returns to the basic state  $|0\rangle$ .
- Or an emission of a photon of lower energy in the red, part of the energy being also mechanically absorbed by the diamond structure. The presence or absence of these red photons makes it possible to identify the state of the qubit at  $|0\rangle$  (red photon) or  $|1\rangle$  (no red photon).

<sup>570</sup> See [Spin Readout Techniques of the Nitrogen-Vacancy Center in Diamond](#) by David Hoper et al, 2018 (30 pages).

<sup>571</sup> See this excellent review paper: [Quantum computer based on color centers in diamond](#) by Sebastien Pezzagna and Jan Meijer, May 2020 (17 pages).

NV centers qubits operate theoretically at room temperature<sup>572</sup>. In practice, a temperature of 4K is frequently used<sup>573</sup>! The reason is that at this temperature, the spectral lines of the different energy states of the cavity are different, better spaced and easier to distinguish<sup>574</sup>. This reduces qubit readout errors. On top of that, the diagram *below* is not necessarily accurate as it seems to associate data related to ambient temperature such as the infrared emission at 1042 nm when measuring a qubit at the  $|1\rangle$  state.



The general principle of operation for these qubits is as follows<sup>575</sup>:

- **Qubit quantum state** is based on a two-state computational basis, with  $|0\rangle$  corresponding to the  $^3A$  energy zero spin base level and  $|1\rangle$  to the same level but with a non-zero spin. The computational basis is sometimes  $|+1\rangle$  and  $| - 1\rangle$  corresponding to the two non-zero spin levels of the  $^3A$  basis. Various techniques also use the neighboring nitrogen atom nucleus spin and/or that of the neighboring  $^{13}C$  atoms. These are used for creating qubits entanglement as well as for quantum memory management due to their greater stability than the cavity spin state.
- **Single-qubit quantum gates** are microwave-activated and exploit hyperfine energy transitions at a frequency of 2.87 GHz<sup>576</sup>. These transitions work together with a magnetic field for zone A and an electric field for zone E.

<sup>572</sup> See [A programmable two-qubit solid-state quantum processor under ambient conditions](#) by Yang Wu of Hefei's USTC in China, 2018 (5 pages). He describes an NV center managing two qubits at ambient temperature exploiting the cavity electron spin and the associated nitrogen atom nucleus spin.

<sup>573</sup> The technique is documented in [Quantum information processing with nitrogen vacancy centers in diamond](#) by Gang-Qin Liu and Xin-Yu Pan, 2018 (15 pages) and in [Diamond NV centers for quantum computing and quantum networks](#) by Lilian Childress and Ronald Hanson, 2017 (5 pages).

<sup>574</sup> This interdependence between hyperfine spectral lines and temperature is not unique to diamond cavities. They are common in crystalline structures because temperature modifies many parameters such as the relative arrangement of the atoms in the crystals which leads to changes in electrical and magnetic gradients and therefore spins, etc.

<sup>575</sup> I was initially inspired by a diagram from [lecture 3](#) of Hélène Perrin's course, February 2020. Then I integrated other sources of information. See in particular [The nitrogen-vacancy color center in diamond](#) by Marcus Doherty, Joerg Wrachtrup et al, 2013 (101 pages) which describes in particular the energy levels variations of NV centers as a function of their temperature.

- **Two-qubit quantum gates** use different methods: coupling NV centers with entangled photons, magnetic coupling, or with controlling the core spin of neighboring  $^{13}\text{C}$  carbon atoms with microwaves to create a CNOT gate<sup>577</sup>.
- **Qubits readout** uses the capture of the fluorescence of the cavity activated by a laser and with a CCD sensor, similar to what is done with trapped ions and cold atoms. It consists in illuminating the cavity with a green (546 nm) laser. This excites level  $^3\text{A}$  in  $^3\text{E}$  but without changing the spin. The non-zero spin state  $^3\text{E}$  will generate a non-radiative transition passing through the  $^1\text{A}$  state. The null spin state  $^3\text{E}$  will generate the emission of a red photon (689 nm) which will be detected by the CCD sensor. This optical readout of single isolated qubits works only at low temperatures to avoid the creation of perturbation affecting neighbor qubits.

The measurement of the cavity electron spin can exploit other techniques, each with their advantages and disadvantages: SCC (spin to charge conversion<sup>578</sup>), NMR (readout is assisted by the nucleus spin of neighboring atoms) and only by photonics ways, knowing that lasers are used in all cases.

The technology is not easy to industrialize on a large scale, whether it is the chipset itself or the control lasers.

The main countries involved are China, the Netherlands (TU Delft and Qutech<sup>579</sup>), Australia (University of Melbourne, Quantum Brilliance), Germany (University of Ulm), Japan (NII and NTT), some laboratories in France (such as CEA SPEC) and of course in different labs in the USA.

Commercial news on qubits based on NV Centers has been very low key for a few years. QDTI was willing to create a NV center-based quantum computer but now seem to focus only on quantum sensing. The main commercial players are Quantum Brilliance (Australia) and Turing (USA).

## NV centers qubits

- **works at 4K**, with simple cryogeny without dilution and helium 3.
- **long coherence time**.
- **strong and stable diamond structure**.
- NV centers can also help create **quantum memory** for other qubits types, like superconducting qubits.
- possible to integrate with **optical quantum telecommunications**.

- only **two startup** in this field, Turing and Quantum Brilliance



- **qubits controls complexity with lasers => not easy to scale.**
- practically, NV centers applications are more centered on quantum magnetometry and sensing than computing.

<sup>576</sup> As we have seen about trapped ions, hyperfine transitions are energetic transitions of low energy electrons, here in the microwave regime, which are generally related to the interaction between the magnetic polarities of the nucleus of the atoms with the magnetic field generated by the electrons. Knowing that here we are talking about electrons that do not rotate around the nucleus of an atom but in a cavity.

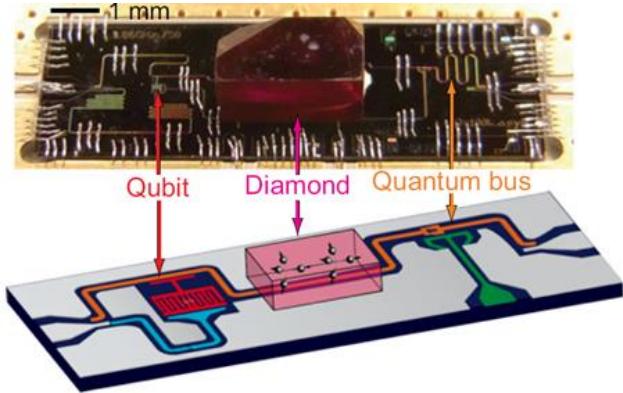
<sup>577</sup> See some detailed explanations in [Colour centers in diamond](#) by Joerg Wrachtrup, 2017 (36 slides).

<sup>578</sup> Explained in detail in [Spin readout via spin-to-charge conversion in bulk diamond nitrogen-vacancy sets](#) by Harishankar Jayakumar, September 2018 (5 pages).

<sup>579</sup> See [NV center qubits](#), Qutech. They demonstrated a 10-qubit prototype.

Indeed, it seems that NV Centers have more promising uses in quantum sensing for the creation of precision magnetometers or for quantum memories interoperable with qubits realized with other technologies such as superconducting qubits in hybrid systems.

This is a path recently explored by the University of Delft<sup>580</sup>, in Japan<sup>581</sup> and by CEA-SPEC with Patrice Bertet (diagram opposite of a superconducting qubit linked to a memory qubit in NV center)<sup>582</sup>.



There are also variants of NV center techniques with defects introduced in phosphorus-doped silicon carbide which would have the advantage of creating qubits whose readout is more accurate because it is based on the emission of a narrow frequency fluorescence<sup>583</sup>.

In a similar fashion, MIT prototyped in 2020 a NV Centers chipset replacing nitrogen with silicon and germanium. They reach 128 qubits but these qubits are not operational<sup>584</sup>.

One of the challenges of NV centers is their implantation in diamonds. One promising technique created by Berkeley Labs is using gold ions-based implantation that could scale to thousands of qubits. But this is just about fabrication and not functional qubits<sup>585</sup>.

We still have **Quantum Brilliance** (2019, Australia) and **Turing Inc** (2016, USA) who are dedicated to creating NV center-based quantum computers.



**Quantum Brilliance** (2019, Australia/Germany, \$11.4M) is developing a NV centers quantum processor that operates at room temperature, created by ANU (Australian National University) researchers, Andrew Horsley (CEO) and Marcus Doherty (CSO).

They estimate that their solution will be size/weight/performance/cost/power competitive and bring some quantum advantage earlier than competing systems from Google and IBM that they brand « quantum mainframes ». They want to create “quantum desktops” and why not pushing the envelope a bit too far with “smartphone quantum computers”<sup>586</sup>. They introduced in March 2021 a 5-qubits prototype fitting into a 2U classical 19-inch server form factor<sup>587</sup>. They expect to reach 50 qubits by 2026 and to then scale up this architecture with connecting several units together<sup>588</sup>. Probably with photons... and there, you'd probably need some cooling for photon sources and detectors!

<sup>580</sup> See [Diamond-based 10-qubit register with coherence more than one minute](#), November 2019.

<sup>581</sup> See [Coherent Coupling between a Superconducting Qubit and a Spin Ensemble](#) by Shiro Saito et al, 2012 (7 pages).

<sup>582</sup> See [Quantum technologies with hybrid systems](#), Patrice Bertet et al, 2015 (8 pages).

<sup>583</sup> See [Study Takes Step Toward Mass-Producible Quantum Computers](#), 2017.

<sup>584</sup> See [Large-scale integration of artificial atoms in hybrid photonic circuits](#) by Noel H. Wan et al, Nature, 2020.

<sup>585</sup> See [Ion-Trap Advance: Berkeley Lab Pioneers Way That Could Increase Scalability to Over 10,000 Qubits for Quantum Sensing, Quantum Computing](#) by Matt Swayne, May which refers to [Direct formation of nitrogen-vacancy centers in nitrogen doped diamond along the trajectories of swift heavy ions](#) by Russell E. Lake et al, March 2021 (5 pages).

<sup>586</sup> See [Breakthrough: Quantum computers will soon fit in your phone - Quantum Brilliance has developed a diamond-based quantum computer that can run at room temperature and be miniaturised](#) by Maija Palme, Sifted, August 2021.

<sup>587</sup> In some sources, the number of available qubits is two and not five... !

<sup>588</sup> See [Diamond-Based Quantum Accelerator Puts Qubits in a Server Rack](#) by Charles Q. Choi, March 2021. The illustrative picture comes from Quantum Brilliance. See also some technical details in [Quantum accelerators: a new trajectory of quantum computers](#) by Marcus Doherty, Quantum Brilliance, March 2021.

The Australian Pawsey Computing Center is partnering with this company to install a quantum computer there.



In April 2021, Quantum Brilliance also announced a partnership with **Quantum-South** (Uruguay) and to develop proof of concepts optimization quantum applications for air and maritime cargo companies. This is a bit far-fetched given their existing 5-qubits but why not exploring the path.

# TURING

**Turing Inc** (2016, USA, \$15.5M) is a startup willing to create quantum computing hardware and software, based on NV centers qubits and operating at 4K<sup>589</sup>.

They also develop error correction systems that they market to other industry specialists. A way to avoid putting all your eggs in the same basket!

## Topological qubits

In this category of qubits and quantum computing, we must create a distinction between the notion of "topological" which defines a type of qubit based on anyons and the "Majorana fermions" which are a variant of anyons to create topological qubits. Of all the types of qubits, they are the most mysterious and complex to understand<sup>590</sup>! It's part of the broad field of topological matter.

The principle of topological quantum computing is based on the notion of anyons which are "quasi-particles" integrated in two-dimensional systems, given that there are Abelian and non-Abelian anyons! Anyons are asymmetrical and two-dimensional physical structures whose symmetry can be modified. This makes it possible to apply some topology principles with sets of successive permutations applied to pairs of anyons that are in close proximity in circuits.

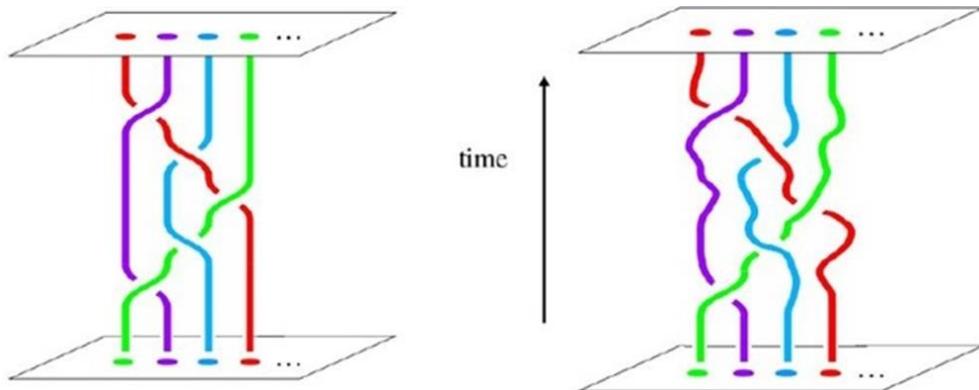
The related algorithms are based on the concepts of topological braid or node organizations ("braids"). Their representation explains this, with a temporal evolution of the permutations of temporal anyons going from bottom to top, knowing that in other representations, it may go from top to bottom<sup>591</sup>.

---

<sup>589</sup> See [Turing Inc: Large Scale Universal Machines](#), 2017, which details this a little bit.

<sup>590</sup> See [Topological Quantum Computing](#) by Torri Yearwood, January 2020 and [A Short Introduction to Topological Quantum Computing](#) by Ville Lahtinen and Jiannis K. Pachos, May 2017 (44 pages).

<sup>591</sup> Topological qubits could also be realized in photonics-based architecture. See [New photonic chip promises more robust quantum computers](#), September 2018, involving researchers in Australia, Italy and Switzerland.

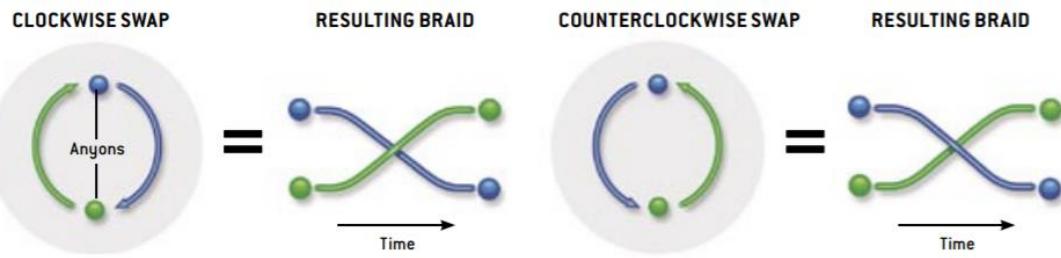


The following diagram clarifies it a little<sup>592</sup>. Topological quantum gates require a long sequence of anyonic permutations as with the CNOT gate shown at the bottom of the diagram. They are a sort of quantum error correction code.

## HOW TOPOLOGICAL QUANTUM COMPUTING WORKS

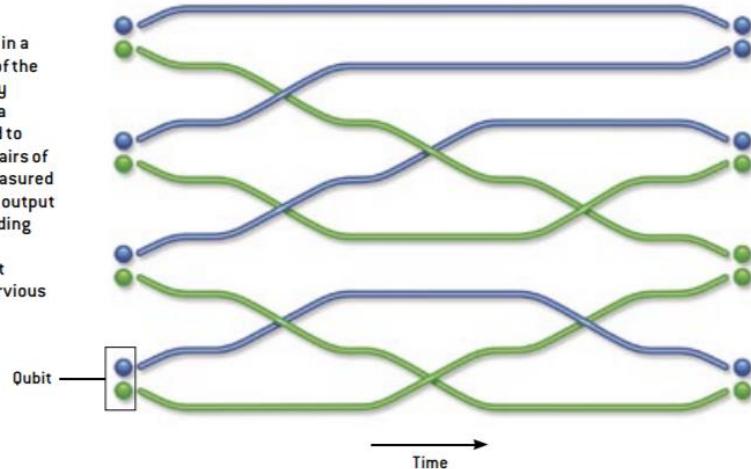
### BRAIDING

Just two basic moves in a plane—a clockwise swap and a counterclockwise swap—generate all the possible braidings of the world lines [trajectories through spacetime] of a set of anyons.

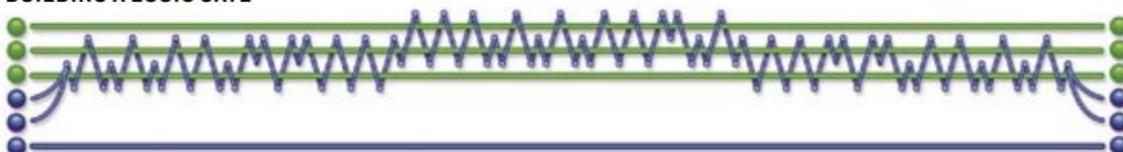


### COMPUTING

First, pairs of anyons are created and lined up in a row to represent the qubits, or quantum bits, of the computation. The anyons are moved around by swapping the positions of adjacent anyons in a particular sequence. These moves correspond to operations performed on the qubits. Finally, pairs of adjacent anyons are brought together and measured to produce the output of the computation. The output depends on the topology of the particular braiding produced by those manipulations. Small disturbances of the anyons do not change that topology, which makes the computation impervious to normal sources of errors.



### BUILDING A LOGIC GATE



A logic gate known as a CNOT gate is produced by this complicated braiding of six anyons. A CNOT gate takes two input qubits and produces two output qubits. Those qubits are represented by triplets (green and blue) of so-called Fibonacci anyons. The particular style of

braiding—leaving one triplet in place and moving two anyons of the other triplet around its anyons—simplified the calculations involved in designing the gate. This braiding produces a CNOT gate that is accurate to about  $10^{-3}$ .

<sup>592</sup> The diagram comes from [Computing with Quantum Knots](#) by Graham Collins, Scientific American, 2006 (8 pages).

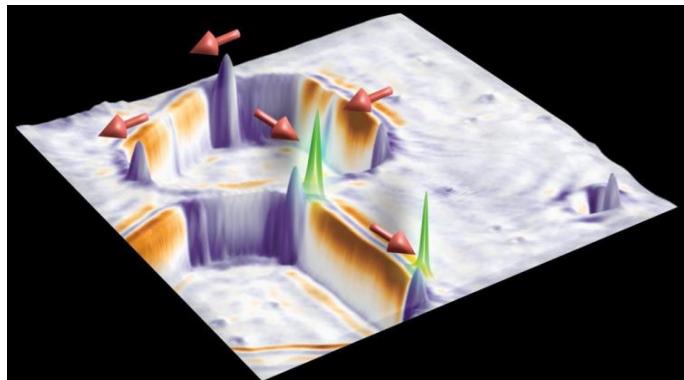
**Alexei Kitaev**, back then a researcher at Microsoft, had the idea in 1997 to use anyons for quantum calculations. From a physical point of view, anyons are "quasi-particles", i.e. particle representation models that describe the state of electron clouds around atoms, in the superconducting regime. Majorana fermions are a specific type of these quasiparticles organized along a small superconducting wire. They have collective electron behaviors in crystalline networks at very low temperature.

Topological qubits combine mathematics, physics and computer science at a doctoral level<sup>593</sup>. To understand the topology and fermions of Majorana, we must come back into the physics of particles. Fermions are the particles of matter and include leptons (electrons, neutrinos) and baryons (protons, neutrons, quarks-based), which make up the nuclei of atoms.

The fermions of Majorana are a special case corresponding to a kind of state of electrons which appears at both ends of tiny superconducting wires. A debate is going on among physicists about the very existence of these fermions.

Leo Kouwenhoven of the Delft Lab (then MSR) announced the detection of quasi-particles in 2012 at TU Delft and later on in 2018. But his 2017 paper generated concerns and had to be withdrawn in early 2021<sup>594</sup>.

But some discovery was also done in 2016 at MIT and in 2018, a group of three American universities UC Irvine, UCLA and Stanford claimed they had discovered real Majorana fermions. In May/June 2019, German and Austrian researchers said they succeeded in creating two-dimensional topological phenomena similar to fermions of Majorana<sup>595</sup>. Princeton researchers also published in June 2019 the results of their work that led them to control the state of a quasi-particle<sup>596</sup>.



In August 2019, NIST physicists led by Nick Butch announced the discovery by chance of interesting properties of uranium ditelluride ( $\text{UTe}_2$ ). It would be superconducting at 1.7K with the ability to do so via Cooper pairs with identical spins in addition to opposite spins, allowing three types of pairs. This would give it a rare ability to get a magnetic flux resistant superconductivity.

This material would thus have topological properties in this framework allowing to create topological qubits that are more stable and less subject to decoherence<sup>597</sup>.

Related work was published by researchers from John Hopkins University in 2018 with superconducting topological qubits made of a bismuth-palladium alloy<sup>598</sup>.

<sup>593</sup> This is the thesis of Hugo de Garis in [Topological Quantum Computing The TQC Shock Wave and its Impact on University Computer Science Teaching](#), 2011 (29 pages).

<sup>594</sup> See [Quantized Majorana conductance](#) by Leo Kouwenhoven et al, 2017 (26 pages) which was followed by an "[expression of concern](#)" from the authors warning readers about the veracity of the published results, which were not reproducible due to a problem with the calibration of measuring instruments. The coverage on the paper withdrawal in 2021 was dense, startup with [Data manipulation and omission in 'Quantized Majorana conductance'](#), [Zhang et al](#), Nature 2018 by Frolov et al, March 2021 (31 slides) which spurred [Microsoft's Big Win in Quantum Computing Was an 'Error' After All](#), by Tom Simonite, Wired, February 2021.

<sup>595</sup> See [Computing Faster With Quasi-Particles](#), May 2019.

<sup>596</sup> See [Mysterious Majorana Quasiparticle Is Now Closer To Being Controlled For Quantum Computing](#), June 2019 mentioning [Observation of a Majorana zero mode in a topologically protected edge channel](#) by Ali Yazdani et al, Science, June 2019 (12 pages).

<sup>597</sup> See [Newfound Superconductor Material Could Be the 'Silicon of Quantum Computers'](#) Possible "topological superconductor" could overcome industry's problem of quantum decoherence, August 2019, mentioning [Nearly ferromagnetic spin-triplet superconductivity](#) by Sheng Ran et al, 2019.

And the story goes on and on around fermions of Majorana that are discovered, believed to be discovered or rediscovered depending on the case.

We have them on gold<sup>599</sup>, on the surface of superconducting nanowires<sup>600</sup>, in crystals<sup>601</sup>, in 2D graphene<sup>602</sup>, not to mention other publications that are not obvious to analyze<sup>603</sup>, all this in 2020.

It is still largely a field of fundamental physics. The debate is also raging with many physicists regularly questioning the discoveries of Majorana fermions that would not be fermions.

Different physics laboratories are working on the subject, notably in the USA, China, the Netherlands, Denmark, Finland<sup>604</sup> and also in France.

In particular, there is a team at the IRIG of the CEA in Grenoble (Manuel Houzet, Julia Meyer and Xavier Waintal), Pierre Mallet of CNRS Institut Néel in Grenoble, Hugues Pothier at the CEA in Saclay and Pascal Simon at the LPS in Orsay.

They do not work on Majorana fermions per se, but on topological matter at the fundamental level and particularly on Andreiv's states, the linked states and the physics of weak links, different areas that remain to be explored in these lines. Some of these researchers are conducting joint projects with TU Delft.

## Majorana fermions qubits

- **theoretically very stable qubits** with low level of required error correction.
- **long coherence time and gates speed** enabling processing complex and deep algorithms.
- **potential qubits scalability**, built with technologies close to electron spin qubits.
- some researches in the topological matter field could be fruitful with no Majorana fermions.

- **no Majorana fermion qubit demonstrated yet.**
- **topological qubits programming** is different and requires an additional software layer.
- **rather few laboratories** involved in this path.
- **no startup** was launched in this field. Microsoft is the only potential vendor. IBM is investigating the field in Zurich.
- works at **low cryogenic temperatures** like superconducting qubits < 20mK.

With this in mind, let's see where the two main players in this field, Microsoft and Nokia, stand. Their parallel investment has nothing to do with their failed joint venture in smartphones a few years ago.

<sup>598</sup> See [Observation of half-quantum flux in the unconventional superconductor  \$\beta\$ -Bi<sub>2</sub>Pd](#) by Yufan Li & Al, October 2018 (12 pages).

<sup>599</sup> See [Quantum Computing Breakthrough: First Sighting of Mysterious Majorana Fermion on Gold](#) by Jennifer Chu, MIT, Indian Institute of Technology, University of California & Hong Kong University, 2020. And [Signature of a pair of Majorana zero modes in superconducting gold surface states](#) by Sujit Manna et al, MIT, 2019 (35 pages).

<sup>600</sup> See [Alternative route to topological superconductivity Hub](#), April 2020. University of Copenhagen in collaboration with Microsoft. Refers to [Flux-induced topological superconductivity in full-shell nanowires](#) by S. Vaitiekėnas et al, March 2020 (38 pages).

<sup>601</sup> See [Building block for quantum computers more common than previously believed](#) by Chanapa Tantibanchachai, Johns Hopkins University, April 2020.

<sup>602</sup> See [Observation of Yu-Shiba-Rusinov states in superconducting graphene](#) by E. Cortés-del Río, Pierre Mallet et al, 2020 (22 pages) and published in Advanced Materials in April 2021.

<sup>603</sup> See [The observation of photon-assisted tunneling signatures in Majorana wires](#) par Ingrid Fadelli, May 2020, [Quantum computers do the \(instantaneous\) twist](#) by Chris Cesare, August 2020 on a topological error correction system and [Fractional statistics of anyons in a two-dimensional conductor](#), C2N, April 2020.

<sup>604</sup> See [Ultra-thin designer materials unlock quantum phenomena](#), Aalto University, December 2020 and [Topological superconductivity in a van der Waals heterostructure](#) by Shawulienu Kezilebieke et al, March 2021 (27 pages).

In February 2020, **John Preskill** (father of the notions of quantum supremacy and NISQ) predicted that by 2030, we will be able to demonstrate two entangled topological qubits, against **Jonathan Dowling** (photonicist) who did not believe it could be created! The object of this symbolic wager? A good beer and a pizza. Jonathan Dowling died on June 5, 2020 and will therefore not be able to see if he won or lost his bet in 2030.

**in February, John Preskill predicted that by 2030, scientists could demonstrate two entangled topological qubits, against Jonathan Dowling who didn't believe it could happen.**

John Preskill @preskill · Feb 24  
Thread.

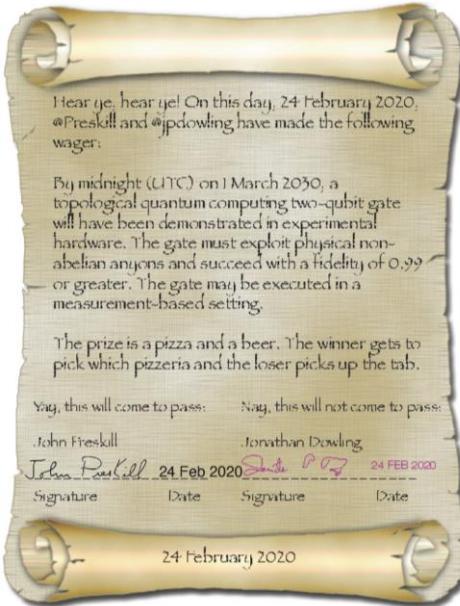
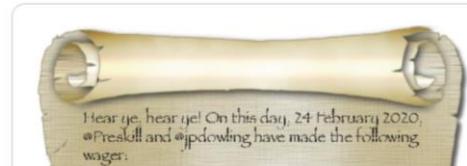
I made a bet with @jpdowling!

#WhenScientistsBet

John Preskill @preskill · Feb 24  
Replying to @jpdowling @quantum\_geoff and @warrench92  
Okay, deal!

8 37 197

Jonathan P. Dowling @jpdowling · Feb 25  
It's official and let all 13,000 of our followers be witnesses.



Microsoft Research has investigating topological quantum computing and Majorana fermions for quite a few years but has no prototype at this stage. The company is making a bet there, up to say that if they fail, everybody will also fail in quantum computing. While being a little arrogant and a very risky bet, it would bring lots of strategic advantages if it worked!

Indeed, Majorana qubits would be much more reliable and generate fewer errors ( $10^{-30}$ ), with the implication that we could avoid using some of the classical quantum error correction codes that are implemented with other types of qubits<sup>605</sup>.

A Fields Medal in 1986 for his work on the Poincaré conjecture, **Michael Freedman** joined Microsoft in 1997, coming from the University of Santa Barbara, the same where John Martinis came from when he joined Google in 2014. Freedman demonstrated with Alexei Kitaev the possibility of doing quantum computing with a hypothetical particle, the Majorana fermion, conceptualized in 1937 by the Italian Ettore Majorana from the resolution of mathematical equations of Dirac<sup>606</sup>. This fermion is a strange particle, whose charge and energy are zero and which is its own antiparticle.

Freedman and Kitaev were recruited by Microsoft Research. Run by Michael Freedman, Microsoft Quantum Santa Barbara (Station Q) is located on the campus of the University of Santa Barbara.

<sup>605</sup> Here are a few leads to find out more: [Microsoft Ready to Build a Quantum Computer](#) by Juliette Raynal, 2016, [A Software Design Architecture and Domain-Specific Language for Quantum Computing](#), 2014 (14 pages), Quantum [Computing at Microsoft](#) (56 slides) and [Quantum Computing Research at Microsoft](#) (59 slides) by Dave Wecker and [A short introduction to topological quantum computation](#) by Ville Lahtinen and Jiannis Pachos, 2017, (43 pages). And some videos: [keynote of November 2017](#) with Leo Kouwenhoven (43 mn), [Build conference of May 2018](#) on Q# (1h15mn) and [Majorana qubits](#) by Xiao Hu, in May 2017 (22 mn).

<sup>606</sup> In [Topological Quantum Computation](#) published in 2002 and updated in 2008 (12 pages).

They are complemented by **Leo Kouwenhoven**'s team based in Microsoft's Delft Lab in the Netherlands and with **Charles Marcus** from the Niels Bohr Institute who also joined Microsoft Research. Microsoft also collaborates with **Purdue University** in Indiana, where it has a dedicated research team **Microsoft Quantum Purdue**, working on III-V superconductors.



**Ettore Majorana**  
1906-1938



**Michael Freedman and Alexei Kitaev**  
MSR



**Leo Kouwenhoven**  
Delft Lab then MSR



**Charles M. Marcus**  
Niels Bohr Institute  
and MSR

fermions theory built in 1937,  
virtual particle without  
energy nor charge which is its  
own antiparticle

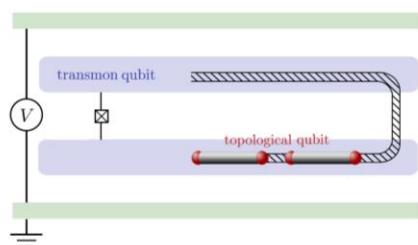
publish « Topological Quantum Computation » in 2002, setting the stage of topological quantum computing

detect quasi-particles in  
2012 at TU Delft then in  
2016 at MIT

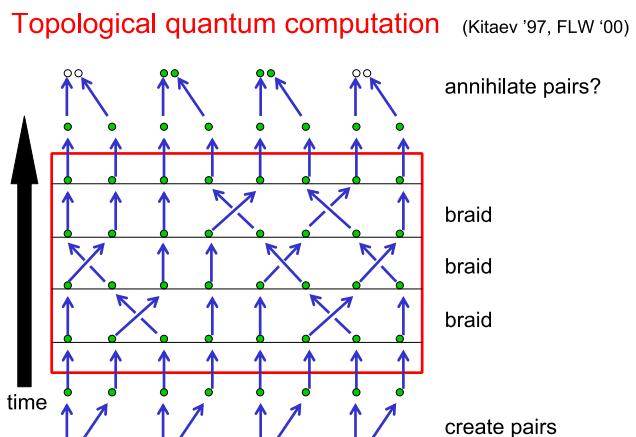
working on quasi-particles qubits

Majorana fermions are strange behaviors of electrons and their spin that are found at both ends of superconducting wires. They operate at very low temperatures, as for superconducting and silicon-based qubits, at about 15-20 mK<sup>607</sup>. Seen up close, these qubits are sophisticated variants of superconducting qubits. These "topological" mesh associations provide protection against qubit decoherence because the shape of the braids does not matter as long as their topology is stable.

Microsoft announced at the Build conference in May 2018 that they would release their first fermion-based quantum computer from Majorana in 2023<sup>608</sup>. After Leo Kouwenhoven's 2017 paper withdrawal in 2021, this planning seems somewhat challenging<sup>609</sup>. But let's not count Microsoft out of the game too rapidly. All discoveries have their up and downs. If a failure meant *stop all research*, Thomas Edison would not have discovered the light bulb and many vaccines and cancer treatments wouldn't see the light of day!



**Fig. 6:** Read out of a parity qubit in a Cooper pair box. Two superconducting islands (blue), connected by a split Josephson junction (crosses) form the Cooper pair box. The topological Majorana qubit is formed by four Majorana fermions (red spheres), at the end points of two undepleted segments of a semiconductor nanowire (striped ribbon indicates the depleted region). A magnetic flux  $\Phi$  enclosed by the Josephson junction controls the charge sensitivity of the Cooper pair box. To read out the topological qubit, two of the four Majorana fermions that encode the logical qubit are moved from one island to the other. Depending on the quasiparticle parity, the resonance frequency in a superconducting transmission line enclosing the Cooper pair box (green) is shifted upwards or downwards by the amount which is exponentially small in  $E_J/E_C$ .



<sup>607</sup> Source of the diagram: [Majorana Qubits](#) by Fabian Hassler, 2014 (21 pages).

<sup>608</sup> See this video ad: [Introducing Quantum Impact \(Ep. 0\)](#), February 2020 (4 minutes).

<sup>609</sup> Diagram source: [Topological quantum computing for beginners](#), by John Preskill (55 slides).

Microsoft obviously also invested on software development, first with its Liquid platform, then with F# for scripting and with the Q# language used for quantum programming, launched at the end of 2017. One of the contributors to these efforts is researcher **Krysta Svore** from Columbia University. In 2018, Microsoft recruited a certain **Helmut Katzgraber**, one of the apostles of D-Wave quantum annealing and MBQC (measurement-based quantum computers)<sup>610</sup>.

# NOKIA

Nokia's Bell Labs in the USA, located in Murray Hill, New Jersey, also work or worked on topological qubits but are relatively quiet about it<sup>611</sup>. Nokia also supports Oxford University's [Quopal](#) initiative on the use of quantum in machine learning.

Nokia likes to remind us that Grover and Shor's algorithms were discovered by their creators when they worked at the Bell Labs. Nokia is also working on quantum cryptography, at least at the level of its transport on optical fibers, as demonstrated by this [partnership](#) with SK Telecom of 2017.

But Nokia's many economic difficulties didn't mean good news for these various research projects.

## Trapped ions qubits

Trapped ions are positively ionized atoms that are trapped magnetically and/or by electrodes in a confined space and placed next to each other. The atoms are generally alkaline metals from the second column of Mendeleev's table (called "Group IIA" in Mendeleev's notation or group 2 in the modern notation, with beryllium, magnesium, strontium, barium and particularly calcium), then as ytterbium which is a rare earth in the lanthanide family or even mercury, and finally, quite rarely, metals of group IIB or 12 (zinc, cadmium, mercury).

### trapped ions qubits

- **identical ions** => no calibration required like with superconducting/electron spin qubits.
- **good qubits stability** with best in class low error rate
- **long coherence time** and high ratio between coherence time and gate time => supports deep algorithms in number of gates.
- **entanglement** possible between all qubits on 1D architecture. Speed up computing.
- works at **4K to 10K** => simpler cryogeny than for superconducting/electron spins.
- **easy to entangle ions with photons** for long distance communications.

- **questionable scalability** beyond 50 qubits => but 2D architectures could make it, with Honeywell.
- **relatively slow computing** due to slow quantum gates => problematic for deep algorithms like Shor.
- ions requiring **ultra-vacuum** ... but not hard to obtain.

Realizations	Lifetimes	Gate Speed
Topological (Majorana)	1 minute	Nanoseconds
Flux Qubit	/ $10^{10}$	same
Charge Qubit	/ $10^{10}$	same
Transmon	/ $10^7$	same
Ion Trap	/ $10^2$	$10^3$ slower

better stability qubits  
low decoherence noise  
few errors  
long coherence time  
high gate speed

nothing demonstrated so far  
no prototype  
different algorithms

<sup>610</sup> See [Quantum Driven Classical Optimizations](#), August 2018 (28 min video).

<sup>611</sup> See [Quantum computing using novel topological qubits at Nokia Bell Labs](#) published in 2017, which describes their approach with topological qubits.

Trapped ion qubits were devised in the 1950s by **Wolfgang Paul**, Nobel Prize in Physics in 1989. The first to test them, in 1995, were **Juan Cirac** and **Peter Zoller** from the University of Innsbruck in Austria<sup>612</sup>.

## Quantum Computations with Cold Trapped Ions

J. I. Cirac and P. Zoller\*

*Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria*  
(Received 30 November 1994)

A quantum computer can be implemented with cold ions confined in a linear trap and interacting with laser beams. Quantum gates involving any pair, triplet, or subset of ions can be realized by coupling the ions through the collective quantized motion. In this system decoherence is negligible, and the measurement (readout of the quantum register) can be carried out with a high efficiency.

PACS numbers: 89.80.+h, 03.65.Bz, 12.20.Fv, 32.80.Pj

The general principle of these qubits is as follows<sup>613</sup>:

- **Preparation:** lasers are used to cool and stabilize the ions, using the Doppler effect. Ions are then confined in vacuum in different ways by a magnetic and/or electric field. They are placed in an ultra-vacuum chamber.
- **Qubit quantum state** corresponds to two relatively stable energy levels of the trapped ions.
- **Single-qubit quantum gates** are activated by microwaves, lasers or magnetic dipoles.
- **Two-qubit quantum gates** use lasers with entangled photons or electrodes. In particular, they can exploit the phonon phenomenon that links atoms together by vibrations that propagate from one atom to another, which is valid for qubits aligned in linear Paul traps<sup>614</sup>.
- **Qubits readout** uses the detection of the cavity fluorescence with a CCD sensor after ions are excited by a laser. The excited ions corresponding to the  $|1\rangle$  state are visible while the unexcited ions corresponding to the  $|0\rangle$  state are not.

About a hundred research teams around the world are working on trapped ion qubits in almost every country working on quantum technologies (Australia, Austria, Canada, China, Denmark, Finland, France, Germany, India, Israel, Japan, Netherlands, Singapore, Switzerland, UK, USA)<sup>615</sup>.

**Rainer Blatt** from the University of Innsbruck is one of the pioneers in this field. He created a register of 14 addressable qubits in 2011 and increased it to 20 addressable and individually controllable qubits in 2018, using calcium ions. Rainer Blatt then cofounded **Alpine Quantum Technologies** (2017, Austria) where he characterized up to 10 high quality ion trapped qubits. In 2021, his team also demonstrated the use of trapped-ions to create qudits with 3, 5 and 7 levels, potentially opening the path for more powerful trapped-ion based quantum computing<sup>616</sup>.

<sup>612</sup> See [Trapped-Ion Quantum Computing: Progress and Challenges](#) by Colin Bruzewicz et al from MIT, April 2019 (56 pages). This is a very well-documented state-of-the-art review of trapped ion technology. And the founding article [Quantum Computations with Cold Trapped Ions](#) by Juan Cirac and Peter Zoller, 1995 (4 pages).

<sup>613</sup> See this interesting synthesis in [Introduction to Trapped-Ion Quantum Computing](#) by Gabriel Mintzer from MIT, February 2020.

<sup>614</sup> Trapped ions single and two qubit gates could be generated with only microwave magnetic fields and radiofrequency magnetic field gradients and no lasers. See [High-fidelity laser-free universal control of two trapped ion qubits](#) by R. Srinivas et al, February 2021 (40 pages).

<sup>615</sup> There were 98 research laboratories in the world working on trapped ions in 2020. See this table listing them all in [List of Ion Trapping Groups](#), February 2020.

<sup>616</sup> See [A universal qudit quantum processor with trapped ions](#) by Martin Ringbauer et al, September 2021 (14 pages). 8 levels for a calcium-based trapped-ion qubit.

Quantum simulation using trapped ions, and an Ising model as with the D-Wave, is also investigated by some laboratories such as at **ETH Zurich**, the **University of Maryland**, and elsewhere in the USA<sup>617</sup>.

**Long coherence time:** trapped ions have a rather long coherence time of up to several tens of seconds, but this is compensated by equally long gate times in proportion. The ratio between coherence time and gate time is however very good at  $10^6$ , while it is  $10^3$  for superconducting qubits and about 200 for cold atoms qubits.

**High fidelity:** they have the advantage of generating a fairly low error rate with up to 99.9999% fidelity for single-qubit gates and 99.9% fidelity for two-qubit gates. The table below illustrates these fidelities according to the quantum gate management method and the ions used. This makes it possible to theoretically execute "deep algorithms" with a large number of quantum gates and to obtain a good quantum volume, to use IBM's marketing terminology. However, this error rate increases with the number of qubits, at least in 1D architectures like the one from IonQ.

Type	Method	Fidelity	Time ( $\mu\text{s}$ )	Species	Ref.
1-qubit	Optical	<b>0.99995</b>	5	$^{40}\text{Ca}^+$	Bermudez 2017
	Raman	<b>0.99993</b>	7.5	$^{43}\text{Ca}^+$	Ballance 2016
	Raman	<b>0.99996</b>	2	$^9\text{Be}^+$	NIST 2016
	Raman	0.99	0.00005	$^{171}\text{Yb}^+$	Campbell 2010
	Raman	0.999	8	$^{88}\text{Sr}^+$	Keselman 2011
	$\mu\text{wave}$	<b>0.999999</b>	12	$^{43}\text{Ca}^+$	Harty 2014
	$\mu\text{wave}$		0.0186	$^{25}\text{Mg}^+$	Ospelkaus 2011
Type	Method	Fidelity	Time ( $\mu\text{s}$ )	Species	Ref.
2-qubit	Optical	0.996	–	$^{40}\text{Ca}^+$	Erhard 2019
	(1 sp.)	0.993	50	$^{40}\text{Ca}^+$	Benhelm 2008
	Raman	<b>0.9991(6)</b>	30	$^9\text{Be}^+$	NIST 2016
	Raman	<b>0.999</b>	100	$^{43}\text{Ca}^+$	Ballance 2016
	Raman	<b>0.998</b>	<b>1.6</b>	$^{43}\text{Ca}^+$	Schafer 2018
	Raman	0.60	0.5	$^{43}\text{Ca}^+$	Schafer 2018
	$\mu\text{wave}$	0.997	3250	$^{43}\text{Ca}^+$	Harty 2016
(2 sp.)	$\mu\text{wave}$	0.985	2700	$^{171}\text{Yb}^+$	Weidt 2017
	Ram./Ram.	<b>0.998(6)</b>	27.4	$^{40}\text{Ca}^+ / ^{43}\text{Ca}^+$	Ballance 2015
	Ram./Ram.	0.979(1)	35	$^9\text{Be}^+ / ^{25}\text{Mg}^+$	Tan 2015

Adapted from Bruzewicz et al.  
source des schémas : lecture 1 de 77 slides du cours d'Hélène Perrin à l'Université Paris 13 en quatre parties, février 2020.

**Connectivity:** in general, trapped ions qubits can all be entangled with each other with using of phonons but it depends on how they are distributed in space<sup>618</sup>. In superconducting qubit technologies, only neighbor qubits can be entangled, which creates constraints in the design and/or compilation of quantum algorithms.

**No calibration:** since these qubits are atoms, they are identical and do not require calibration adjustments like with superconducting qubits whose physical properties vary from one qubit to another depending on their materials and manufacturing.

**Temperature:** these qubits are supposed to operate at room temperature. In practice, this is not really the case. They generate an annoying temperature rise effect, which is not fully explained at the moment. This requires a cooling between 4K and 10K<sup>619</sup>. The interest of such a cooling is also to improve the quality of the chamber ultra-high vacuum.

**Why ions?** The interest of exploiting ions is to allow to trap them magnetically or with electrodes. It is also possible to couple them at long distance, of the order of several tens of microns. It can also be hybridized with several ions types mixed together, like calcium and strontium, to get their related benefit (fast gate for calcium and stability time for strontium)<sup>620</sup>.

<sup>617</sup> See [Digital Quantum Simulation with Trapped Ions](#) by Kenny Choo and Tan Li Bing, 2016 (29 slides) and [Programmable Quantum Simulations of Spin Systems with Trapped Ions](#) by Christopher Monroe et al, 2019 (42 pages).

<sup>618</sup> See [Benchmarking an 11-qubit quantum computer](#) by Christopher Monroe et al, March 2019 (8 pages).

<sup>619</sup> See [Closed-cycle, low-vibration 4 K cryostat for ion traps and other applications](#) by P. Micke et al, May 2019 (15 pages) which describes a cryostat for ion trapped processors using a pulsed head.

<sup>620</sup> See [Benchmarking a high-fidelity mixed-species entangling gate](#) by A. C. Hughes et al, Oxford University, August 2020 (7 pages).

The elements used have several common characteristics related to their electron layer configuration. They have excitation levels from the ground state that are of short duration and allow their use for the cooling of atoms by laser and Doppler effect. The basic energy state corresponding to the  $|0\rangle$  and the excited energy level corresponding to  $|1\rangle$  state are stable over time, which facilitates quantum gate operations.

There are five main variations of trapped ions being used, depending on the energy transitions applied to manage the two states of a qubit. Each of these modes correspond to different transition frequencies:

- **Zeeman qubits** use electromagnetic waves of a few MHz with magnetic field control. They are very sensitive to it but allow to have qubits with a very low error rate once this field is well controlled<sup>621</sup>. They are rather used in quantum sensing since their control frequency is too low to allow a precision control of several qubits close to each other.
- **Hyperfine structure qubits** use microwaves of a few GHz and laser-based Raman transitions<sup>622</sup>. This works with ions having a non-zero spin nucleus. The other cases concern ions with zero spin nuclei, i.e. those whose proton and neutron numbers are both even. This explains why some elements such as calcium are sometimes used in several of these categories, with different isotopes such as  $^{40}\text{Ca}^+$  in optical qubits and  $^{43}\text{Ca}^+$  in qubits of hyperfine structure<sup>623</sup>.

The number of neutrons in these ions changes the spin of the nucleus of atoms and its hyperfine energy states. In this category, IonQ and Honeywell are using hyperfine structure qubits driven by lasers and Oxford Ionics is using microwave gates.

- **Fine structure qubits** use submillimeter waves of a few THz.
- **Optical qubits** use photons of a few hundred THz. AQT is using this type of qubits.
- **Rydberg qubits** use so-called Rydberg energy states controlled by VUV ultraviolet rays (vacuum ultraviolet, not transmitted in air, needs vacuum), with wavelengths under 122 nm<sup>624</sup>.

Below is an explanation of these variants based on ion energy levels. On the left, a generic structure of ion energy levels with the transitions allowing the change of qubit state and those used to prepare the qubit state or to read it<sup>625</sup>.

In the middle and on the right, the different energy transitions used to define the  $|0\rangle$  and  $|1\rangle$  of the qubit. The height between the two levels characterizes the energy level that separates these two states. The higher it is, the higher the frequency used to modify the qubit state, going from radio waves of a few MHz to extreme ultraviolet in the case of Rydberg qubits.

---

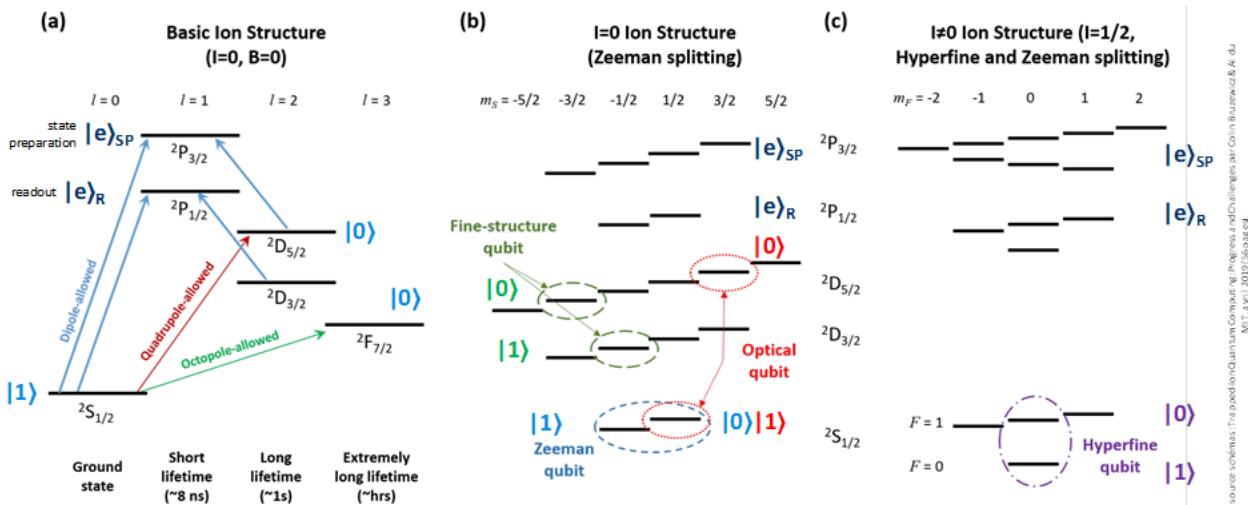
<sup>621</sup> See [Comparing Zeeman qubits to hyperfine qubits in the context of the surface code:  \$^{174}\text{Yb}^+\$  and  \$^{171}\text{Yb}^+\$](#)  by Natalie Brown, April 2018 (7 pages).

<sup>622</sup> See [Controlling Qubits With Microwave Pulses Reduces Quantum Computer Error Rates, Increases Efficiency](#) by Matt Swayne, 2020, which references [Robust and resource-efficient microwave near-field entangling  \$^9\text{Be}^+\$  gate](#) by G. Zarantonello, November 2019 (6 pages). See glossary for Raman transition.

<sup>623</sup> Diagram inspired by [Quantum Computing with ions](#) by F. Schmidt-Kaler, 2019 (40 slides).

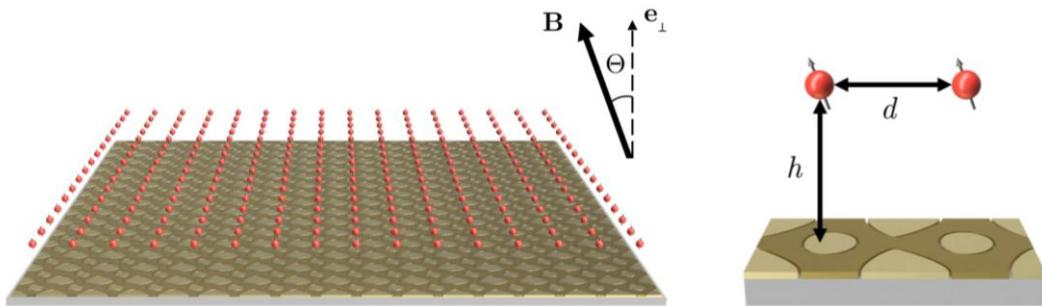
<sup>624</sup> See for example [Speeding-up quantum computing using giant atomic ions](#) by Stockholm University, April 2020.

<sup>625</sup> These charts showing atoms electronics energy transitions including fine and hyperfine transitions are called Grotrian diagrams.



The spatial stabilization of trapped ions is achieved in two main ways with ion traps that allow individual control of their position:

- With a **magnetic field** and an **electric quadrupole**: these are the Penning traps, invented in 1959. They have been tested at the ETH Zurich and in a 2D version which has the advantage of being theoretically scalable<sup>626</sup>.



- With a **variable electric field**: these are the Paul traps named after Wolfgang Paul. These traps are either linear in 1D structure (*below in (f)*), or flattened to create 2D structures. They are the most often used. The flat version corresponds to the technique used by Honeywell and IonQ.

<sup>626</sup> See [Scalable arrays of micro-Penning traps for quantum computing and simulation](#) by S. Jain et al, April 2020 (21 pages).

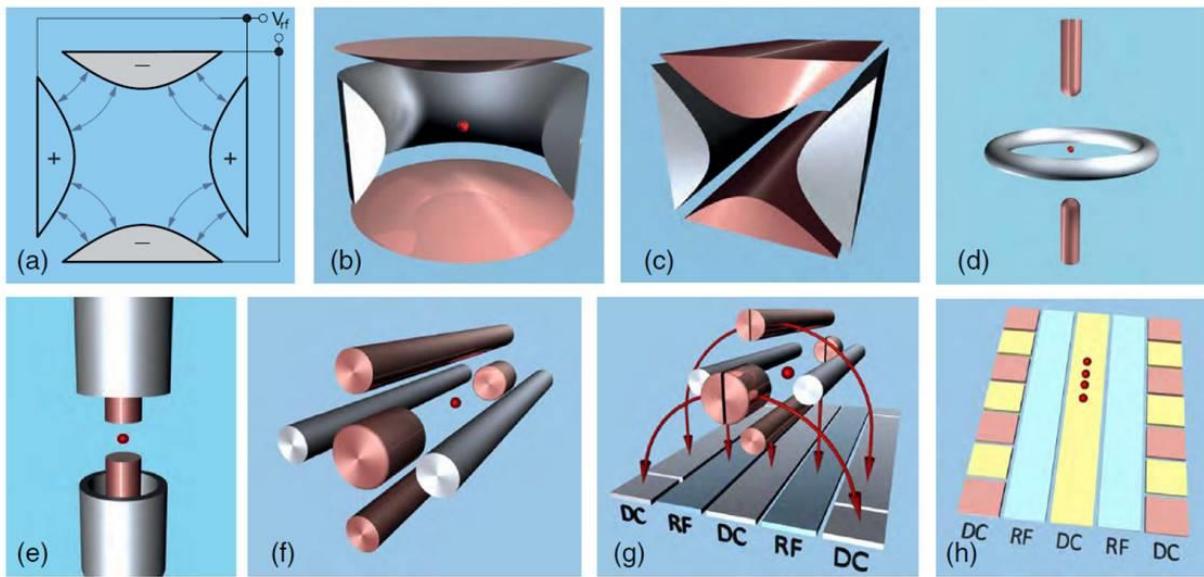


FIG. 2. (Reproduced from [68].) RF Paul trap geometries. (a) The basic concept of RF trapping, where quadrupolar fields oscillating at an RF frequency are produced using a set of (parabolic) electrodes. (b) The simplest cylindrically symmetric version of the basic RF trap. This is of the “ring and endcap” point-trap geometry. (c) The simplest translationally symmetric version of the basic RF trap. This will form a quadrupole mass filter and can be used to make a linear trap. (d,e) Topologically equivalent deformations of the geometry shown in (b). (f) Topologically equivalent deformations of the geometry shown in (c) with additional endcap electrodes added to form a four-rod, linear trap. (g) The four-rod trap in (f) may be deformed such that all electrodes reside in a single plane, forming a linear “surface-electrode trap.” (h) A subset of the electrodes in a linear trap [a surface-electrode trap is depicted here, but segmentation may be applied to other linear trap geometries, such as that shown in (f)] may be segmented to allow trapping in multiple zones, along the axial direction.

Lasers play several roles: they are used to cool the ions with the Doppler effect and by sideband cooling to slow down phonons (these are inter-ions vibrations, kind of shock waves), to initialize the energy state of the qubits to its ground  $|0\rangle$  state, to create quantum gates and finally, for qubits state readout<sup>627</sup>.

The main disadvantage is that the solution will probably not scale well, particularly with laser light control that goes through a light splitter and some lenses to focus it on the controlled ions. The ions are aligned in rows and separated by about 2 to 5  $\mu\text{m}$ . Finally, the technique is difficult to miniaturize because of the various control systems and the inexistence of adapted production lines. Except when the ions are managed by electrodes as Honeywell does.

Researchers from the University of Innsbruck and from ETH Zurich are thinking about making the trapped ion technology “portable”, forgetting the vacuum system and the cryostat, necessary for their operation<sup>628</sup>. They are part of the EU-funded **PIEDMONS** project (E2020). It also involves Infineon Austria<sup>629</sup>.

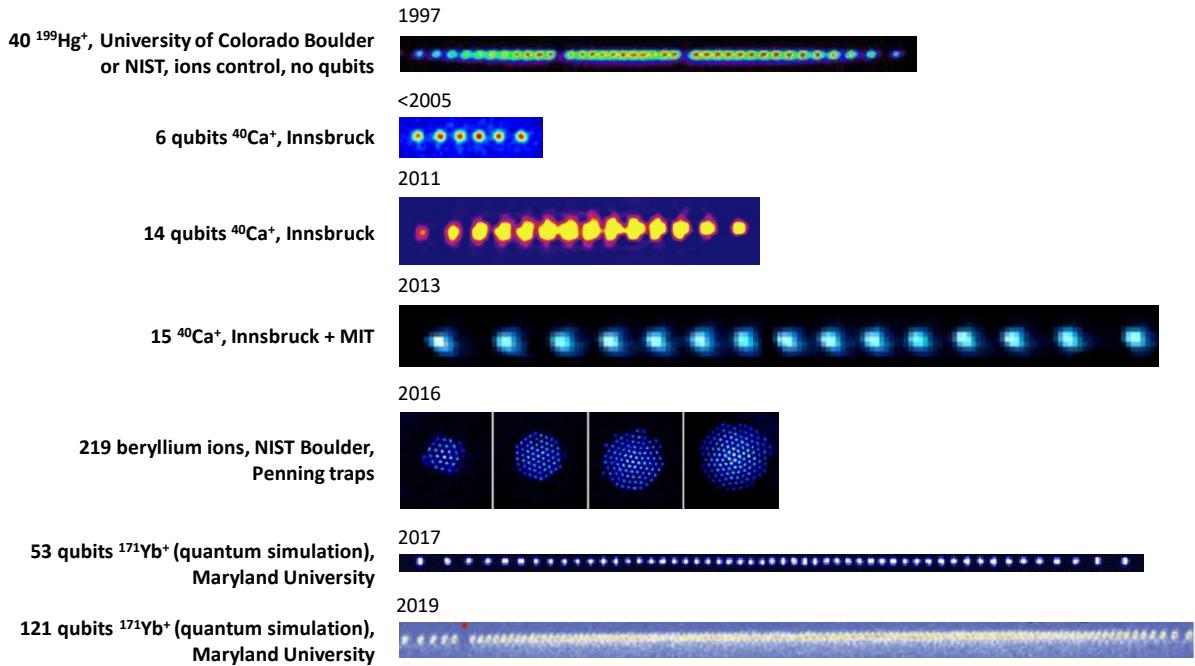
Trapped ions have at least two other use cases: quantum memories, and their integration in quantum repeaters for secure quantum telecommunications, including quantum keys distribution<sup>630</sup>.

<sup>627</sup> To learn more about the activation details of trapped ion qubits, see for example the presentation [Quantum information processing with trapped ions](#) by Christian Roos, 2012 (53 slides).

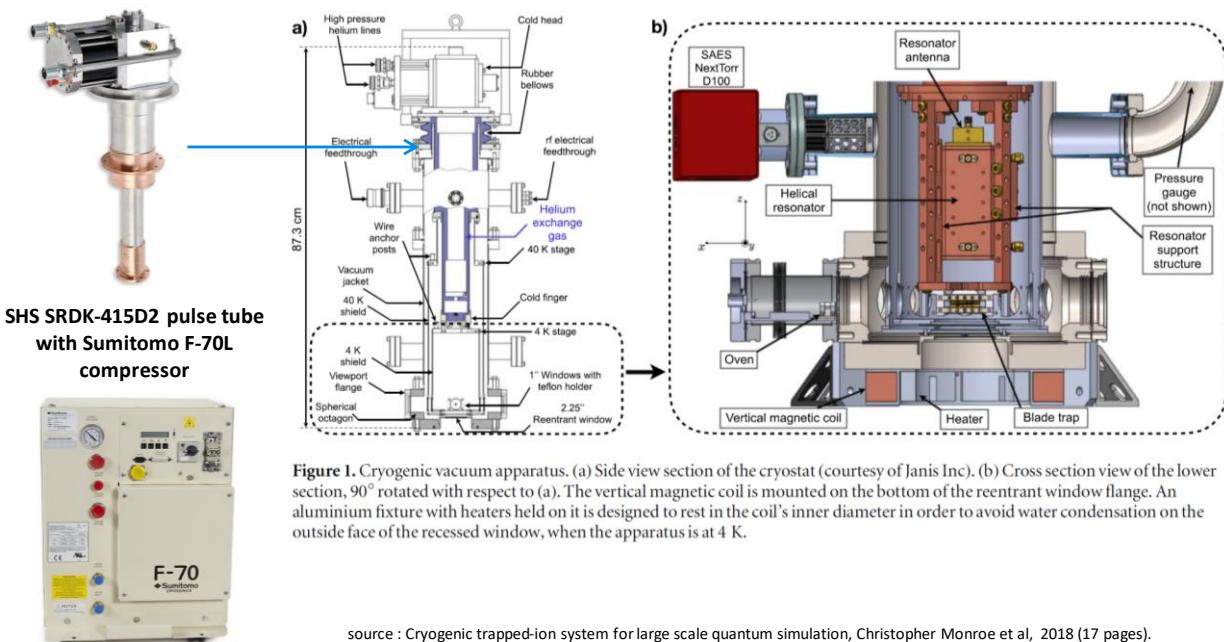
<sup>628</sup> See [Quantum computers to become portable](#), August 2019.

<sup>629</sup> See [2D Linear Trap Array for Quantum Information Processing](#) by Philip C. Holz, Rainer Blatt et al, September 2020 (20 pages).

<sup>630</sup> See [Single-qubit quantum memory exceeding 10-minute coherence time](#) by Ye Wang (Chine), 2017 (6 pages).



This involves interactions between trapped ions and photons, using cavities. It is already possible to entangle trapped ions via a photonic link of several hundred meters, a feat done over a distance of 400 m at the University of Innsbruck. This would enable the creation of distributed quantum computing architectures, a plan devised by IonQ to circumvent the scalability limitations of their qubits<sup>631</sup>.



**Figure 1.** Cryogenic vacuum apparatus. (a) Side view section of the cryostat (courtesy of Janis Inc). (b) Cross section view of the lower section, 90° rotated with respect to (a). The vertical magnetic coil is mounted on the bottom of the reentrant window flange. An aluminium fixture with heaters held on it is designed to rest in the coil's inner diameter in order to avoid water condensation on the outside face of the recessed window, when the apparatus is at 4 K.

source : Cryogenic trapped-ion system for large scale quantum simulation, Christopher Monroe et al, 2018 (17 pages).

the 4K cryostat used by Christopher Monroe's team at University of Maryland to trap more than a hundred ytterbium ions<sup>632</sup>. It operates a 4.2K SHS pulse tube and a Sumitomo compressor<sup>633</sup>.

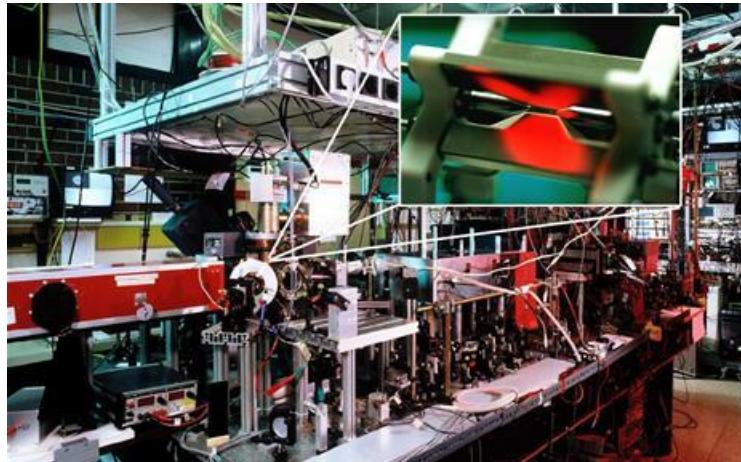
<sup>631</sup> See [Large Scale Modular Quantum Computer Architecture with Atomic Memory and Photonic Interconnects](#) by Christopher Monroe et al, 2014 (16 pages).

<sup>632</sup> Source of illustration: [Cryogenic trapped-ion system for large scale quantum simulation](#) by Christopher Monroe et al, 2018 (17 pages).

In May 2020, Wesley Campbell's **UCLA** team associated with UNSW announced that they had stabilized barium ions ( $^{133}\text{Ba}^+$ ) to build quality qubits in a linear trap<sup>634</sup>. The quality of these barium ions is compared to that of 2,014 qubits with a 10-fold improvement. This quality is evaluated only with the SPAM indicator which measures a fidelity on a qubit after preparation, some initialization single qubit gates and measurement (SPAM = "state preparation and measurement").

Let's also mention the **IQOQI** (Austria, see Rainer Blatt, one of their laboratories *opposite*) and the **IQST** (Germany), and the calcium based 20 qubits prototype<sup>635</sup> and the Ion Quantum Technology Group from the **University of Sussex** (UK) and its 10 qubits prototype, claiming to scale up to 1,000 qubits through a cluster of quantum processors<sup>636</sup>.

This led to the creation of the startup **Universal Quantum** (2019, UK).



In March 2021, the DoE **Sandia Labs** launched the QSCOUT (Quantum Scientific Computing Open User Testbed), a cloud quantum computing resource available to selected researchers from universities and other government research agencies<sup>637</sup>. It is an  $^{171}\text{Yt}$  based trapped ions system of 3 qubits used for benchmarking and for algorithms development, particularly in computational chemistry. It will later be expanded to a 10 and then 32 bits system, by 2023, on par with 2021's IonQ's capacity. At a low-level, this system is programmed with the in-house assembly language Jaqal ("Just Another Quantum Assembly Language").

The European Flagship includes the **AQTION** project, which is led by the University of Innsbruck and has a budget of €9.57M. The objective is to reach 50 operational qubits to prepare the next phase, beyond 100 qubits, by adopting a distributed architecture with photonic links. Alpine Quantum Technologies (AQT), the University of Oxford, ETH Zurich, Fraunhofer IOF and Atos are participating. Atos works on the solution software stacks and applications.

In France, various CNRS laboratories are working on trapped ions. Finally, we should add the American company **Honeywell**, whose March 2020 announcement we will detail below. In Germany, **Infineon** is also manufacturing trapped-ions qubits in collaboration with the **University of Innsbruck** in Austria, on top of electron spin and superconducting qubits.

---

<sup>633</sup> See also the thesis [Towards Cryogenic Scalable Quantum Computing with Trapped Ions](#) by Matthias Brandl, 2016 (138 pages) which documents very well the overall engineering of a quantum computer based on trapped ions.

<sup>634</sup> See [Physicists develop world's best quantum bits](#) by Stuart Wolpert of UCLA, May 2020 which refers to [High-fidelity manipulation of a qubit enabled by a manufactured nucleus](#) by Justin Christensen et al, May 2020 (5 pages). First precaution of use: identify the author of the article. It happens to be a certain Stuart Wolpert from UCLA, in charge of media relations at the University where the published work comes from. So he does the PR for the laboratory and publishes his article on a site where it is possible (Physorg).

<sup>635</sup> They coauthored [Observation of Entangled States of a Fully Controlled 20-Qubit System](#), April 2018 (20 pages).

<sup>636</sup> See [Blueprint for a microwave trapped ion quantum computer](#) by Winfried Hensinger et al, 2017 (12 pages).

<sup>637</sup> See [Rare open-access quantum computer now operational](#), Sandia Labs, March 2021.



**IonQ** (2016, USA, \$736M<sup>638</sup>) is a spin-off from the University of Maryland specialized in the design of universal quantum computers based on ytterbium trapped ions.

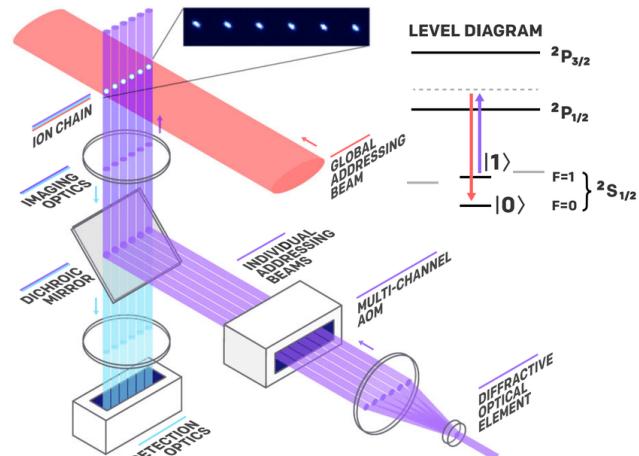
Co-founded by Christopher Monroe, professor at the university who also is their Chief Scientist<sup>639</sup>, the startup has raised a total of \$84M, part coming from Google Ventures and Amazon, in 2019, from Samsung Ventures and Microsoft, then in 2020 at Lockheed Martin and Bosch. HPE is also on board.

In June 2020, they created an advisory board including David Wineland, Umesh Vazirani, Margaret Williams (ex Cray) and Kenneth Brown (Duke University). In September 2021, they announced the creation of a joint laboratory with the University of Maryland (UMD), the Q-Lab, with \$20M funding. Among other things, the lab is tasked with training UMD students on quantum computing. They also partner with Accenture to develop customer applications.

In March 2021, IonQ announced a new round of funding with a merger agreement through the Special Purpose Acquisition Company (SPAC) mechanism, with the fund dMY Technology Group III that will yield a \$650 million investment. The funding is made of \$350M coming from investors including Hyundai, Kia Corporation<sup>640</sup> and Breakthrough Energy Ventures. The remaining \$300M come from dmY and an IPO<sup>641</sup>.

Their qubits record at the beginning of 2018 was 53 coherent and entangled qubits but for quantum simulation, not for gate-based computing. At the end of 2018, it had reached 79 qubits associated with 160 storage qubits but with a probable low fidelity<sup>642</sup>. Then, in 2019, they had 11 characterized qubits. These ups and downs are related to the fact that the performances are not the same according to the number of assembled qubits<sup>643</sup>.

On the right, their qubits control and readout architecture<sup>644</sup>.



Their quantum gates have high a fidelity rate of 99.9% for one-qubit gates and 99% for two-qubit gates. The system topology allows arbitrary gates of two to three qubits linking any of the aligned qubits.

<sup>638</sup> This amount includes \$84M from VCs and the 2021 SPAC. It excludes the total \$165M grants the company and Christopher Monroe's lab in Maryland University got from the US government, per their 2021 investor presentation.

<sup>639</sup> See [A Reconfigurable Quantum Computer](#) by David Moehring, 2017 (20 slides).

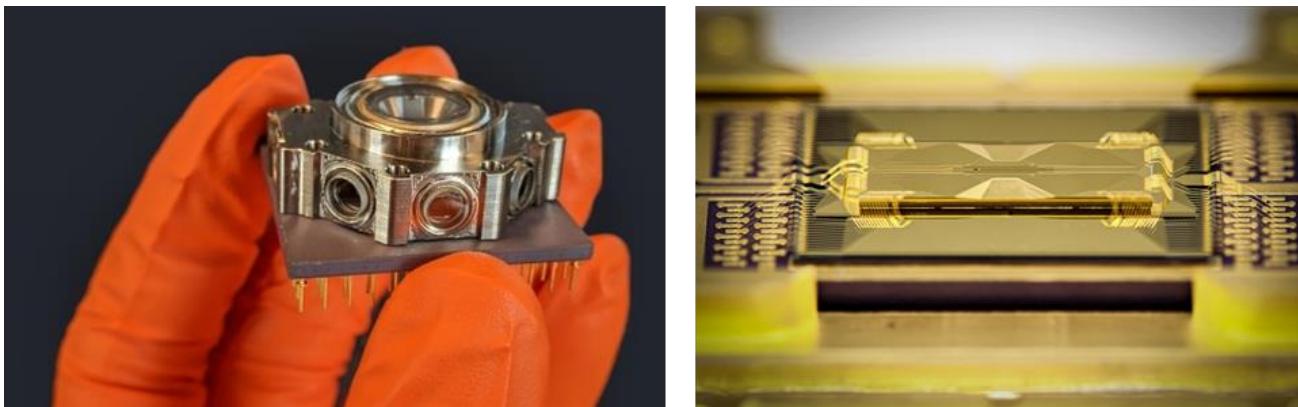
<sup>640</sup> They seem to have closed links with South Korea. These investors add up with a partnership with Q Center. See [IonQ and South Korea's Q Center Announce Three-Year Quantum Alliance](#), January 2021. To provide to the Q Center students to the IonQ computer online.

<sup>641</sup> See [QC ethics and hype: the call is coming from inside the house](#) by Scott Aaronson, October 2020, who found this IPO to be pushing the envelope of bullshit a bit too far.

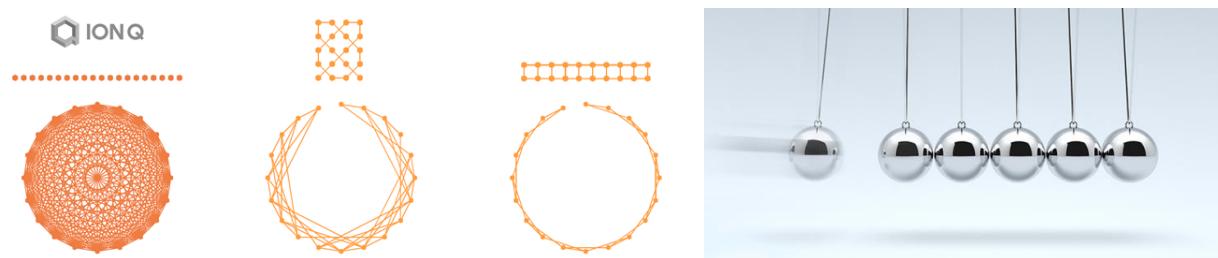
<sup>642</sup> See [IonQ Has the Most Powerful Quantum Computers With 79 Trapped Ion Qubits and 160 Stored Qubits](#) by Brian Wang, December 2018.

<sup>643</sup> See [Benchmarking an 11-qubit quantum computer](#) by K. Wright et al, November 2019.

<sup>644</sup> Illustration source: [Ground-state energy estimation of the water molecule on a trapped ion quantum](#) by Yunseong Nam, Christopher Monroe et al, March 2019 (14 pages).

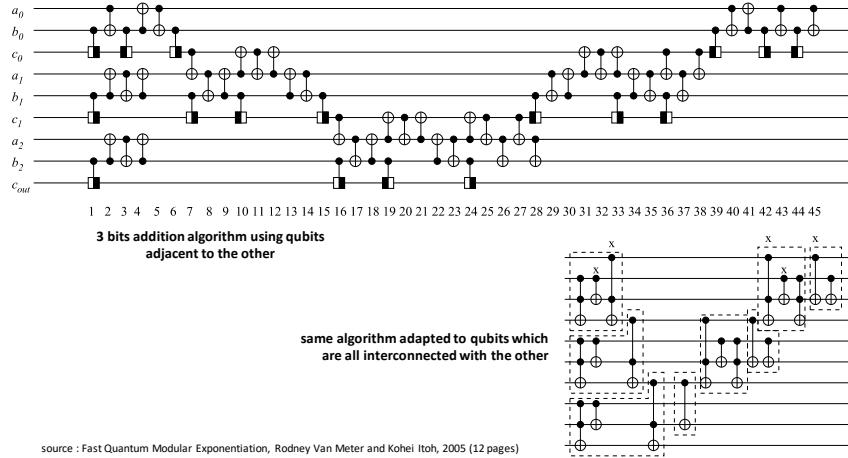


This is due to couplings between ions that exploit long-range Coulomb forces and phonons, a bit like when, in an abacus, the impact of a ball on one side drives ball move at the other side end.



This allows implementing a very good optimization of quantum algorithms to minimize the number of gates to be executed as shown in this example<sup>645</sup>.

They propose a software offer for programming in the cloud. The approach is also "full-stack". But the software approach seems to be very proprietary.



In November 2019, Microsoft announced the integration of IonQ's quantum accelerator support (in addition to QCI's superconductors and Honeywell's trapped ion accelerator) into its Azure Quantum cloud offering and its Q#, QDK and Visual Studio development tools. All this was made available to developers from late spring 2020. IonQ is also proposed by Google in its own cloud offering, on top of Amazon. IonQ became in 2021 the only one quantum computer vendor available on Amazon, Google and Microsoft clouds (with 10 qubits).

In October 2020, IonQ announced that it had created the world's most powerful quantum computer with 32 qubits and a quantum volume of 4,000,000, topping the Honeywell previous record with its 64 quantum volume announced in June 2020 and discussed below<sup>646</sup>.

<sup>645</sup> Source: [Fast Quantum Modular Exponentiation](#) by Rodney Van Meter and Kohei Itoh, 2005 (12 pages).

<sup>646</sup> See [IonQ Unveils World's Most Powerful Quantum Computer](#), IonQ, October 2020.

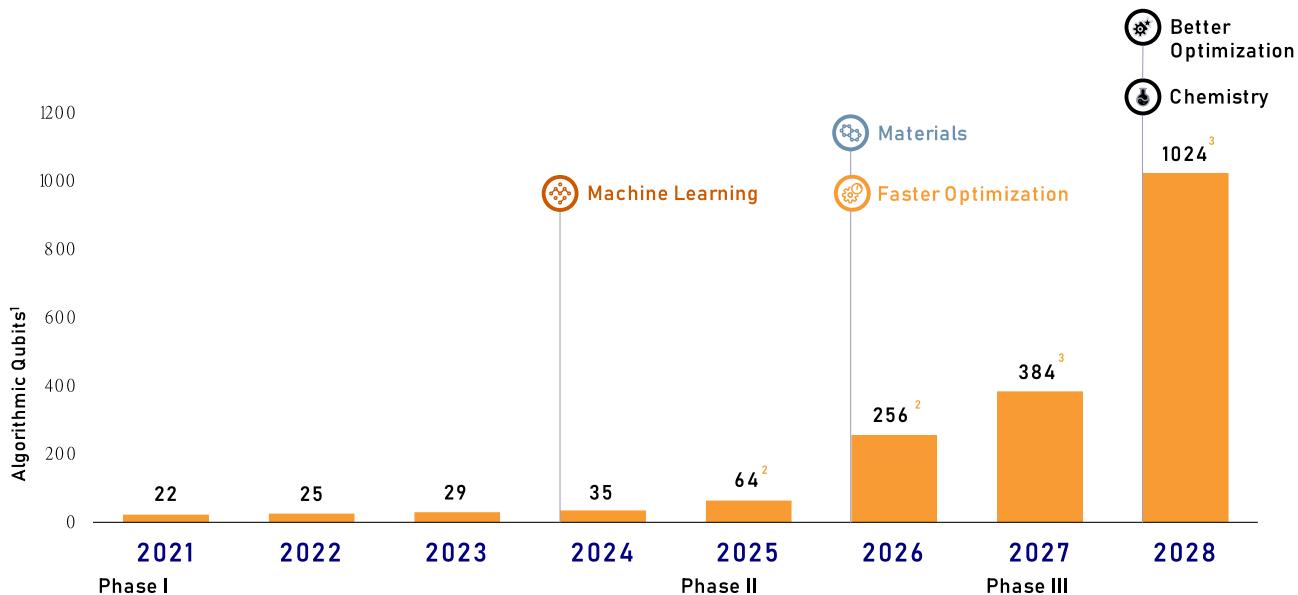
They claim the ability to handle error correction code with only 13 (and sometimes, 16) physical qubits per logical qubits vs. the 10,000 physical qubits that are usually expected to be required for superconducting and electron spin qubits. This is the result of their better qubit fidelity. This 32-qubit system is to be made available to customers of Amazon Braket, Microsoft Azure Quantum and Google cloud offerings. They also announced the creation of a Quantum Data Center sized to host 10 of their quantum computers.

In December 2020, IonQ unveiled its 5 years roadmap. They plan to use rack-mounted modular quantum computers small enough to be networked together in a datacenter by 2023. IonQ now uses a new benchmark metric of its own: algorithmic qubits, using  $\log_2$  of IBM's quantum volume which makes a lot of sense. It relates to the number of qubits that can be practically used with an equivalent depth of quantum gates computing.

Their 32 bits with 99.9% fidelity support 22 algorithmic qubits, the  $\log_2$  of their quantum volume. Their plan is to reach 29 algorithm qubits by 2023, 64 by 2025 with using a 16:1 error-correction encoding (meaning: 16 physical qubits per logical qubits). Later on, they will rely on a 32:1 ratio.

Then, they expect to scale beyond 64 and reach a broad quantum advantage with 256 then 1024 algorithmic qubits by 2026 and 2028. Let's mark our calendar! The caveat is that this can be achieved only with scaling-out their quantum processors, assembling several units of 64 qubits through photonic links in a distributed computing manner.

IonQ announced in August 2021 their Reconfigurable Multicore Quantum Architecture (RMQA) detailing how they would create 64 ions chipsets ([video](#)). It will assemble 4 chains or lines of 16 ions, 12 being usable as qubits and the 4 remaining for cooling, in a single chipset manufactured on a glass support (Evaporated Glass Traps) replacing their previous silicon based platform built by Sandia Labs. These chunks of 16 ions can be moved around, paired and entangled, to create dynamic 32 ions units. IonQ stated that this architecture could scale-up and support even more blocks of 16 ions. Well, if that actually works in practice, why not!



At last, a team associating IonQ, Duke University in Durham and ColdQuanta published an interesting paper describing the architecture of a trapped-ions systems cryostat from Montana Instruments that is optimized to minimize the vibrations coming from the pulse tube.

This seems to be one of the figures of merit to ensure the stability of the trapped ions qubits and their control devices like lasers<sup>647</sup>. The qubits are cooled at 5K while laser-based cooling using the Doppler effect cool it at an even lower temperature.



In March 2020, **Honeywell** announced that it had developed a quantum computer that would be the most powerful in the world and double the power of the previous record that was held by IBM<sup>648</sup>. The initial announcement was for a four-qubit trapped ions-based quantum processor<sup>649</sup>. The power doubling was evaluated using IBM's quantum volume.

They started with their 4 qubits prototype then launched their H0 system in June 2020 with 6 qubits<sup>650</sup> and their H1 system in October 2020 with 10 qubits with an initial quantum volume of 128 (7 qubits x 7 gates depth). The physical layout is still linear (1D). Their 2D architecture will come with the H2 generation expected in 2021 or 2022.

Their quantum volume with 10 qubits reached 512 in March 2021 (9x9 qubits). Single-qubit gate fidelity is above 99.991% and two-qubit gate fidelity above 99.76% while readout fidelity is at 99.75% with a measurement crosstalk at 0.2%, characterized as the decay of a qubit coherence in an equal superposition state, while repeatedly measuring the nearest qubit<sup>651</sup>.

They are using the mid-circuit measurement and qubit reuse technique (MCMR) which can be used to optimize the length of quantum algorithms.

Honeywell is using **trapped ion QCCD**, for "quantum charge-coupled device". It uses ytterbium-based ions coupled with barium ions to cool the device.

This technique was developed in 2002 by Christopher Monroe, David Wineland and Dave Kielpinski<sup>652</sup>. Honeywell is reusing many other works from other research laboratories spread out between 2008 and 2012.

Ions are generated from a jet of collimated atoms obtained by heating a solid ytterbium target. They are then "hit" by a laser, which removes an electron from the valence layer of the atom (the last one). Only one electron remains in this layer, giving rise to an ion with a positive charge, Yb+. The laser cooling of these ions is well-controlled thanks to their favorable energy level pattern. Thanks to their electrical charge, it is possible to trap and move these atoms using electrostatic and radiofrequency potentials.

---

<sup>647</sup> See [High stability cryogenic system for quantum computing with compact packaged ion traps](#) by Robert F. Spivey et al, August 2021 (12 pages). ColdQuanta seems involved here given a cold-atoms system can reuse some of the experimental setting crafted for trapped-ions. Interestingly, in its 2021 investor presentation, IonQ pretended that their system was operating at room temperature!

<sup>648</sup> See [Honeywell Achieves Breakthrough That Will Enable The World's Most Powerful Quantum Computer](#) and [How Honeywell Made the Leap into Quantum Computing](#) by Honeywell, March 2020. In Honeywell [has it created the world's most powerful quantum computer?](#), March 2020, I analyze the ad in detail, with the text embedded in the ebook as a compacted version.

<sup>649</sup> The performance is described in detail in: [Demonstration of the QCCD trapped-ion quantum computer architecture](#) by J. M. Pino et al, 2020 (8 pages). This can be complemented by the presentation [Shaping the future of quantum computing](#) by Tony Uttley, the head of Honeywell's quantum team at the Q2B conference at QC Ware in California in December 2019 ([slides](#)).

<sup>650</sup> And we need to distance ourselves from the press headlines on the subject as in [Honeywell says it's got the fastest quantum computer on the planet For now...](#) by Stephen Shankland in C-Net, June 2020.

<sup>651</sup> See [Get to Know Honeywell's Latest Quantum Computer System Model H1](#) by Honeywell, October 2020.

<sup>652</sup> It is described in [Architecture for a large-scale ion-trap](#), 2002 (4 pages).

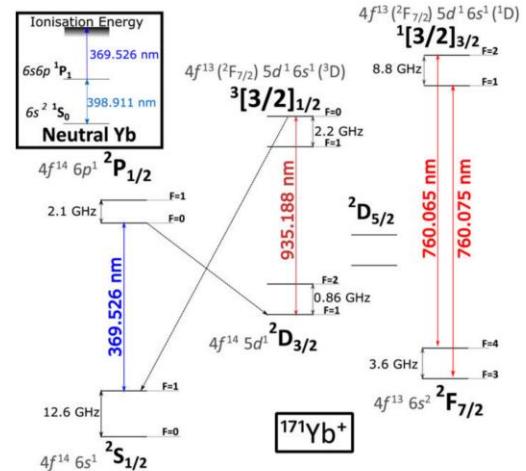
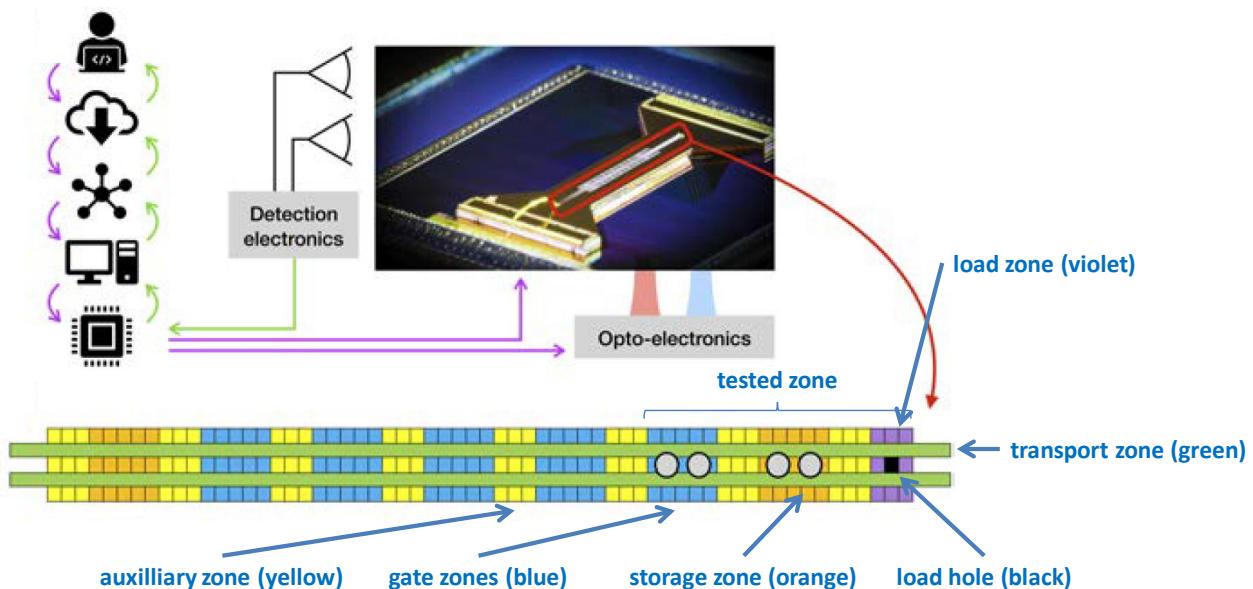
The ions quantum states correspond to two "hyperfine" energy states related to the interaction between the magnetic moment of the nucleus and that of the electrons of the ion. These hyperfine levels are also used in cesium atomic clocks. The transition frequency between the two hyperfine levels of ytterbium is 12.6 GHz<sup>653</sup>. The hyperfine states of the ytterbium ion are well suited for quantum computation because they are very stable, which allows them to have a long coherence time.

Honeywell's quantum processor ions are **shuttling ions**. This is a rare case of shuttling qubits, the other one being shuttling electrons. Usually, qubits based on electrons, cold atoms or ions don't move (too much) where they are installed. This idea was proposed in 2002 by Dave Wineland and co. This would be the first complete realization and the result of a lot of engineering work.

Their system is based on a conventional system that prepares ytterbium atoms, ionizes them and sends them into a hole that feeds the chipset. It then uses about ten ion storage and sorting areas (in orange, yellow and blue in the diagram *below*).

The ytterbium ions are confined above a rail of three rows of electrodes whose variable voltage allows to control their position and to move them laterally. The aim of Honeywell's experiment is to be able to demonstrate logical operations between several qubits - now, up to 10 - while moving them at will between storage areas and interaction areas during operations.

The system uses 198 DC electrodes for controlling the displacement and positioning of ytterbium ions coupled with barium ions used for cooling. The chip uses cryogenic surface traps that dynamically rearrange the positioning of the ytterbium/barium ion pairs and implement quantum gates running in parallel on several areas of the circuit.



**Figure 2:** Partial term schemes showing the driven atomic transitions and the required laser wavelengths and microwave frequencies. The inset shows the transitions in neutral ytterbium used for photoionization. The main diagram shows the  $^{171}\text{Yb}^+$  term scheme.

<sup>653</sup> See [Laser-cooled ytterbium ion microwave frequency standard](#) by S. Mulholland et al, 2019 (16 pages).

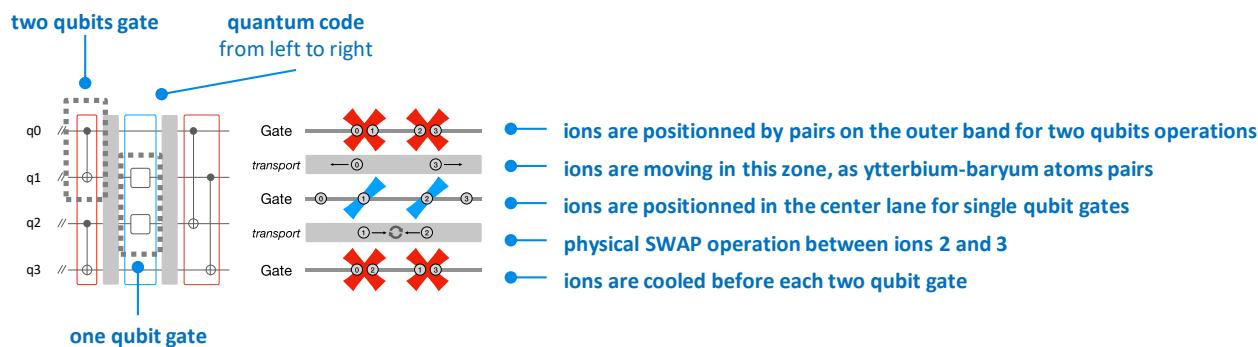
Ions circulate above the green band, allowing arbitrary movements of the ions along the band. Once positioned, they are transferred to the middle band to get submitted to a single qubit quantum gate, or in the side bands for two-qubits quantum gates, as explained in the diagram *below*. One of these operations is a SWAP gate that allows the ions to be physically interchanged.

The disadvantage of the technique is its slow quantum gates. The time required to configure the ions to create a quantum gate is 3 to 5 ms, which is not negligible, especially for algorithms that require a large number of quantum gates.

The system operates at a temperature of 12.6K and with a temperature stability of 2mK which avoids disturbing the ions and their superposed and entangled quantum states. Helium cooling is complemented by a so-called "sympathetic cooling" technique which combines the use of Doppler effect and Raman cooling on the barium ions next-door to the ytterbium ions. The Coulomb interaction between the barium ions cools the ytterbium ions next to the barium ions. A barium ion cooling operation takes place before each two-qubit gate execution.

Ion laser cooling has been operating at room temperature for more than 30 years. Like many research groups, Honeywell cools the ion trap (to 12.6K) to minimize the effect of abnormal ions heating, which is a major problem that is not fully understood. This abnormal heating is greatly reduced when the trap is cooled.

The system is built around four-qubit chunks and uses one- and two-qubit **quantum gates** that are activated by lasers, via the Raman effect that requires a pair of beams. The single-qubit gates are activated by a pair of 370.3 nm Raman beams in circular polarization. The system allows the generation of X, Y and Z gates for which quarter and half turns are performed around the three axes of the Bloch sphere. These rotations are done with very high precision according to Honeywell. This ensures a minimum error rate for single-qubit quantum gates.



Two-qubit gates use two additional pairs of laser beams that act on pairs of ytterbium atoms that have been brought closer together by the circuit's positioning control electrodes. Two ions are thus moved by the electrodes into the same potential well before being coupled by laser. The qubits can then be separated and moved elsewhere to interact with other qubits.

**Qubits state readout** is performed with a classical imager that detects the energetic state of the ions via their laser-activated fluorescence. This imager is a "PMT array", i.e. a linear array of photomultipliers (Photo-Multiplier Tubes). Their architecture allows a qubit readout during processing, without disturbing the neighboring qubits. This would allow the implementation of conditional logic, with IF THEN ELSE like with classical programming.

Finally, the system includes an FPGA programmable electronic circuit for the control of the qubits, sitting outside the cryogenic enclosure.

The **performance of their qubits** seems very good. The error rate would be only around 2% after executing a hundred quantum gates. This allows running deep quantum algorithms with a large number of quantum gate sequences.

This compares to a depth of about 20 quantum gates executed with the 53 superconducting qubits of Google's Sycamore chipset. They also showcase a small crosstalk between qubits pairs, i.e. independent qubits do not seem to interfere with their neighbors, except of course when they are entangled.

Honeywell says its architecture would be scalable, keeping this low error rate with scaling. To date, they have only implemented 10 qubits! They are considering a three-step ramp-up approach. For now, they are using a "1D" trapped ion bar. In the next two steps, they would move to a "2D" bar that would allow them to move the ions in two directions, allowing them to accumulate more of them and connect them with their neighbors in two dimensions. It will take some time to perfect this.

As already mentioned in the QEC section, page 212, in July 2021, HQS announced the creation of the first logical qubits using color codes with their 10 trapped-ions qubits<sup>654</sup>.

Honeywell started this investment in quantum computing in 2016 but in "stealth" mode, without communicating around it. This was, however, known because they hired researchers in various American universities. Their team now comprises over a 150 people, including physicists, engineers and developers. They come in particular from the NIST laboratory in Boulder and the University of Colorado. There are also alumni from the University of Maryland and Christopher Monroe's team (IonQ).

Honeywell is touting several partnerships: with **Microsoft**, for the integration of its quantum accelerators in Azure Quantum which became operational in July 2020, an investment in the **Cambridge Quantum Computing** (2014, UK, \$22.4 raised in total) and **Zapata Computing** (2017, USA, \$64M).

These will develop software tools for Honeywell machines. And then a partnership with **JPMorgan Chase** to create quantum algorithms in the financial sector. In June 2021, Honeywell announced it was spinning-off its quantum business (Honeywell Quantum Systems) and merging it with **Cambridge Quantum Computing** (UK) with an investment of about \$300M for a stake of 55% in the resulting company<sup>655</sup>. The merged company was renamed as **Quantinuum** in December 2021.

Their first customers include **DHL**, **Merck**, **Accenture** and **Samsung**, who works on new batteries designs. All of this for pilot projects given the number of available qubits is way too small to enable production grade applications.



**Alpine Quantum Technologies** or **AQT** (2017, Austria, \$34.8M) is a spin-off from the University of Innsbruck created by Rainer Blatt, Peter Zoller and Thomas Monz.

Their funding is currently of public origin, coming from the Austrian Ministry of Research.

AQT pilots its microwave trapped ions without the use of lasers, which simplifies the device. They use only one laser for photoionization, which creates the ions at start-up, and another for measuring the qubit state by fluorescence after calculations. The fidelity of their qubits is 99.6% for two qubits and drops to 86% for 10 qubits<sup>656</sup>.

---

<sup>654</sup> See [Realization of real-time fault-tolerant quantum error correction](#) by C. Ryan-Anderson et al, HQS, July 2021 (22 pages).

<sup>655</sup> See [Honeywell Quantum Solutions And Cambridge Quantum Computing Merge With Go-Public In Mind](#) by Paul Smith-Goodson, June 2021.

<sup>656</sup> See [Characterizing large-scale quantum computers via cycle benchmarking](#) by Alexander Erhard et al, 2019 (13 pages).

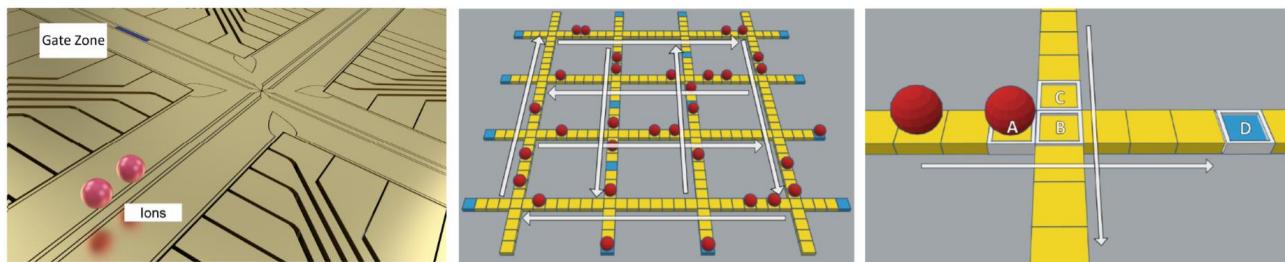


**Oxford Ionics** (2019, UK) is a spin-off from the Department of Physics at Oxford University developing a quantum computer based on trapped ions and low-noise control electronics.

They were originally called Nqie Limited. The company was founded by Thomas Harty and Christopher Ballance and also includes Jochen Wolf, all from Oxford University.



**Universal Quantum** (2018, UK, \$4.5M) is a spin-off from the Ion Quantum Technology Group at the University of Sussex in the UK led by Winfried Hensinger. They are developing a trapped ion system that uses microwaves transmitted by electrical circuits, and magnetic fields to control them instead of lasers.



They actually use penning traps which are well known. The company presentation [video](#) gives the impression that they use a 2D process similar to Honeywell's<sup>657</sup>. The cooling required is around 70K, which is done with liquid nitrogen.

They still need to use lasers at least for the Doppler based ions cooling during their preparation, then for the qubit state readout combining the usual laser excitation and fluorescence readout with a CMOS or CCD sensor<sup>658</sup>.



**Aquabits** (2021, Canada) is developing a trapped ions qubit processor using ‘aquaporins’, that trap ions inside artificial water channels. It is supposed to avoid using lasers and micro-nano fabrication techniques, making these qubits highly scalable. There’s no public way to find out how all these qubits are controlled, entangled and measured.



**Quantum Factory** (2018, Germany) wants to commercialize quantum computers based on trapped ions as resources in the cloud.



**eleQtron GmbH** (2020, Germany) develops a NISQ trapped ions quantum computer. They use their Magnetic Gradient Induced Coupling (MAGIC) to control the qubits. The project involves the University of Siegen and Infineon.

<sup>657</sup> The ion routing process is described in [Efficient Qubit Routing for a Globally Connected Trapped Ion Quantum Computer](#) by Winfried Hensinger et al, February 2020 (13 pages). This is the origin of the illustration used in these lines.

<sup>658</sup> The ion control process with Penning Traps used by Universal Quantum seems to be described in [Microfabricated Ion Traps](#) by Winfried Hensinger et al, 2011 (28 pages).

## Cold atoms qubits

Cold atoms are another atomic form of qubits in addition to trapped ions<sup>659</sup>. They are both trapped, but not exactly in the same way. Since these atoms are not used in ionized form, they are not trapped with electrodes. Lasers are used to control atom's positions. Beams are sent in several directions using the method of "optical tweezing" or optical traps<sup>660</sup>. It can be combined with magnetic traps.

The atom elements are part of the first column in the table of elements with a single electron in the valence layer, such as hydrogen, sodium, lithium, cesium, dysprosium, praseodymium or rubidium, the last one being the most commonly used. This alkaline metal has interesting energy transitions that correspond to common lasers wavelengths as well as easily generated microwaves between 3 and 10 GHz. It is possible to manage with them so-called closed transitions which allow, with lasers, to make atoms transit between several states in a cyclic and controlled manner. On top of that, states are stable long enough to perform computations, i.e. about a hundred microseconds.

Cold atoms are also used in so-called Rydberg states, which correspond to a very high level of energetic excitation, between 50 and 100 electron quantum number (layer position in atom against Bohr's model, labelled n or N). This creates very large electron orbits, magnified by  $N^2$ . These high energy states are used to create entanglement between atoms and thus to operate multi-qubit quantum gates. These excited states have a fairly good stability level of about 100  $\mu$ s. They are several orders of magnitude longer than the classical excited states (hyperfine, used for qubit states). This stability is somehow equivalent to the coherence time of superconducting qubits.

It also exploits a Rydberg blockade effect, where a Rydberg atom excited with a high energy level (with  $n > 50-70$ , n being the quantum energy level of an electron around the nucleus of an atom) will prevent neighboring atoms from reaching this level.

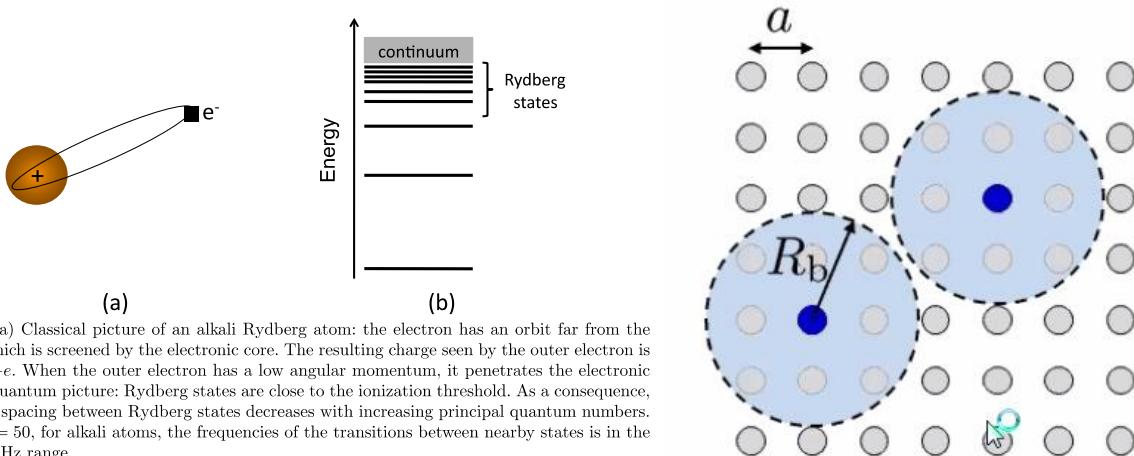


Figure 1: (a) Classical picture of an alkali Rydberg atom: the electron has an orbit far from the nucleus, which is screened by the electronic core. The resulting charge seen by the outer electron is therefore  $+e$ . When the outer electron has a low angular momentum, it penetrates the electronic core. (b) Quantum picture: Rydberg states are close to the ionization threshold. As a consequence, the energy spacing between Rydberg states decreases with increasing principal quantum numbers. Around  $n = 50$ , for alkali atoms, the frequencies of the transitions between nearby states is in the 10 – 100 GHz range.

When excited, these atoms behave like accentuated dipoles, the orbit of the electrons of the valence layer being very inclined as shown here<sup>661</sup>. They also have a disproportionate size of up to one micron ( $\mu\text{m}$ ) in diameter for  $n=100$  with  $^{87}\text{Ru}$ . This is close to being in an ionized state<sup>662</sup>.

<sup>659</sup> See this excellent review paper: [Quantum simulation and computing with Rydberg-interacting qubits](#) by Manuel Agustin Morgado and Shannon Whitlock, Laboratory of Exotic Quantum Matter, University of Strasbourg, December 2020 (28 pages).

<sup>660</sup> See [Quantum information processing with individual neutral atoms in optical tweezers](#) by Philippe Grangier, (47 slides).

<sup>661</sup> Diagram source and detailed explanations in [Interacting Cold Rydberg Atoms: a Toy Many-Body System](#) by Antoine Browaeys and Thierry Lahaye, 2013 (20 pages).

<sup>662</sup> This [presentation of 52 slides](#) from 2014 describes well the history and geometry of the Rydberg atoms.

Their electromagnetic characteristics make the atoms react with their neighbors whose excitation they block at Rydberg within a perimeter of up to 20  $\mu\text{m}$ , which is huge at the atomic scale.

In addition to quantum computing, an activated Rydberg atom can be excited by lasers to generate well-isolated single photons that can be used in nonlinear optics<sup>663</sup>. This provides yet another source of single photons, in addition to quantum dots. The Rydberg blockade phenomenon is also implemented in cryptography and quantum telecommunications, in spectroscopy and in atomic clocks<sup>664</sup>.

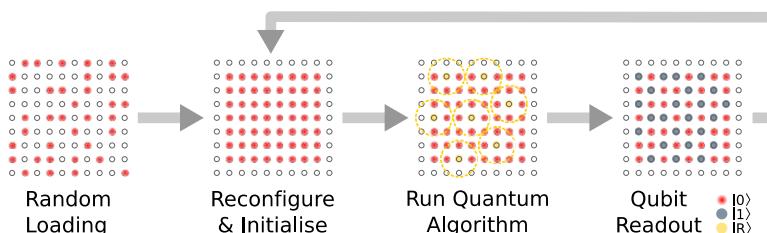
## cold atoms qubits

- long **coherence time**.
- **identical atoms**, that are controlled with the same laser and micro-wave frequencies.
- **reuse trapped ions qubits tools** for qubits readout using fluorescence.
- useful also in **simulation mode**.
- no need for specific **integrated circuits**.
- uses **standard apparatus**.

- **acceptable quantum gates error rate** although not “best in class”.
- **cross-talk** between qubits.
- **adapted to simulation** more than to universal gates computing.
- control **lasers and optical** not scaling well beyond one thousand qubits with the current state of the art.

Rydberg atoms are finally also used to create quantum memories<sup>665</sup>. Topological states allowing to create more reliable qubit-based computing systems are also studied<sup>666</sup>.

The qubits are arranged in a 2D<sup>667</sup> or 3D matrix in space<sup>668</sup>. They are cooled, controlled and positioned by several lasers organized in precision "optical tweezers". A qubit can be based on a single atom or on a group of atoms depending on the methods used. The atoms are prepared with a cold source of some  $\mu\text{K}$  which then feeds a vacuum chamber where laser control takes place<sup>669</sup>.



**Figure 2.** Schematic of a Rydberg array quantum computer. Atoms are initially loaded stochastically, followed by rearrangement to achieve a defect free qubit register. Coherent excitation to Rydberg states allows implementation of quantum algorithms exploiting long-range interactions to couple neighbouring qubits, followed by state-selective readout which is repeated many times to tomographically reconstruct the output state.

<sup>663</sup> See [Observation of coherent many-body Rabi oscillations](#) by Yaroslav Dudin and Alex Kuzmich, GeorgiaTech, 2012 (5 pages) and [Nonlinear quantum optics mediated by Rydberg interactions](#) by Sebastian Hofferberth et al, 2016 (26 pages).

<sup>664</sup> See [Photon-Mediated Quantum Information Processing with Neutral Atoms in an Optical Cavity](#) by Stephan Welte, 2019 (124 pages).

<sup>665</sup> See [Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble](#) by Julien Laurat et al, 2018 (6 pages) and [Experimental realization of 105-qubit random access quantum memory](#) by N. Jiang et al, 2019 (6 pages).

<sup>666</sup> See [Topologically protected edge states in small Rydberg systems](#) by Antoine Browaeys et al, 2018 (6 pages) and [Observation of a symmetry protected topological phase of interacting bosons with Rydberg atoms](#) by Antoine Browaeys, Thierry Lahaye et al, 2019 (20 pages). Quantum simulation using cold atoms is also a tool to simulate topological matter. See [Scientists unveil first quantum simulation of 3-D topological matter with ultracold atoms](#) by Hong Kong University of Science and Technology, July 2019.

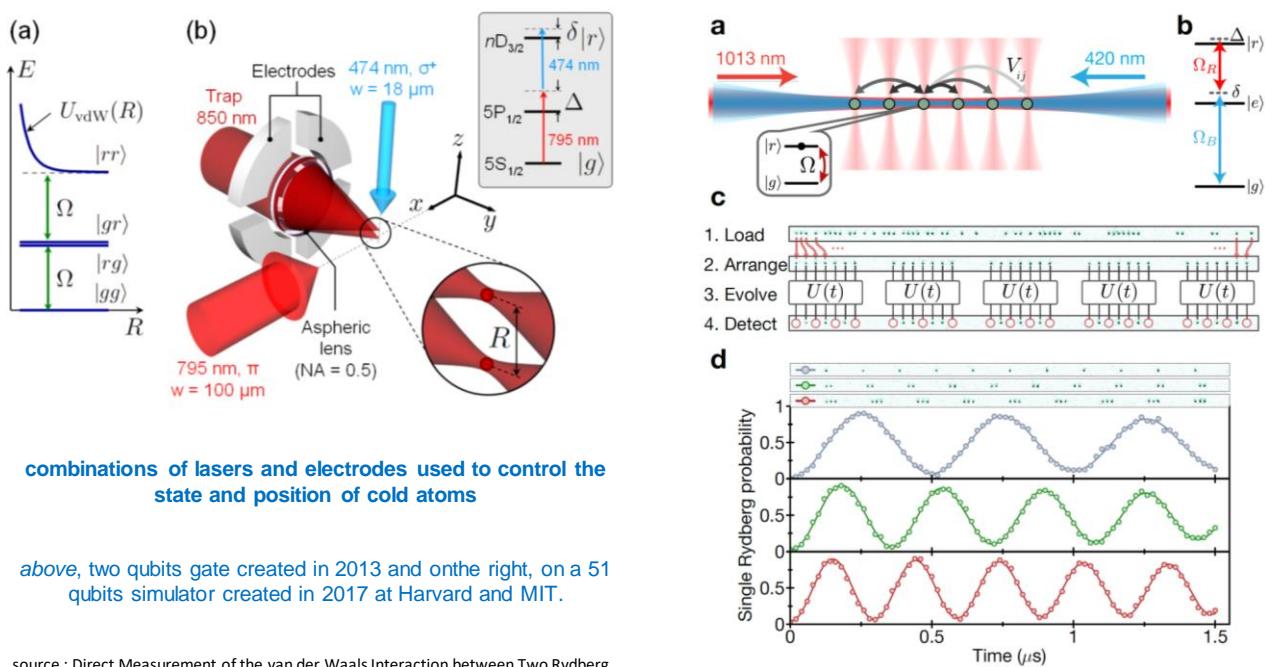
<sup>667</sup> See the thesis [Rydberg interactions in a defect-free array of single-atom quantum systems](#) by Daniel Ohl de Mello, 2020 (147 pages) which describes the way to fill a 2D matrix of a hundred heavy atoms.

<sup>668</sup> See [Three-Dimensional Trapping of Individual Rydberg Atoms in Ponderomotive Bottle Beam Traps](#) by Antoine Browaeys, Thierry Lahaye et al, 2019 (8 pages).

<sup>669</sup> Diagram source: [Rydberg atom quantum technologies](#) by James Shaffer, 2019 (24 pages).

The general principle of these qubits is as follows:

- **Quantum state** generally uses two hyperfine states separated by a microwave frequency energy level to define the  $|0\rangle$  and  $|1\rangle$  qubit basis states. These are two relatively stable excited energy states above the ground state of the atom.
- **Single-qubit quantum gates** are activated by a mix of microwaves (a few GHz, compatible with hyperfine states) and laser pumping to change the energy state of the cold atom between its ground and hyperfine states. These gates can also use Raman transitions driven by lasers on two frequencies or by a combination of the Stark effect of spectral line shifting under the effect of an electric field and microwaves. The best single-qubit gate fidelities are around 99.6% with a long-term objective of reaching an error rate of  $10^{-4}$ <sup>670</sup>. Fortunately, there are optical systems for multiplexing laser beams, which make it possible to avoid having more lasers than qubits.



- **Two-qubit quantum gates** also use microwaves and lasers<sup>671</sup>. They are applied to atoms in their excited (Rydberg) state, which projects its valence layer electrons into a high orbit. For rubidium, there is only one electron to manage in this layer. These quantum gates can in practice implement more than two qubits. The fidelity of two qubit gates was quite low in 2016 with a maximum of 75% with rubidium and 81% in 2016 with cesium. It had increased to a better level of 97% in 2019<sup>672</sup>. The decoherence of cold atoms qubits has different origins: photoionization, spontaneous emission of photons, transitions induced by black body radiation, stability of control lasers and laser pulse timing and precision control of atoms in space<sup>673</sup>.

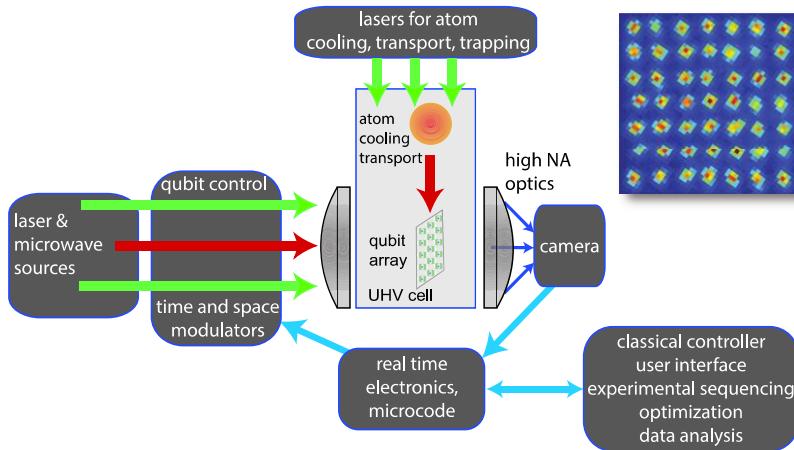
<sup>670</sup> See [High-Fidelity Control, Detection, and Entanglement of Alkaline-Earth Rydberg Atoms](#) by Ivaylo Madjarov, January 2020 (13 pages) which uses strontium.

<sup>671</sup> In August 2019, American researchers were able to create multi-qubit quantum gates with 95% fidelity based on cold atoms. See [Parallel implementation of high-fidelity multi-qubit gates with neutral atoms](#) by H. Levine et al, August 2019 (16 pages). Two-qubit gate bases in [Direct Measurement of the van der Waals Interaction between Two Rydberg Atoms](#) by Lucas Béguin, Antoine Browaeys et al, 2013 (5 pages).

<sup>672</sup> According to [Rydberg atom quantum technologies](#) by James Shaffer, 2019 (24 pages), page 10.

<sup>673</sup> Source: [Quantum Computing with Neutral Atoms](#), 2013 (42 slides).

- **Qubit readout** uses a CCD camera that detects the atoms fluorescence with a method similar to the one used with trapped ions and NV centers. On the right is a simplified description of a system of cold atom qubits with laser and microwaves-based control tools and qubit measurement using fluorescence and a camera<sup>674</sup>.



In general, cold atom-based systems operate at temperatures below 50 mK and in ultra-high vacuum. In practice, it is the ultra-high vacuum and the atoms laser cooling that ensures this thermalization. It is not necessary to use dilution refrigerators as with superconducting and silicon qubits.

The most active research laboratories with cold atom-based qubits are in the USA (University of Wisconsin, Colorado, Harvard, Caltech, GeorgiaTech), in the UK at the University of Cambridge, in Austria at the University of Innsbruck and the University of Vienna, Germany (Max-Planck Institute, Free University of Berlin, University of Stuttgart) and in France, in particular at the Charles Fabry Laboratory of the Institute of Optics in Palaiseau. This led to the creation of **Pasqal** (France), supported by the abundant research work of its co-founders Antoine Browaeys and Thierry Lahaye, who have been active on the subject for over ten years. In France, the **Unistra** laboratory in Strasbourg is also working on cold atoms computing, run by Shannon Whitlock, part of the project **aQCess**. Other startups are positioned on cold atoms: **Atom Computing** (2018, USA), **ColdQuanta** (USA) and **QuEra Computing** (2020, USA).

Finally, the European H2020 **AtomQT** project covers research in cold atoms, both qubits and metrology. In France, it involves the Bordeaux Optics Institute (Philippe Bouyer) and the LPMMC in Grenoble.

The first qubit systems based on cold atoms are for the moment rather simulators and not yet universal calculators<sup>675</sup>. In 2017, Mikhail Lukin's team from **Harvard** University and a team from **MIT** assembled 51 rubidium atoms<sup>676</sup>. It went up to 256 qubits in July 2021<sup>677</sup>. Antoine Browaeys's team at **Institut d'Optique** reached 72 cold atoms in a 3D structure in 2018 and 196 in 2020<sup>678</sup>.

<sup>674</sup> See [Quantum computing with atomic qubits and Rydberg interactions: Progress and challenges](#) by Mark Saffman, 2016 (28 pages), from which the schematic is extracted.

<sup>675</sup> See [Toward quantum simulation with Rydberg atoms](#) by Thanh Long Nguyen, 2016 (182 pages), [Quantum simulations with ultra-cold atoms in optical lattices](#), 2017 (8 pages), [Tunable two-dimensional arrays of single Rydberg atoms for realizing quantum Ising models](#) by Thierry Lahaye and Antoine Browaeys, 2017 (13 pages), [Quantum read-out for cold atomic quantum simulators](#), par J. Eisert et al, 2018 (20 pages), [Quantum critical behaviour at the many-body localization transition](#) by Markus Greiner et al, 2018 (10 pages), [Quantum Kibble-Zurek mechanism and critical dynamics on a programmable Rydberg simulator](#) by Alexander Keesling et al, 2019 (16 pages) and [Many-body physics with individually controlled Rydberg atoms](#) by Antoine Browaeys and Thierry Lahaye, 2020 (14 pages).

<sup>676</sup> See [Quantum simulator with 51 qubits is largest ever](#) by Matt Reynolds, 2017 which refers to [Probing many-body dynamics on a 51-atom quantum simulator](#) by Hannes Bernien, Mikhail Lukin et al, 2017 (24 pages).

<sup>677</sup> See [Harvard-led physicists take big step in race to quantum computing](#), Harvard, July 2021. Their work is like Pasqal/IOGS based on the same technique with rubidium atoms and SLM tweezers.

<sup>678</sup> See [Synthetic three-dimensional atomic structures assembled atom by atom](#) by Daniel Barredo, Antoine Browaeys et al, 2018 (4 pages).

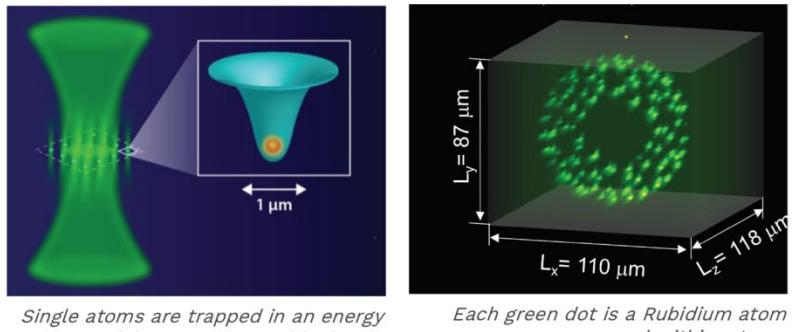
**Pasqal** (2019, France, 25M€) is the first quantum computing startup in France based on cold atoms. They use magnetically confined rubidium atoms cooled by Doppler laser to reach mK and with a variant of the Atomic Sisyphus effect to go down to 30  $\mu\text{K}$ <sup>679</sup>.

The atoms are trapped in 2D matrices or 3D toric structures with a spacing of a few microns between each of them. They are managed with two levels of energy. Quantum gates are laser-activated to control the energy state of the atoms. Qubits entanglement comes from atoms excitation in the Rydberg state which allows them to interact with other at long distance<sup>680</sup>.

Pasqal plans first to implement quantum simulators and then, to move to gate-based quantum computing<sup>681</sup>.

The technology would allow to quickly reach about 100 quality qubits and then a thousand by 2023<sup>682</sup>. They are already able to control two hundred atoms in the laboratory. They are initially positioned on the PQS (Programmable Quantum Simulator, or analog quantum computers) and then on the NISQ (Noisy Intermediate-Scale Quantum), computers using universal quantum gates<sup>683</sup>.

In terms of qubits performance and quality, they reach a coherence time of 1 ms with 1  $\mu\text{s}$  gates (for a CNOT), which is enough to reach a thousand quantum gates, excluding error correction codes. The gate error rate would be 3% and the readout error rate at 1%, which is quite reasonable, at least for quantum simulators.



The computer will eventually fit into a 4-unit wide data center rack and will operate at room temperature and under vacuum. It is based on standard components and does not require the creation of specific chipsets as it is the case for all other types of qubits.

In April 2020, startups **Pasqal** and **Muquans** announced a partnership that had been in preparation for a long time and on the use of a Muquans lasers system to control the cold atoms.

Milestone scientific papers and achievements happened between late-2020 and mid-2021, led by Pasqal and by the research team at IOGS behind Pasqal's cold-atom-based system.

<sup>679</sup> This method also uses lasers emitting orthogonally polarized photons. The method was invented by Claude Cohen-Tannoudji who was awarded the Nobel Prize in Physics in 1997.

<sup>680</sup> See [Quantum Computing with Arrays of Atoms](#) by Lucas Béguin and Adrien Signoles from Pasqal, April 2020, which details the functioning of the startup's quantum processors. And their white paper [Quantum Computing with Neutral Atoms](#), June 2020 (41 pages). They could be awarded a golden medal for the scientific documentation of a quantum startup!

<sup>681</sup> See [Microwave-engineering of programmable XXZ Hamiltonians in arrays of Rydberg atoms](#) by P. Scholl et al, July 2021 (9 pages) which presents an hybrid analog-digital architecture based on Hamiltonian evolutions and one-qubit gates;

<sup>682</sup> Rydberg atoms have unsuspected uses, such as managing random music. See [Quantum music to my ears](#), June 2019. This is a change from music generated by deep learning!

<sup>683</sup> Qubits encoding will be different according to the use case. For gate-based computing, qubits are encoded with two hyperfine ground states. For Ising-like Hamiltonian, qubits use a ground state and a Rydberg state and for XY exchange Hamiltonian, they use two Rydberg states.

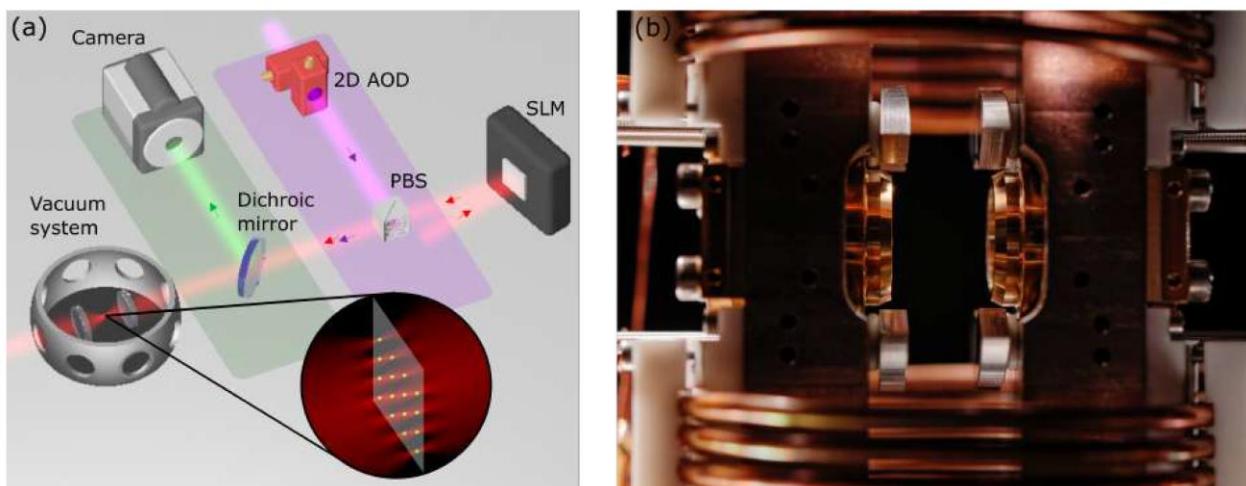
The first one from December 2020 describes how a 2D matrix of 196 qubits was assembled using optical tweezers created with an SLM (a high-resolution Spatial Light Modulator) and an optimized arrangement technique using fewer than 200 steps<sup>684</sup>.

These SLMs enable phase grading and controlling phases spatial pattern. This atoms-positioning system will be extended to 3D arrays.

All this will lead Pasqal to launch their system with 100 and 200 qubits between 2021 and 2022<sup>685</sup>.

This 196 cold-atoms setup was then used to program an Ising model simulating ferromagnetism and enabling quantum simulation, with 100 active qubits<sup>686</sup>. This was a result of a research funded through the European Flagship PASQuanS project in partnership with labs from Spain, Germany and Austria.

Then came a real-world problem, the optimization of smart-charging of electrical vehicles co-developed with EDF, using a QAOA hybrid algorithm and classical emulators of Pasqal systems and the QLM emulator from Atos<sup>687</sup>. It was also funded through the PASQuanS flagship project.



The cold atom-based qubit control system includes a spatial light modulator (Spatial Light Modulator, SLM, based on LCoS liquid crystals<sup>688</sup>) that controls the phase of the transmitted light of the atoms in a focal plane with optical micro-traps. Laser tweezers or traps/pinches for rearranging the atoms are controlled by the AOD (Acousto-Optic laser beam Deflector) and added to the beam from the SLM by a birefringent filter. The fluorescent light emitted by the atoms during qubit readout is filtered by a PBS (Polarizing Separator Filter) and analyzed by a camera. The atoms of the system are confined in a space of 1 mm<sup>3</sup>.

<sup>684</sup> See [Enhanced atom-by-atom assembly of arbitrary tweezers arrays](#) by Kai-Niklas Schymik, Antoine Browaeys, Thierry Lahaye et al, November 2020 (10 pages).

<sup>685</sup> See [The path to Pasqal's first 200 qubits processors](#) by Pasqal, October 2020.

<sup>686</sup> See [Programmable quantum simulation of 2D antiferromagnets with hundreds of Rydberg atoms](#) by Pascal Scholl, Thierry Lahaye, Antoine Browaeys et al, December 2020 (16 pages). Also published in [Nature](#) in July 2021.

<sup>687</sup> See [Qualifying quantum approaches for hard industrial optimization problems. A case study in the field of smart-charging of electric vehicles](#) by Constantin Dalyac, Loïc Henriet, Emmanuel Jeandel, Wolfgang Lechner, Simon Perdris, Marc Porcheron and Margarita Veshchezerova, 2021 (29 pages).

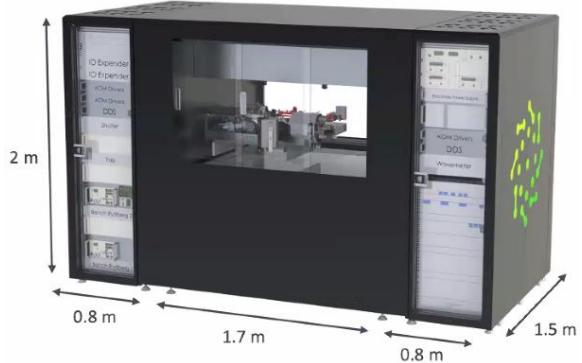
<sup>688</sup> See a description of an SLM in [Spatial Light Modulators](#) by Aurélie Jullien, 2020 (6 pages).

Atos and Ecole Polytechnique researchers also evaluated the specifications of a cold-atom simulator needed to reach some quantum advantage to solve an optimization task, the UD-MIS problem (Unit-Disk Maximum Independent Set problem)<sup>689</sup>.

They found out that over 1,000 qubits were required with a time budget of 0.2 seconds, if and when the system coherence could be improved by a factor ten<sup>690</sup>. This explains the ultimate goal of Pasqal to reach 1,000 qubits at some point in time.

They also designed a PQS model to implement a graph kernel machine learning model although the provided acceleration was not documented<sup>691</sup>.

Pasqal has created its own low-level programming environment that interfaces with high-level programming tools, including support for development platforms such as Google's **Cirq** that is supported in emulation mode, in digital gate-based programming mode<sup>692</sup>, **TensorFlow Quantum** and IBM's **Qiskit**.



In July 2020, **Cambridge Quantum Computing** (CQC) announced their support of Pasqal's qubits with their development tool `tket`.

Pasqal added a partnership with **ParityQC** with a 3 years collaboration to advance quantum optimization and parallelization<sup>693</sup> and released the open-source library Pulse, co-developed with the **Unitary Fund** enabling the control of their processor at the level of laser pulses<sup>694</sup>. They also announced a partnership with **Atos** in November 2020 to integrate a Pasqal accelerator with Atos supercomputers. At last, they also work with **Rahko** as well as with **Multiverse Computing**, in association with Crédit Agricole CIB.

In January 2021, the Italian HPC consortium **CINECA** announced that will use Pasqal's "Fresnel" 100-qubits processor by 2021<sup>695</sup>. The startup was also selected as part of the project HPC-QS from EuroHPC to provide two of their systems to HPC public datacenters, one in Germany (FZ Jülich *aka* Jülich Research Centre) and one in France (GENCI). Both Pasqal systems will be connected to an Atos QLM.

Pasqal funding came through an initial round of 2,5M€ led by Quantonation and Christophe Jurczak who is their chairman, then a 4,5M€ grant from the European Union EIC Accelerator<sup>696</sup>, and finally a second round of funding of 25M€ announced in April 2021.

<sup>689</sup> An MIS problem consists in determining the size of the largest possible independent set in a graph and returning an example of such a set. The Unit-Disk MIS (UD-MIS) problem is the MIS problem restricted to unit-disk graphs. A graph is a unit-disk graph if one can associate a position in the 2D plane to every vertex such that two vertices share an edge if and only if their distance is smaller than unity.

<sup>690</sup> See [Solving optimization problems with Rydberg analog quantum computers: Realistic requirements for quantum advantage using noisy simulation and classical benchmarks](#) by Michel Fabrice Serret, Bertrand Marchand and Thomas Ayral, November 2020 (25 pages).

<sup>691</sup> See [Quantum evolution kernel : Machine learning on graphs with programmable arrays of qubits](#) by Louis-Paul Henry, Slimane Thabet, Constantin Dalyac and Loïc Henriet, Pasqal, July 2021 (19 pages).

<sup>692</sup> See [Quantum circuits on Pasqal devices](#).

<sup>693</sup> See [ParityQC and Pasqal partner to build the first fully parallelizable quantum computer](#), Pasqal, October 2020.

<sup>694</sup> See [Pulser: a control software at the pulse-level for Pasqal quantum processors](#) by Pasqal, January 2021.

<sup>695</sup> See [CINECA-Pasqal agreement on quantum computing](#), January 2021.

<sup>696</sup> See [Europe is betting on quantum computing with neutral atoms](#), Pasqal, December 2020.

**ColdQuanta** (2007, USA, \$71.6M) is a startup created by Dana Anderson, now his CTO, which develops laser-based solutions for cooling cold atoms and also designs a cold atoms-based computer.

It is located in Boulder, Colorado, not far from the NIST Quantum Laboratory. They present this in the form of the Quantum Core (*below left*), a light guide that converges laser beams to control cold atoms that are usually cooled to less than  $50\mu\text{K}$ .

In particular, it is integrated in QuCAL, a complete Bose-Einstein condensate generator, and in the Physics Station, a complete optical device for the control of cold atoms that can be used for various purposes. Atom Chips are chips that can be integrated in these systems including miniaturized cold atom control optics.

The startup uses these generic technologies to create a wide variety of systems, and above all for quantum metrology, especially for geopositioning instead of GPS, microgravimetry or cesium quantum clocks. They also offer ultra-high vacuum pumps for the control of cold atoms, called RuBECi.

Their approach to the market is truly diverse, wondering whether they have real products or whether they are creating custom solutions for large U.S. federal clients. In particular, they have equipped the ISS space station with measuring instruments for NASA and JPL.



They also have ambitions to create a cold atoms-based quantum computer. The company is now positioned to create complete quantum processors based on cold atoms<sup>697</sup>. To do so, they obtained funding from DARPA in April 2020 under the ONISQ program with a \$7.4M collaborative project involving numerous universities and Raytheon. The DARPA asked them to develop a scalable ( $>1000$  qubits) system that can demonstrate quantum advantage on real-world problems. They are partnering with ParityQC (Austria) for development of quantum software targeting optimization problems. Their first 2021 “Hilbert” cloud-based quantum computer will start with 100 qubits, a milestone they announced having reached in July 2021. In May 2021, ColdQuanta joined a couple other quantum computers vendors like Pasqal with supporting IBM’s Qiskit, formally joining the “IBM Quantum Network”. The startup has in excess of 125 people onboard!

**Atom Computing** (2018, USA, \$35M) aims to create a quantum computer based on optically controlled neutral atoms<sup>698</sup>. It is one of the competitors of Pasqal and ColdQuanta.

The startup was launched after analyzing the results of Antoine Browaeys' laboratory at the Institut d’Optique in France.

<sup>697</sup> See [ColdQuanta - Life in Quantum's Slow \(and Cold\) Lane Heats Up](#) by John Russell, April 2020 and the webinar [Powering the Quantum Information Age](#) with Bo Ewald, April 2020 (53 minutes).

<sup>698</sup> Here is some information in [Neutral Atom Quantum Computing](#) by Anderson Group Optical Physics and in [Quantum computing with neutral atoms](#) by David Weiss 2017 (7 pages).

This illustrates the issue of timing in the race to create quantum computing startups even with unmatured technologies. They demonstrated in October 2021 their 100-qubit Phoenix system.



**QuEra Computing** (USA, 2020, \$17M) develops a cold atom gate-based quantum computer. The startup was created by researchers from Harvard University and MIT.

With Nathan Gemelke, Alexei Bylinskii, Shengtao Wang and Mikhail D. Lukin, among others, who is one of their scientific advisors<sup>699</sup>. They published a research paper on a 2D array 256 programmable cold atom system in 2021 and announced in November 2021 it would become a commercial product<sup>700</sup>. They didn't make it clear whether/or its would be a quantum simulator or a gate-based quantum computing system beyond saying that it would be used to solve "specific problems" including optimization tasks.



**BraneCell Systems** (2015, Cambridge Massachusetts and Dusseldorf, \$1.8M) is a startup launched by Wassim Estephan and Christopher Papile.

It develops a quantum processor operating at room temperature. It is in fact a system using cold atoms with a process that is very similar to what Pasqal is doing. The idea is to allow to run quantum programs in a decentralized way and not in data centers<sup>701</sup>! They have filed a few patents, including USPTO patent 9607271, validated in March 2017<sup>702</sup>.

## Photons qubits

Contrarily to all the previous qubits, photons have no mass and move at about the speed of light, modulo the optical refractive index of the physical media they pass through. While photons were used everywhere in solid qubits in control and readout features with microwaves or laser beams, they can be used to create qubits exploiting polarization or other physical characteristics such as frequency, amplitude, phase, mode, path or photon number. This is the vast field of linear and non-linear optics. It is found in both the generation of qubits for quantum computation or simulation and with their application in telecommunications and quantum cryptography which we study in [another part](#) of this document (page 605).

Photonics is both an interesting solution for creating qubits as well as a transversal technology that is indispensable to other types of qubits because it is the only one that allows long-distance communications between quantum sensors, quantum networks and quantum computers. Photons are also used directly in quantum sensing, particularly for precision time measurement and even for pressure measurement.

---

<sup>699</sup> See in particular [Parallel Implementation of High-Fidelity Multiqubit Gates with Neutral Atoms](#) by Harry Levine et al, August 2019 (16 pages).

<sup>700</sup> See [Quantum Phases of Matter on a 256-Atom Programmable Quantum Simulator](#) by Sepehr Ebadi, Michail D.Likin et al, 2020 (20 pages) and [This new startup has built a record-breaking 256-qubit quantum computer](#) by Siobhan Roberts, November 2021.

<sup>701</sup> Their communication is cryptic to say the least, as [BraneCell Systems Presents Distributed Quantum Information Processing for Future Cities](#), April 2018 and a partnership announced with the US government service provider, AST, in July 2018 in [AST and BraneCell Announce Their Partnership to Improve Critical Government Functions Through the Power of Quantum Computing](#). They do not provide any technical or popularization information about their solution, qubits and error rates. They were also aiming for an ICO that would have been the first of its kind for a quantum computing startup. Their main goal was to create a secure communication system. They target the financial, energy, health, chemical and public sectors. A Quantum Theranos? At the very least, we have the right to doubt.

<sup>702</sup> Here is the patent description: "*The subject matter relates to multiple parallel ensembles of early stage spherical pulses radiated through engineered arrays forming the foundation for quantized computer processors taking advantage of integer thermodynamics. The materials, architecture and methods for constructing micro- and/or nano-scale three-dimensional cellular arrays, cellular series logic gates, and signature logic form the basis of small- and large-scale apparatuses used to execute logic, data bases, memory, mathematics, artificial intelligence, prime factorization, optical routing and artificial thought tasks not otherwise replicated in electron-based circuits*".

- **stable qubits** with absence of decoherence.
- qubits processing at **ambiant temperature**.
- **emerging nano-photonic** manufacturing techniques enabling scalability.
- **easier to scale-out** with inter-qubits communications and quantum telecommunications.
- **MBQC/FBQC** circumventing the fixed gates depth computing capacity.

- **not yet scalable** in number of operations due to probabilistic character of quantum gates and the efficiency of photon sources.
- **photons can't be stopped or be stored**, they can just be slightly delayed.
- **need to cool photon sources and detectors**, but at relatively reasonable temperatures between 2K and 10K, requiring lightweight cryogenic systems.
- **boson sampling based quantum advantage** starts to being programmable but a practical quantum advantage remains to be proven.

The advantages of photonics are that it allows to manage quite stable qubits with a very low error rate at the quantum gate level thanks to their weak coupling with the environment. The main source of decoherence is related to the optical losses happening with the photons propagation.

Photons also operate at any temperature<sup>703</sup>, do not require expensive nanoscopic manufacturing techniques and can be based on nanophotonic CMOS manufacturing processes<sup>704</sup>.

Their disadvantage lies in the fact that photons are even more probabilistic beasts than any of the other qubits. Scalability issues make it difficult to assemble more than a few dozens of qubits, at least for the moment. Photon sources must be more powerful to accommodate a larger number of entangled qubits.

Current technology developments are based on progresses made with more efficient single photon sources, better photon detectors, non-linear optics, advanced quantum states preparation (multi-mode, spatial or spectral multiplexing, non-Gaussian states) with a larger computing space than traditional two-states qubits, using cluster-states measurement-based techniques (MBQC) to avoid the pitfalls of a physically limited quantum gates depth and quantum error corrections.

## Photonics background

To understand photons in quantum information systems, one needs to get a bit deeper in quantum optics and statistical optics. This section constitutes a very rudimentary primer, enabling you to understand some of the vocabulary used by quantum information photonicians. It can also help us segment the various kinds of photonic qubits like discrete variables and continuous variables qubits.

So far, we've mainly mentioned photons as wave-particles interacting with matter, with the photoelectric effect and atoms energy transitions. But exactly, what are photons? How do we define and classify it?

A photon is a moving perturbation of the electromagnetic field with orthogonal magnetic and electric field variations themselves orthogonal to the photon propagation direction.

Photons are described with their quantum numbers which are:

<sup>703</sup> In general, solid-state light source must be cooled to 10K and the photon detectors output to about 2K to 4K. At least, one avoids going below 1K, which allows the use of cryogenic systems that are satisfied with helium 4 and do not require helium 3. These cryogenic systems are miniaturizable and require much less energy than the dilution systems used for superconducting and silicon qubits.

<sup>704</sup> See [Photonic quantum information processing: A concise review](#) by Sergei Slussarenko and Geoff Pryde of the Centre for Quantum Dynamics and the Centre for Quantum Computation and Communication Technology at Griffith University in Brisbane, Australia (20 pages) which describes the state of the art of photon qubits. This is the source of the diagram. See also the older [Why I am optimistic about the silicon-photonic route to quantum computing](#) by Terry Rudolph, a cofounder of PsiQuantum, published in 2016 (14 pages).

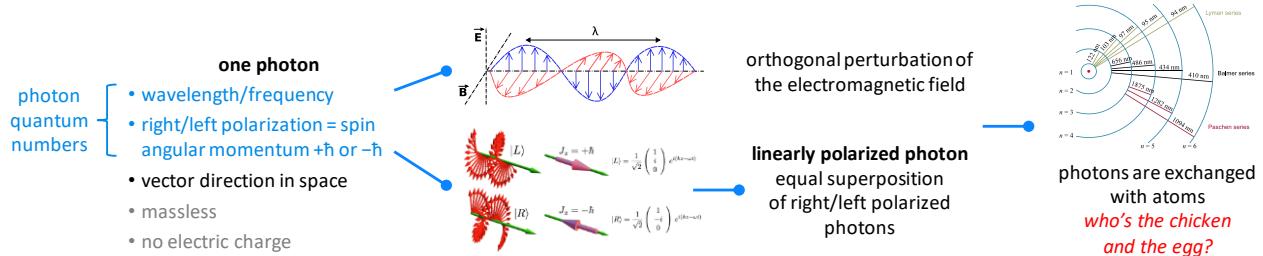
- Their **wavelength** or their frequency. Several photons with same or different frequencies can be coherently superposed and create a “photon number” or a “wavepacket”. Wavepackets are usually generated by femto-lasers pulses, mostly in the visible and infrared ranges, or by digital-to-analog microwave generators like those used to drive superconducting and electron spin qubits.
- Their **circular right or left polarization**, which corresponds to their angular momentum having quantized values  $+\hbar$  or  $-\hbar$ . Any single monochromatic photon is a linear superposition of these two basic circular polarizations, including linearly horizontally or vertically polarized photons.
- Their **orbital angular momentum** where the electromagnetic field is rotating helically along its propagation axis or vector.

Photons are massless, have no electric charge and are stable while moving in vacuum at the speed of light. Their energy and momentum depend only on their wavelength. Photons interact with other particles, mainly electrons either tied to atom nucleus, for photons absorption and/or emission, or free electrons like with the Compton effect. They can be created, destroyed and modified by many of these interactions. Pairs of photons can also be generated by the collision between particles and their antiparticles. Their behavior is mainly described with Maxwell's equations and its derivatives.

**Photon directionality.** Is a photon directional? Textbooks usually make a distinction between spontaneous emission with photons going in any direction, from a lightbulb or the Sun, and stimulated emission, with directional light, coming from lasers. Radio-frequency antennas can also create spherical radiations going in many directions.

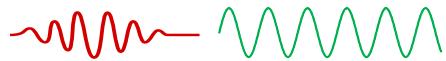
But whatever its source and wavelength, a single photon is mostly always directional and moving in space as a planar wave. A photon electromagnetic wave is represented by orthogonal electric and magnetic fields variations travelling along a vector orthogonal to them. A photon direction can change when it traverses various materials having different refraction indices. Can we have non-planar photons? “Any direction” photons can come from a statistical view of random multidirectional photons emissions or from a coherent superposition of photons emitted in several directions.

With light bulbs, many photons are emitted in various directions by random thermal processes, with various photon wavelengths. Laser coherent light is made of photons with the same wavelength, phase and direction. The distinction between a wave and a point-like particle is as blurred with photons as it is with electrons as far as their exact physical nature and dimensional scope is concerned.



**Photon length** and size are thus notions that are rarely mentioned. According to the Hunter-Wadlinger electromagnetic theory of the photon established in 1985 and verified experimentally for some wavelengths, an optical photon has a shape similar to elongated ellipsoid of length  $\lambda$  and diameter  $\lambda/\pi$ ,  $\lambda$  being the photon's wavelength.

What this means is the usual graphic representations on the right in green are not exact... !



According to other literature, the longitudinal length of a single photon is half of its wavelength ( $\lambda/2$ )<sup>705</sup>. This length's range is quite broad, with 1 nm for X-rays and several orders of magnitude smaller for gamma rays, to over one millimeter and up to several kilometers for radio waves. A classical representation in the above illustration with an EM field of 1,5 wavelengths doesn't correspond to a single photon according to this interpretation, but to three or 1,5 consecutive single photons.

Nothing says that this can represent reality. On top of that, with a photon having half a wavelength, its Fourier transform won't be decomposed with a single frequency, but with some harmonic frequencies. We're safe since this can be explained with Heisenberg's indeterminacy, related here to two complementary properties, the photon length and its wavelengths. In other words, if you try to describe with precision the length of the photon wave (time/space domain), you end up losing precision with its wavelength (energy domain). And vice versa!

**Photon modes** are not that easy to define and their simplified descriptions are diverse. These are defined by coherence and orthogonality properties of the EM field. These are orthogonal solutions of the EM wave equations. Different photon modes do not interfere. The energy of a linear superposition of modes equals the sum of the energy of the individual modes. Only photons with the same mode can be coherent and interfere.

There are two types of photon modes: spatial modes that are transverse to their direction of propagation and temporal modes in the direction of propagation (time and frequency)<sup>706</sup>. We find these multimode photons in various quantum optics setups like with boson sampling experiment that we'll describe a bit later.

**Photon number** is a way to describe groups of similar photons. Several photons with the same wavelength and polarization, can be at the same place and at the same time. They also share the same direction vector. These photons are indistinguishable. This is a property of bosons which are elementary or composite particles with the same quantum characteristics which can get together, following Bose-Einstein statistics, while fermions with the same quantum characteristics can't be together, following Fermi-Dirac statistics.

A group of similar photons form an electromagnetic wave whose energy  $E = h\nu N = \hbar\omega N$ , i.e. the energy of each photon multiplied by the number of added photons having that wavelength<sup>707</sup>.

A photon number is this number of “clustered” photons forming a higher energy EM field than a single photon<sup>708</sup>. You can even create superpositions of multi-photons (or single-mode Fock state as we'll see later) with 0, 1, 2 and 3 photons. This can be used to create photon-number Bell states, namely entangled states of superposed photon numbers<sup>709</sup>. This is head twisting and hard to visualize!

Quantum optics is heavily based on the model of the **quantum harmonic oscillator**, the quantum-mechanical analog of the classical harmonic oscillator, with quantized energy.

<sup>705</sup> See [Electromagnetic fields, size, and copy of a single photon](#) by Shan-Liang Liu, 2018 (4 pages) and [The Size and Shape of a Single Photon](#) by Zhenglong Xu, 2021 (22 pages).

<sup>706</sup> See [The concept of modes in optics and photonics](#) by René Dändliker, 1999 (6 pages).

<sup>707</sup> Here,  $\nu$  is the photon frequency,  $h$  in Planck's constant,  $\hbar$  is Planck's reduced constant or Dirac's constant and  $\omega$  is the photon angular frequency with  $\omega = 2\pi\nu$ , in radians per second,  $2\pi$  radians corresponding to a 1 Hz frequency.

<sup>708</sup> A powerful radio or digital TV emitter is creating these kinds of photons, in the radiowave range! Same for a radar.

<sup>709</sup> See [Generation of non-classical light in a photon-number superposition](#) by J. C. Loredo, Pascale Senellart et al, November 2018 (13 pages), [Generating superposition of up-to three photons for continuous variable quantum information processing](#) by Mitsuyoshi Yukawa et al, 2013 (7 pages), and [Generation of light in a photon-number quantum superposition](#), August 2019. And the entangled photon numbers in [Photon-number entanglement generated by sequential excitation of a two-level atom](#) by S. C. Wein, Pascale Senellart et al, June 2021 (18 pages).

The energy of a quantum oscillator can be described with a simple equation, N being the photon number. When N=0, the oscillator energy corresponds to the vacuum state energy.

$$\text{energy } E \text{ and photon number } N: \quad E = \hbar\omega \left( N + \frac{1}{2} \right) \quad \text{photon wavenumber } k = \frac{2\pi}{\lambda}.$$

**Photon wavenumber** is the spatial frequency of a wave, measured in radians per unit distance. It is defined as k with the above right formula using the photon wavelength.

**Creation and annihilation operators** or ladder operators are mathematical operators used with quantum harmonic oscillators and many-particles systems. An annihilation operator  $\hat{a}$  reduces the number of particles in a given state by one and a creation operator  $\hat{a}^\dagger$  increases this number by one. It is the adjoint operator of the annihilation operator. These operators act on states of various types of particles, and with photons, as adding or removing a quantum of energy to and oscillator system.

The use of these operators instead of wavefunctions is part of the second quantization formalism. It explains why the canonical quantum physics postulates that we described in an [earlier part](#) (page 89) are not entirely applicable to quantum optics, particularly the time evolution postulate related to Schrödinger's wave equation that is applicable only to non-relativistic massive particles and even the structure of the quantum state  $\psi$ .

Mathematically, a photon occupation number operator is a Hermitian operator  $\hat{N} = \hat{a}^\dagger \hat{a}$ . And a photon number of n superposed photons created by the operator  $\hat{a}^\dagger$  applied n times to the vacuum state  $|0\rangle$  creates the state  $|n\rangle = \frac{1}{\sqrt{n!}} (\hat{a}^\dagger)^n |0\rangle$ .

**Second quantization** is the broad field of quantum physics that deals with many-body quantum systems. It was introduced by **Paul Dirac** in 1927 and developed afterwards by **Vladimir Fock** and **Pascual Jordan**. While the first quantization dealt with individual quantum objects and their description by the Schrödinger wave equation, the second quantization describes many-body systems which are represented mathematically by Fock states and Fock spaces.

Its formalism introduces creation and annihilation operators to construct and handle the Fock states, providing the mathematical tools to the study quantum many-body systems.

Instead of describing such a system as a tensor product of all its constituent quantum objects, it is simplified with chaining  $|n_{k_i}\rangle$  describing the  $n_i$  quantum objects that are in the same quantum state  $k_i$  as described in the above equation related to the creation operator.

A many-body system is described as the tensor product of the Fock states  $|n_{k_i}\rangle$  corresponding to each individual quantum states in the system:  $|n_{k_0}\rangle \otimes \dots \otimes |n_{k_n}\rangle$ , given that the photon number  $n_i$  for the Fock state  $|n_{k_i}\rangle$  can be 0 or 1 for fermions and any positive number for a boson. When all occupation numbers are equal to zero, the Fock state corresponds to the vacuum state.

A Fock state with only one non-zero occupation number is a single-mode Fock state. Contrarily, a multi-mode Fock state has several non-zero occupation numbers.

**Quantum optics**. This field of quantum physics started quite late. In 1956, the Hanbury-Brown-Twiss (HBT) experiment was about observing the intensity correlations of the radiation of a mercury lamp and from some bright stars. After traversing a beamsplitter (with a mercury lamp) or at two spatially separated points (for stars), the intensities measured by two detectors were fluctuating, and these fluctuations were correlated.

It was then explained by the emission of photon bunches coming from thermal sources. But it could be explained without using photons and quantum physics.

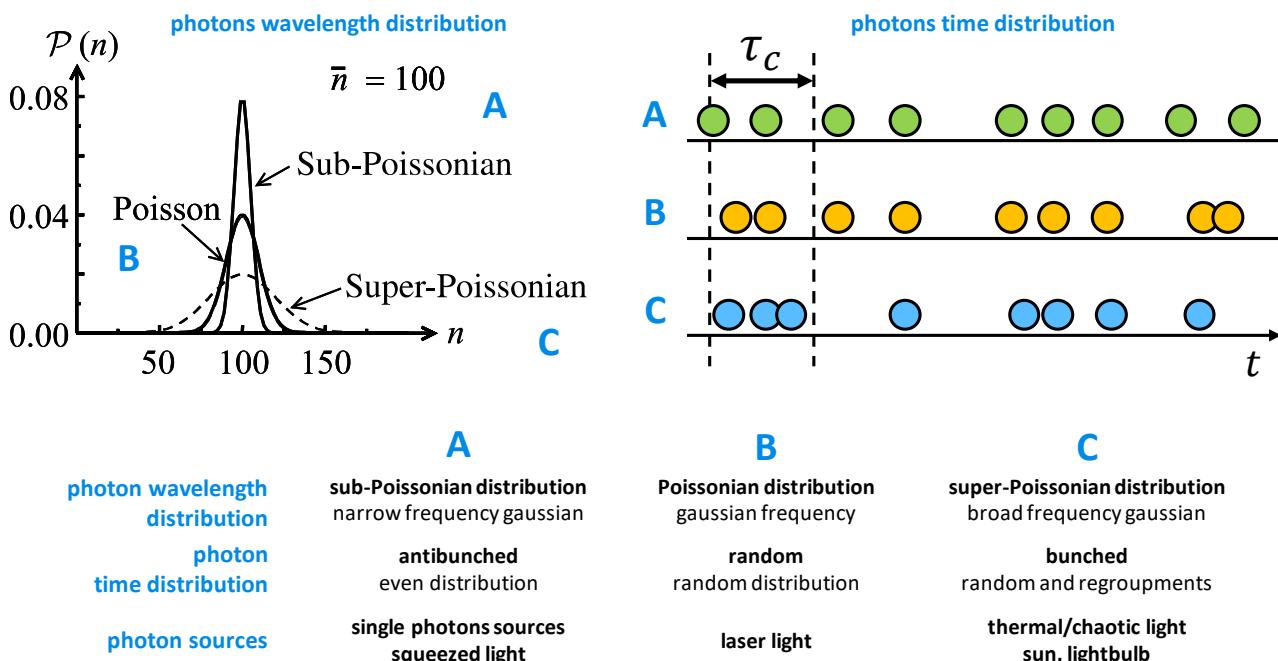
Quantum optics really started when it became possible to create non classical light sources like pairs of photons and single photons, respectively in 1967 and 1977. Photon pairs were first created with using cascaded atom decay and parametric down conversion<sup>710</sup>.

**Semi-classical light.** It describes interactions between quantized matter such as atoms and electrons with classical light fields. Continuous laser light belongs to this category.

**Non-classical light.** Light and photons are always quantum, just because it comes from quantized energy exchanges with matter. Still, light is considered to show non-classical and quantum effects when the electromagnetic field is quantized and photons are handled individually. This happens in a couple situations: creation of entangled Bell states, antibunching, photon noise and negative probabilities with the Wigner function. We'll look at each of these phenomena.

**Bell states** where single photons behave probabilistically and in the general case have no *a priori* properties like polarization, wavelength, wavevector before being measured. These properties are revealed while being measured and show correlations between entangled photons whose measured properties will be random.

**Anti-bunching** corresponds to a light field where photons are equally spaced in time, much better than with a coherent laser field. It is detected with a HBT (Hanbury Brown & Twiss) intensity autocorrelator... with no correlations. It refers to sub-Poissonian photon statistics, that is a narrow photon number distribution. It can be generated by single photon sources as well as from pulse mode lasers. A coherent state from a laser has a Poissonian statistics generating random photon spacing and a thermal source light field has super-Poissonian statistics and yields bunched photon spacing. All these aspects belong to the field of statistical optics.



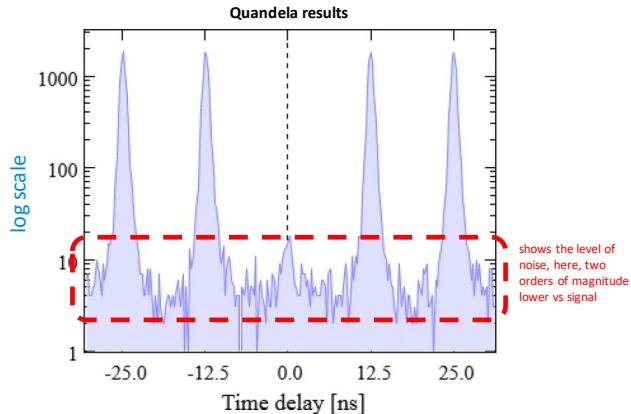
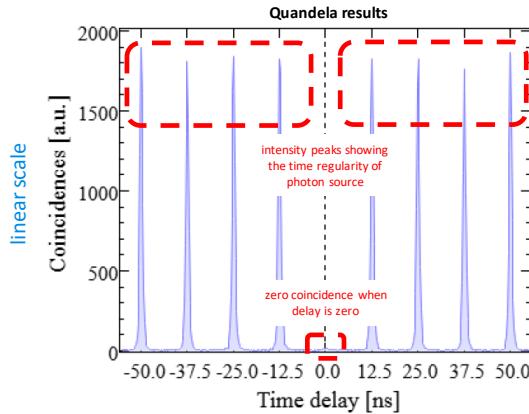
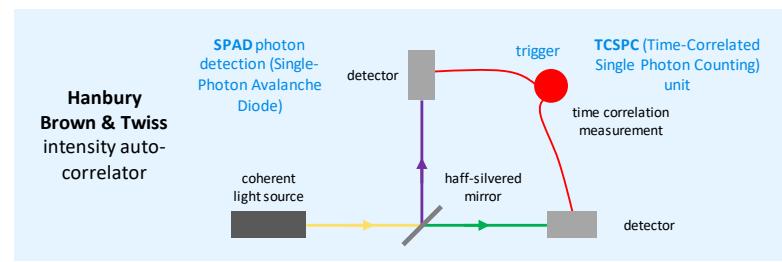
The quality of single photons source is measured with the data from two experiments. The first uses a variant of a **Hanbury Brown and Twiss** (HBT) intensity autocorrelator that checks the photons are emitted in a very regular way, like a metronome. From a starting click on one of the two photon detectors, it analyzes the time distribution of the appearance of the following photons. This produces the plots *below*.

<sup>710</sup> Source: [Lecture 1. Basic concepts of statistical optics](#) (7 pages).

## antibunching measurement

$$g^2(0) = 0,019$$

time correlation of second order or of intensity between pairs of photons with a zero delay. the closer to zero, the better. describes the level of noise in the system.



The ideal model would be that of a high peak on either side of the center. The low peaks represent the system noise<sup>711</sup>.

The second experiment called H.O.M. for **Hong-Ou & Mandel** and created in 1987 uses a Mach-Zehnder interferometer to validate the fact that the emitted photons are indeed identical and impossible to distinguish<sup>712</sup>.

**Quadratures representation** is a way to describe the electromagnetic field and its related uncertainty. An EM wave is positioned in two axis X and Y or  $X_1$  and  $X_2$  corresponding to the rotation of the electric field in the EM field, thus the equations describing  $X_1$  and  $X_2$  below, with the cosine and sine of  $\omega t$  (angular frequency  $\times$  time). Said otherwise, a quadrature describes the real and imaginary parts of a complex amplitude. This EM field complex amplitude is rotating so what's interesting is not the grey circle position in the chart but its shape and size which represents the photon measurement uncertainty. It is represented by the variation of the length of the vector which is the photon number and of the width of the circle, orthogonally to the vector, which corresponds to the phase uncertainty. For unsqueezed coherent light, this uncertainty is the same as the vacuum state.

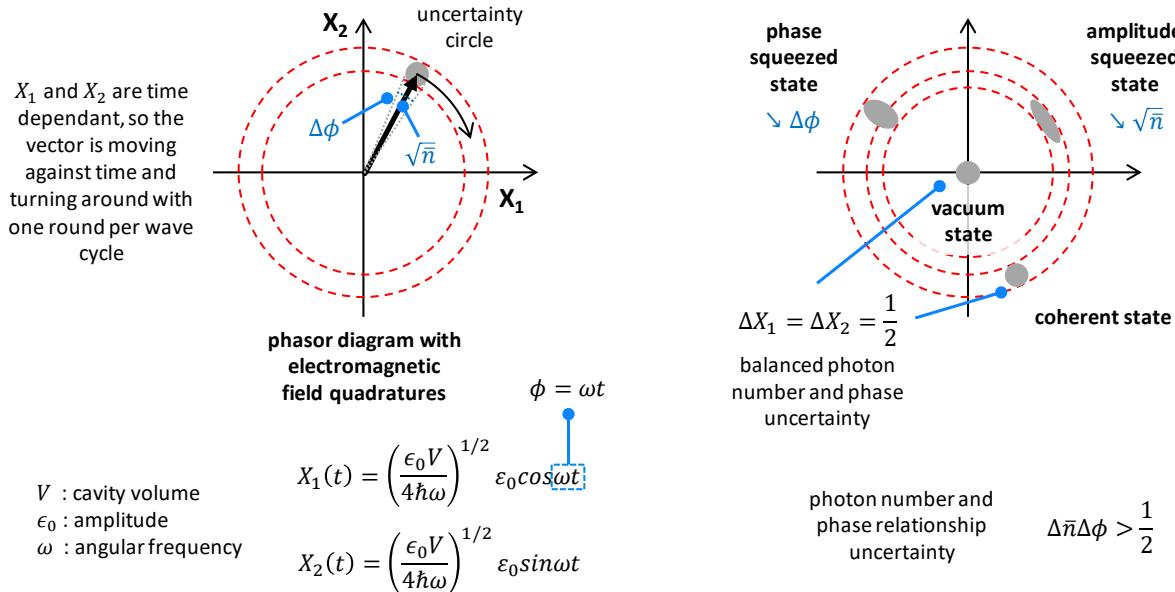
**Photon noise** aka shot noise is found in the detection of light and corresponds to quantum fluctuations in the electromagnetic field. This noise or imprecision can be squeezed in one dimension.

**Squeezed light** corresponds, in a quadrature or phasor diagram representation, to wave functions which have an uncertainty in one of the quadrature amplitudes (phase or photon number) smaller than for the ground-state corresponding to the vacuum state.

<sup>711</sup> This experiment, originally created to detect the size of stars, also allowed to validate the corpuscular nature of photons. The experiment can be easily interpreted in an intuitive way: photons pass through a one-way mirror, whether or not it crosses randomly. Behind this mirror are two photon counters, here with SPADs (avalanche diodes). The system detects when a photon is detected at the same time by both sensors. If the photons take the same way to reach both detectors, there will be no coincidence since the emitted photons are sent in well-ordered trains and can only be on one side or the other. By adding a delay line between the mirror and one of the sensors that is proportional to the period of emission of the photons, it creates many occurrences with photons arriving simultaneously in both sensors. This is what we see in the two curves, one of them being with a linear scale of coincidences (measured over a period of time sufficient to capture hundreds of them) and another logarithmic which allows to better characterize the noise of the system.

<sup>712</sup> See [High-performance semiconductor quantum-dot single-photon sources](#) by Pascale Senellart, Glenn Solomon and Andrew White, 2017 (14 pages) which describes the various ways to characterize the quality of single photons sources.

It can be generated by different means like a parametric down conversion<sup>713</sup>. Balanced homodyne detectors are used to detect squeezed light.



(cc) Olivier Ezratty, June 2021

**Wigner function** is yet another representation of a quantum state, richer than the phase diagram above which is used to measure the level of quantumness of a light pulse. It's not far from a probability distribution of the electric field in the (Q, P) plane that can take negative values in some conditions, for so-called non-Gaussian states<sup>714</sup>. With coherent states,  $W(Q, P)$  is a symmetric Gaussian function peaking at the average values of the sine and cosine components of the electric field with the peak width corresponding to the vacuum noise like in the quadrature representation. The Wigner function equation looks like:

$$W(Q, P) = \frac{1}{\pi\hbar} \int_{-\infty}^{+\infty} \psi^*(Q + y)\psi(Q - y)e^{2iPy/\hbar} dy$$

with  $\psi$  being the quantum object wave function, Q and P the position and momentum and y, the variable used in the integral. It returns a real value that can be positive or negative. Q and P could be replaced by the sine and cosine components of the quantized electric field like in the phasor diagram.

Here are a set of Wigner functions, ranging from the most classical to the most quantum fields. A is a coherent state<sup>715</sup>, B, a squeezed state, C a single-photon state and D a Schrödinger's-cat state. The projections or shadows of the Wigner function are the probability distributions of the quantum continuous variables Q or P.

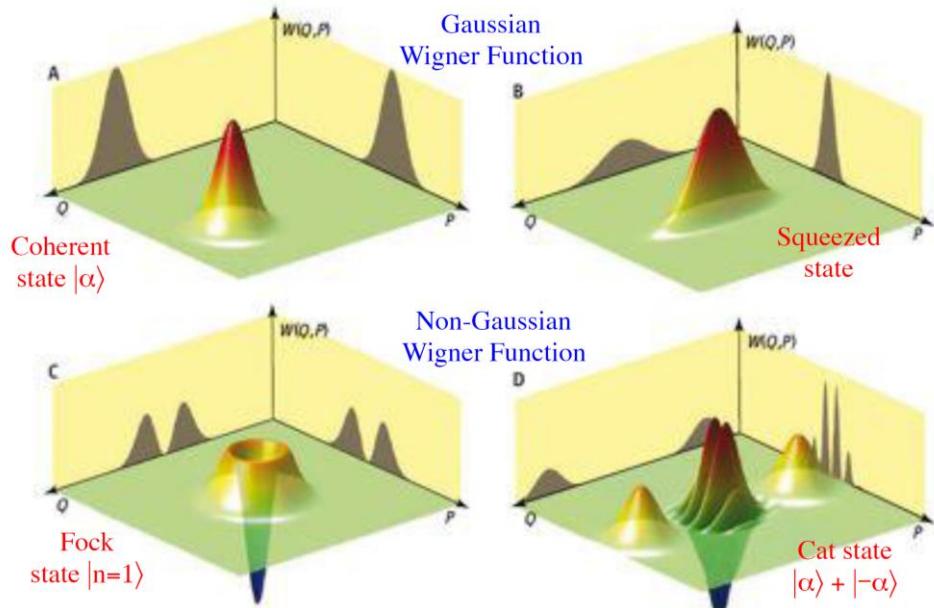
The Wigner function is a Gaussian function for A and B but takes negative values for the non-Gaussian strongly quantum states C and D<sup>716</sup>.

<sup>713</sup> See [Generation of squeezed states by parametric down conversion](#) by Ling-An Wu et al, University of Texas, Physical Review Letter, 1986 (4 pages).

<sup>714</sup> See [Conversion of Gaussian states to non-Gaussian states using photon number-resolving detectors](#) by Daiqin Su et al, Xanadu, April 2019 (37 pages), the tutorial paper [Non-Gaussian Quantum States and Where to Find Them](#) by Mattia Walschaers, LKB - Collège de France, April 2021 (55 pages) and the review paper [Production and applications of non-Gaussian quantum states of light](#) by A. I. Lvovsky, Philippe Grangier et al, June 2020 (50 pages).

<sup>715</sup> The vacuum state has a similar Wigner function, but centered around P=0 and Q=0.

<sup>716</sup> Source: [Make it quantum and continuous](#) by Philippe Grangier, Science, 2011. See also [Recent advances in Wigner function approaches](#) by J. Weinbub and D. K. Ferry, 2018 (25 pages) which shows the various use cases of the Wigner function.

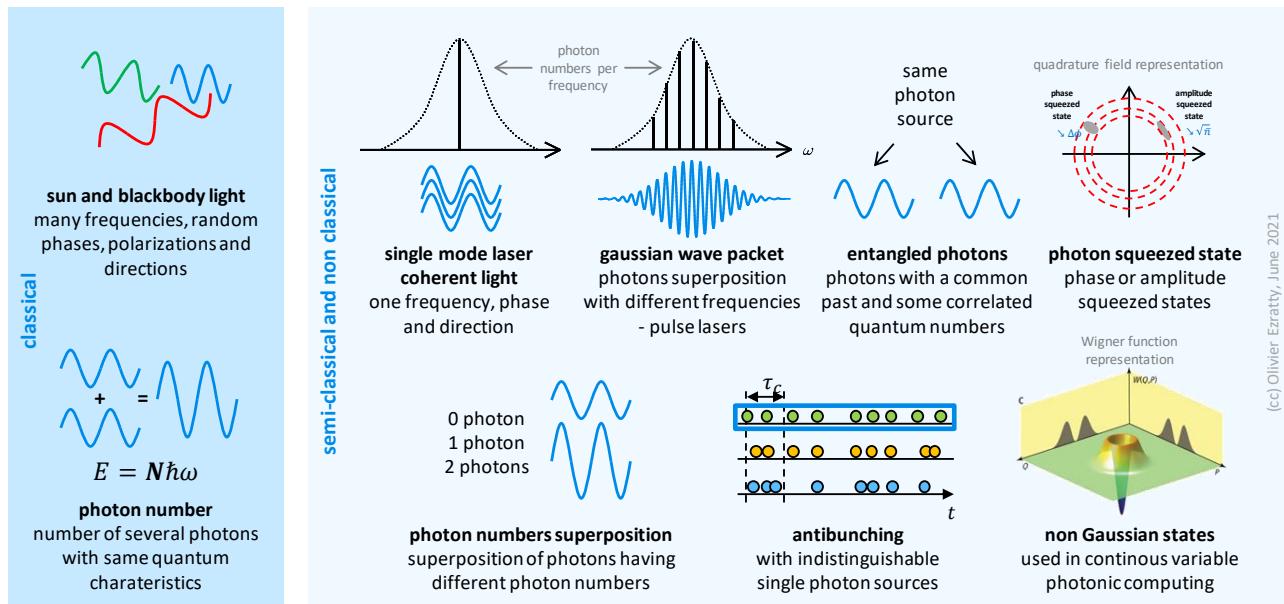


P. Grangier, "Make It Quantum and Continuous", Science (Perspective) 332, 313 (2011)

These negative values vanish very quickly with decoherence.

**Parametric down-conversion** is a nonlinear optical process converting one photon of high energy into a pair of photons of lower energy. It is used to generate pairs of entangled photons.

**Photons zoo.** The illustration *below* shows some various photon states as a summary of this section. Random photons in spontaneous light coming from the Sun or light bulb and “photon number” waves assembling several similar photons belong to classical light. Other forms of light described here are semi-classical or non-classical: photon number superposition, squeezed states where the precision is improved in photon number, amplitude or phase at the expense of the others, single-mode coherent laser light, wavepackets created by pulse lasers or microwave coming from waveform generators used with superconducting and electron spin qubits, entangled photons used in QKD and photon qubits, and non-gaussian states which are weird beasts too complicated to describe in a couple of words that are used to implement non-Clifford quantum gates with photon qubits.



## Photonic qubit types

Photons are "flying qubits". They are the only ones having this characteristic with flying electrons, which are investigated at the fundamental research level. There are two main classes of photon qubits: discrete variable and continuous variable qubits<sup>717</sup>.

	discrete variables	continuous variables	boson sampling
quantum information	discrete degree of freedom of a photon Fock states: $ 0\rangle,  1\rangle,  2\rangle \dots$ single or many photon properties	quadrature of a light field coherent states, qumodes, spectral and time modes	multimode photons
photon sources	single indistinguishable photon sources	entangled photons sources squeezed states, ...	unique photons source
representation	density matrix	Wigner function	permanent
gates	KLM model, MZI (Mach-Zehnder Interferometer) gates	deterministic gates modes measurement gaussian and non gaussian gates	MZI and interferometer
photon detectors	photon counters /detectors APD, SNSPD, VLPC, TES	homodyne and heterodyne detectors	single photons detectors
players	$\Psi$ PsiQuantum  QUANDELA  ORCA Computing 	X AND D U 	

**Discrete Variable** qubits use single photons and use a two-dimensional space like orthogonal polarizations or the absence and presence of single photons. DV systems can even be based on qudits using more than one degree of liberty. DV qubits rely on highly efficient, deterministic and indistinguishable single photon sources. They are using the "particle" side of photons. Their indistinguishability must exceed 95%, meaning this percentage of photons must be indistinguishable. The photon sources must also be efficiently connected to dynamically controllable photonic computing chipsets.

Efforts are also undertaken to create cluster states of entangled photons used in MBQC and to create deterministic multi-qubit gates using spin-photon interactions like in NV centers or other silicon spin defects<sup>718</sup>.

**Continuous Variable** qubits encode information in the fluctuations of the electromagnetic field, in their quadrature components, in qubits that are sometimes baptized qumodes. We are playing here with the wave nature of photons. Photons readout can be done with a Gaussian measurement comprising homodyne detection for one of the two quadrature components and heterodyne detection on one of these<sup>719</sup>, and a non-Gaussian measurement implementing photon counting returning an integer.

<sup>717</sup> See this good review paper: [Integrated photonic quantum technologies](#) by Jianwei Wang et al, May 2020 (16 pages) and [Hybrid entanglement of light for remote state preparation and quantum steering](#) by Adrien Cavaillès et al, LKB (41 slides) which positions well the difference between DV and CV computing.

<sup>718</sup> See [Multidimensional cluster states using a single spin-photon interface coupled strongly to an intrinsic nuclear register](#) by Cathryn P. Michaels et al, University of Cambridge, April 2021 (11 pages).

<sup>719</sup> On the measurement of CV qubits, see [Optical hybrid architectures for quantum information processing](#) by Kun Huang, LKB, 2017 (215 pages). This is not the same Kun Huang as the discoverer of phonon-polaritons in 1951.

There, you hear about Wigner function amplitude, phase encoding, Gaussian states<sup>720</sup>, including squeezed states generated with non-linear media and non-Gaussian gates to execute non-Clifford group gates bringing a real exponential speedup for quantum computing. Quantum gates can be deterministic, homodyne detectors are cheaper than single photons detectors, and quantum states are more robust.

CV qubits are implementing larger cluster states for MBQC, using a large number of photon modes (in the thousands)<sup>721</sup>. There you'll find cat-qubits and GKP states. Hybrid DV/CV qubits approaches are also investigated<sup>722</sup>. CV computing can be used with universal gates quantum computing as well as with quantum simulations.

**Quantum Walks based simulation** is another computing technique using photons. Similarly to the CV/DV computing segmentation, you have two classes of photon-based quantum walk systems: discrete-time quantum walks with discrete steps evolutions and continuous-time quantum walks with a continuous evolution of a Hamiltonian coupling different sites<sup>723</sup>.

**Boson sampling** is a separate technique we'll cover later in a dedicated section, page 347. It's a research field that has not yet brought to life programmable computing.

## Photonic qubits principles

The general principle of quantum computing systems using photon qubits is as follows:

- **Photon sources** are lasers, often coupled with single and indistinguishable photon generators<sup>724</sup>. They are critical to generate simultaneously a large number of indistinguishable photons that will feed in parallel several qubits thanks to delay lines. These are well time-isolated unique and indistinguishable photons generated in well-spaced in time series. These single photons are individually detectable at the end of processing with single photon detectors. The key metrics of these photon sources are the system efficiency (probability that at least one photon is created per pulse), purity (probability of getting a maximum of one photon per pulse) and coherence (how generated photons are quantum mechanically identical or indistinguishable).

The purity and high probability to get a photon per clock cycle are the enabler of quantum interferences based multiple qubit gates with discrete variable qubits.

High-efficiency sources are qualified as “on-demand” or “deterministic” but an alternative is heralded sources, where the emission time can be accurately measured.

---

<sup>720</sup> Understanding how Gaussian states work is already quite a challenge. See [Gaussian Quantum Information](#) by Christian Weedbrook, Seth Lloyd et al, 2011 (51 pages).

<sup>721</sup> See [A fault-tolerant continuous-variable measurement-based quantum computation architecture](#) by Mikkel V. Larsen, January 2021 (16 pages).

<sup>722</sup> See [Hybrid Quantum Information Processing](#) by Ulrik L. Andersen and al, 2014 (13 pages) and [Hybrid discrete and continuous-variable quantum information](#) by Ulrik L. Andersen et al, 2015 (11 pages), [Visualization of correlations in hybrid discrete-continuous variable quantum systems](#) by R P Rundle et al, February 2020 (15 pages) and [Remote creation of hybrid entanglement between particle-like and wave-like optical qubits](#) by Olivier Morin, Claude Fabre, Julien Laurat, LKB France, 2013 (7 pages).

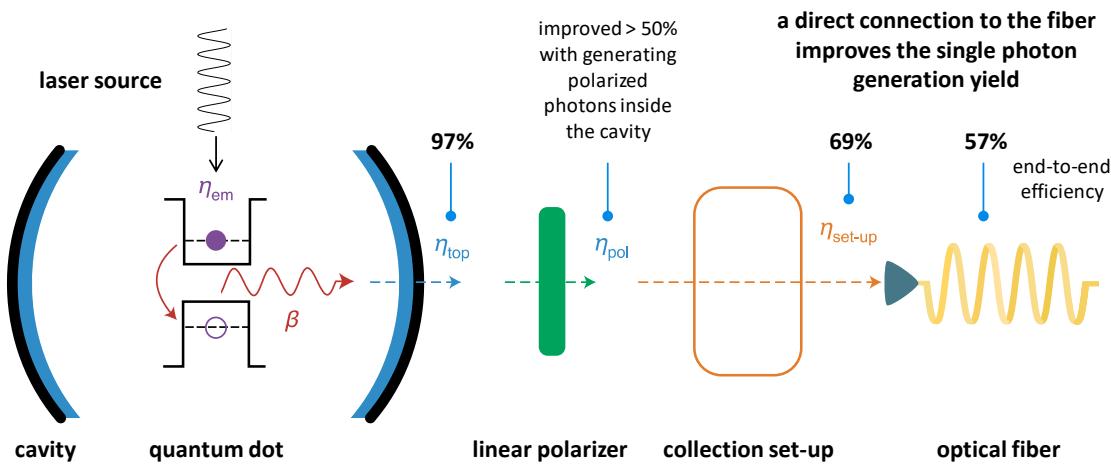
<sup>723</sup> See [Purdue University Scientists Say 'Quantum Rainbow' May Allow Room-Temperature Quantum Computing](#) par Matt Swayne, 2021 referring to [Probing quantum walks through coherent control of high-dimensionally entangled photons](#) by Poolad Imany et al, July 2020 (9 pages).

<sup>724</sup> See [Near-ideal spontaneous sources in silicon quantum photonics](#) by S. Paesani et al, 2020 (6 pages) which describes a single photon source based on a photonics component. It is an Anglo-Italian research project.

There are two main types of single photons sources (SPSs)<sup>725</sup>:

**Quantum dot single-photon source** are the best-in-class devices, able to generate photons with a 99.7% single-photon purity, and overs 65% extraction efficiency, which could potentially reach 80% (meaning, 4 photons generated out of 5 clock cycles). These sources also have an over 99% photon indistinguishability. In the second quantization formalism, they create a single Fock state with a photon number equal to one.

The leaders in this market are **Quandela**<sup>726</sup> and **Sparrow Quantum**<sup>727</sup>. And many research labs are working on quantum dots<sup>728</sup>. These photon sources must be cooled at about 3K to 4K. In their latest Prometheus generation, Quandela directly couples the quantum dot to a fiber, avoiding the use of cumbersome confocal microscopes and significantly increasing the photon generation yield. It creates a path to reaching a combined source–detector efficiency closer to the 2/3 threshold that is mandatory for scalable discrete variable optical quantum computing.



source: The race for the ideal single-photon source is on by Sarah Thomas and Pascale Senellart, Nature Nanotechnology, January 2021

**Parametric photon-pair sources** are laser pumping nonlinear optical waveguides or cavities that create photon-pairs. It can be integrated in nanophotonic circuits. They are using either spontaneous four-wave mixing (SFWM) or spontaneous parametric down-conversion (SPDC) processes in non-linear crystals. The efficiency is lower than with quantum dots, reaching about 50% with a 95% photon indistinguishability from separated SPSs. Photons are created non-deterministically with a rather low 5% to 10% probability, which can be increased to above 60% with time and spatial domains multiplexing.

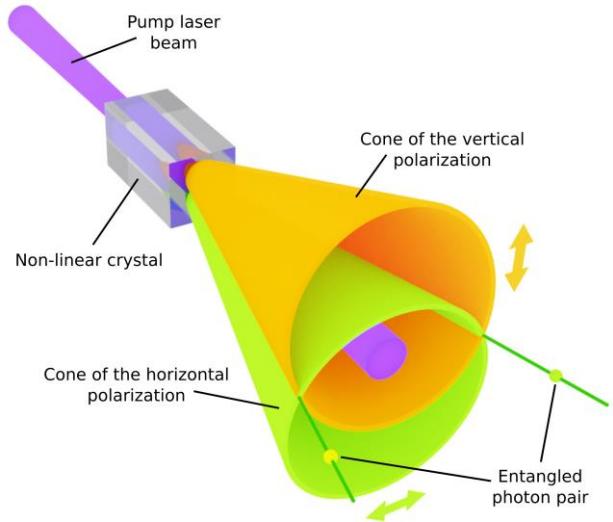
<sup>725</sup> Source: [Integrated photonic quantum technologies](#) by Jianwei Wang et al, May 2020 (16 pages).

<sup>726</sup> See [The race for the ideal single-photon source is on](#) by Sarah Thomas and Pascale Senellart, Nature Nanotechnology, January 2021 (2 pages) which describes the various ways to improve the yields of single photon sources, [Sequential generation of linear cluster states from a single photon emitter](#) by D. Istrati, Niccolo Somaschi, Hélène Ollivier, Pascale Senellart et al, October 2020 and [Reproducibility of high-performance quantum dot single-photon sources](#) by Hélène Ollivier, Niccolo Somaschi, Pascale Senellart et al, October 2019 (10 pages) on benchmarking single photon sources.

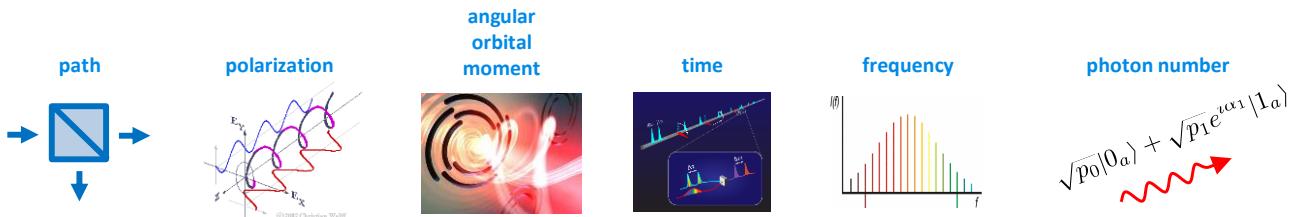
<sup>727</sup> See [Scalable integrated single-photon source](#) by Ravitej Uppu et al, December 2020 (7 pages) which describes the latest advancements of their technology.

<sup>728</sup> See [Planarized spatially-regular arrays of spectrally uniform single quantum dots as on-chip single photon sources for quantum optical circuits](#) by Jiefei Zhang et al, University of Southern California and IBM, November 2020 (8 pages) describes an array with 32 quantum dots and a simultaneous purity of single-photon emission over 99.5%.

Such solutions are embedded in nanophotonic solutions like with **PsiQuantum**. SPDC sources work at room temperature but for efficient multiplexing (>95%), it is necessary to have SNSPD detectors running at low temperature. Progress is regularly being made with nanophotonic-based single photons generation, although their performance still lags quantum-dots sources<sup>729</sup>. On the right, the principle of SPDC to create pairs of entangled photons. The conversion creates pairs of orthogonally polarized photons in two light cones with entangled photons at their intersection.



- **Quantum state** is based on a single or several properties of the photons. The most common is their polarization with a computational basis based on horizontal and vertical polarization. Other parameters of photons are also explored to create qubits such as their phase, amplitude, frequency, path, photon number, spin orbital momentum and even orbital angular momentum<sup>730</sup>. This potentially allows the creation of qutrits or qudits managing more than two exclusive values. Photons are "flying qubits" because they move in space and are not static or quasi-static at the macroscopic scale unlike most other types of qubits<sup>731</sup>.



- **Single-qubit quantum gates** use simple optical circuitry, including beamsplitters, waveplates, mirrors and semi-reflective mirrors, and phase shifters<sup>732</sup>. For example, a Hadamard gate (H) uses a beamsplitter or waveplate, a Pauli X gate (bit flip) combines a beamsplitter and a Hadamard gate, and a Pauli Z gate (phase flip) uses a phase shifter causing a 180° phase change ( $\pi$ )<sup>733</sup>.

---

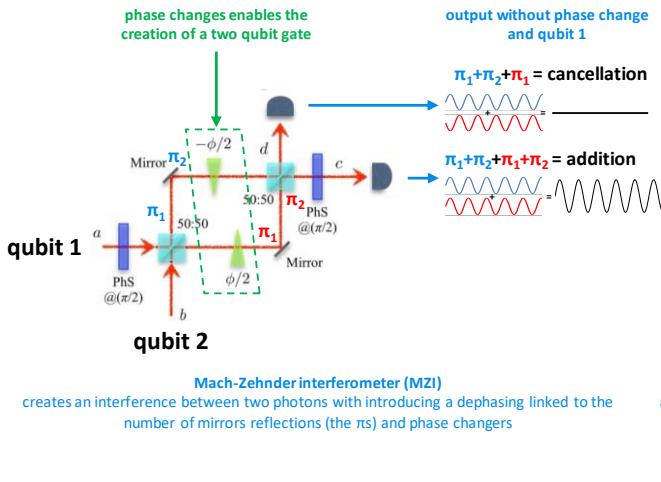
<sup>729</sup> See [High-efficiency single-photon generation via large-scale active time multiplexing](#) by F. Kaneda et al, October 2019 (7 pages), [Researchers create entangled photons 100 times more efficiently than previously possible](#) pointing to [Ultra-bright Quantum Photon Sources on Chip](#) by Zhaohui Ma et al, October 2020 (5 pages) and [A bright and fast source of coherent single photons](#) by Natasha Tomm et al, University of Basel and Ruhr-Universität Bochum, July 2020 (14 pages).

<sup>730</sup> This multiplicity of parameters also makes it possible to encode not only qubits but also qudits, with a greater number of states. But it is quite complex to manage and, if only to manage two-qubit quantum gates, we are content with qubits instead of using qudits. Source of inspiration for the diagram: [The beginnings of the quantum computer: principles, promises, achievements and challenges](#) by Pascale Senellart, January 2020 (98 slides). See also [Forget qubits -scientists just built a quantum gate with qudits](#) by Kristin Houser, July 2019, which refers to [High-dimensional optical quantum logic in large operational spaces](#) by Poolad Imany et al, 2019 (10 pages). See the definition of orbital angular momentum in the glossary. It was discovered in 1992. See [Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes](#) by Les Allen et al, 1992 (5 pages).

<sup>731</sup> The other qubits are "non-flying": spin-controlled electrons trapped in a cavity, cold atoms (which are stabilized in space) and trapped ions (which can move, but in a limited space), NV centers (cavities do not move) and superconducting circuits (which are fixed in space even if they use pairs of circulating Cooper electrons).

<sup>732</sup> This is based on the KLM scheme proposed in [A scheme for efficient quantum computation with linear optics](#) by Emanuel Knill, Raymond Laflamme and Gerard Milburn, 2001 (7 pages).

<sup>733</sup> Source for the table to the right of the illustration: [Quantum Logic Processor: A Mach-Zehnder Interferometer based Approach](#) by Angik Sarkar and Ajay Patwardhan 2006 (19 pages).



The implementation of various quantum logic gates using optical MZI is tabulated in Table 3.

Quantum Logic Gate	Unitary Matrix	Relation for MZI implementation	Elements
Beam Splitter(B(θ))	$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$		
50:50 Beam Splitter(B)	$\begin{bmatrix} 1 & -1 \\ \sqrt{2} & 1 \\ 1 & 1 \end{bmatrix}$		
Hadamard(H)	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	H=BZ	50-50 Beam splitter
Phase flip gate (Z)	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	Z=HB	$\pi$ Phase shifter
Bit Flip gate (X)	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	X=BH	Beam Splitter, Hadamard
T gate	$\begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$		$\pi/4$ phase shifter
S gate	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$		Quarter wave plate
Pauli Y gate	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$		
CNOT gate	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	$(I \otimes H) \times K \times (I \otimes H)$	Kerr Media(K) Hadamard(H) Identity(I)

#### MZI based quantum gates

a one qubit gate can be created with introducing some dephasing in one or two of the circuits, and two qubit gate with using two entries and some dephasing. The table shows the correspondence between quantum gates and the used filters elements.

- **Two-qubit quantum gates** are difficult to realize because it is not easy to have photons interact with each other, particularly when they are not perfectly indistinguishable. They use optical circuits based on beamsplitters or Mach-Zehnder interferometers with two inputs integrating phase changes on the optical paths, based on the KLM method already quoted in footnote.

This does not work well when the photons are uneven, such as those coming from lasers. Namely, in only a few % of the cases. With indistinguishable photons, gates are more than 95% efficient since photons can interfere with each other, and add or subtract. It facilitates Mach-Zehnder interferometry operations.

These sources have the additional advantage of being very bright, which allows them to multiply the incoming photons and then to pass through many quantum gates. There are also solutions based on cavities. Research is also active on the creation of non-linearities to improve the reliability of these quantum gates<sup>734</sup>. Ideally, non-linear separating cubes should be used<sup>735</sup>.

- **Qubit readout** uses single photon detectors that also capture their quantum state. This detection is still imperfect. Several single-photons detection technologies are competing: SPAD (avalanche photodiodes, which detect photon occurrences but not photon number)<sup>736</sup>, transition edge sensor (TES, which can detect photon numbers) and Superconducting Nanowire SPDs (SNSPDs, which also detect photon numbers). Fully integrated SNSPDs are based on GaAs, Si and  $\text{Si}_3\text{N}_4$  waveguides. In order to limit the dark count phenomenon coming from thermal effects, these SNSPDs are usually cooled between 800 mK and 3K which requires a dilution refrigeration system<sup>737</sup>.

<sup>734</sup> See [Quantum Computing With Graphene Plasmons](#), May 2019 which refers to [Quantum computing with graphene plasmons](#) by Alonso Calafell et al, 2019. This is the creation of two-qubit quantum gates with graphene-based nonlinear structures. It comes from the University of Vienna in Austria and from Spanish and Serbian laboratories. As well as [Researchers see path to quantum computing at room temperature](#) by Army Research Laboratory, May 2020 which refers to [Controlled-Phase Gate Using Dynamically Coupled Cavities and Optical Nonlinearities](#) by Mikkel Heuck, Kurt Jacobs and Dirk R. Englund, 2020 (5 pages).

<sup>735</sup> It is a function that can be realized with Quandela's single photon generation component, diverted from its original use. See also [Researchers see path to quantum computing at room temperature](#), May 2020 which refers to [Controlled-phase Gate using Dynamically Coupled Cavities and Optical Nonlinearities](#) by Mikkel Heuck, September 2019 (5 pages) and discusses a nonlinear cavity optical quantum gate technique.

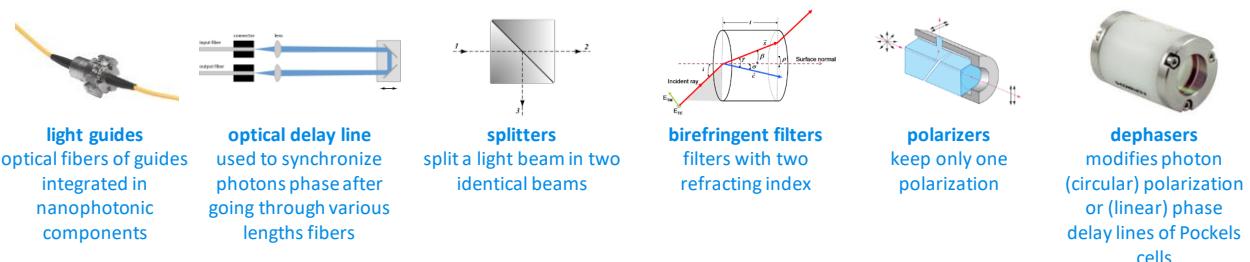
<sup>736</sup> See recent progress with SPADs in [Low-noise photon counting above  \$100 \times 10^6\$  counts per second with a high-efficiency reach-through single-photon avalanche diode system](#) by Michael A. Wayne et al, NIST, December 2020 (6 pages).

<sup>737</sup> See [The potential and challenges of time resolved single-photon detection based on current-carrying superconducting nanowires](#) by Hengbin Zhang et al, October 2019 (19 pages) and [Superconducting nanowire single-photon detectors for quantum information](#) by Lixing You, June 2020 (20 pages). Dark counts are detected photons coming from the environment due to thermal or tunneling effects.

NbTiN-based SNSPDs could work with higher-temperature cooling, between 2.5K to 7K<sup>738</sup>. One goal is to integrate these photon detectors directly in photonic computing circuits. Other detectors are specialized for analyzing continuous variables qubits, like homodyne and heterodyne detectors.

From a physical point of view, these items are classical photonic components: single and identical photon sources, light guides, optical delay lines (optical fibers or voltage-controlled Pockels cells), Mach-Zehnder interferometers, beam splitters (splitters, which divide an optical beam into two beams, generally identical), birefringent filters (which have two different refractive indices), phase shifters and single photon detectors<sup>739</sup>.

To conduct experiments, these discrete and very affordable components are installed on carefully calibrated optical tables of a few square meters with lots of instruments and photons that circulate largely in the free space of a darkened room.

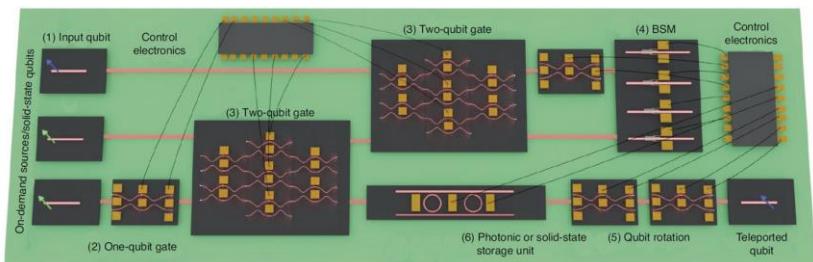


Fortunately, these optical components are miniaturizable on semiconductor integrated circuits. This is part of the vast field of nanophotonics. Nanophotonics components are etched with densities between 220 nm and 3  $\mu\text{m}$ <sup>740</sup>.

In nanophotonics, quantum gates are dynamically programmed by the conditional routing of photons in optical circuits. These circuits are often etched on CMOS (silicon) or III/V (especially germanium) components.

These components could be assembled in a modular way as shown in this diagram<sup>741</sup>.

This enables a better management of processes heterogeneity used to create these different circuits.



Many semiconductor fabs in the world are helping photonician design and prototype nanophotonic circuits to run photon qubits. We'll mention here only a few of them. Many fab technologies are investigated with classical silicon-based CMOS, hybrid CMOS with silicon nitride (SiN) and lithium niobate ( $\text{LiNbO}_3$ ), III/V materials (AsGa, InP, ...), etc<sup>742</sup>.

<sup>738</sup> See [Superconducting nanowire single photon detectors operating at temperature from 4 to 7 K](#) by Ronan Gourgues et al, Optics Express, 2019 (9 pages).

<sup>739</sup> This is well explained in [Silicon photonic quantum computing](#) by Syrus Ziai, PsiQuantum, 2018 (72 slides) as well as in [Large-scale quantum photonic circuits in silicon](#), 2016 (13 pages).

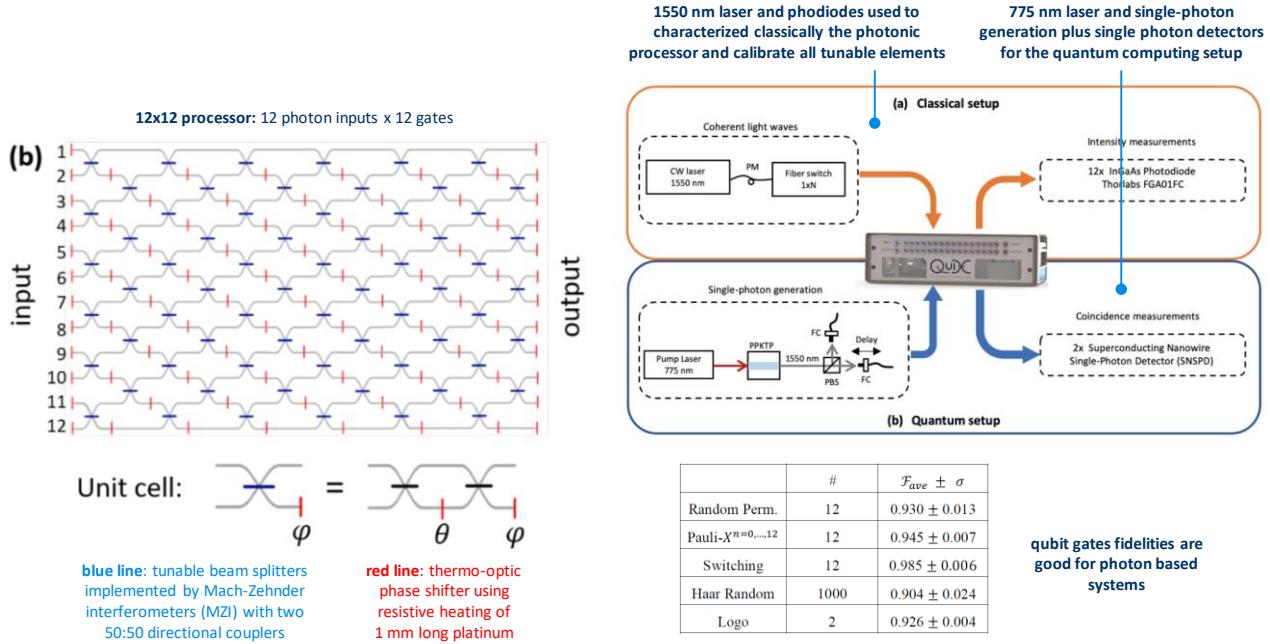
<sup>740</sup> See for example the work of InPhyNi discussed in [High-quality photonic entanglement based on a silicon chip](#) by Dorian Oser, Sébastien Tanzilli et al, 2020 (9 pages).

<sup>741</sup> See [Hybrid integrated quantum photonic circuits](#) by Ali W. Elshaari et al, 2020 (14 pages).

<sup>742</sup> See the review paper [Roadmap on integrated quantum photonics](#) by Galan Moody, Jacquiline Romero, Eleni Diamanti et al, August 2021 (108 pages).

**Quix Photonics** (2019, Netherlands) is developing a photonic quantum processor using silicon nitrides ( $\text{Si}_3\text{N}_4$ ) waveguides. It is a project from the University of Twente and the AMOLF laboratory in Amsterdam. The company is a subsidiary of the fab Lionix. Their fab also provides photonic components to other industry vendors, like Quandela.

They presented in 2021 a record 12x12 programmable photonic processor. It uses thermo-optic phase shifters and tunable beam splitters. The circuit is labelled a 12x12 because it has 12 input photons and a depth of 12 quantum gates<sup>743</sup>.



In France, **CEA-Leti** is also building an integrated silicon photonic qubits platform including single photons source, phase shifters and superconducting nanowire single-photon detectors (SNSPD) or CdHgTe avalanche photodiodes (APD), working at 2,5-4K that is compatible with single photon detectors. They are initially targeting secured QKD based telecommunications.

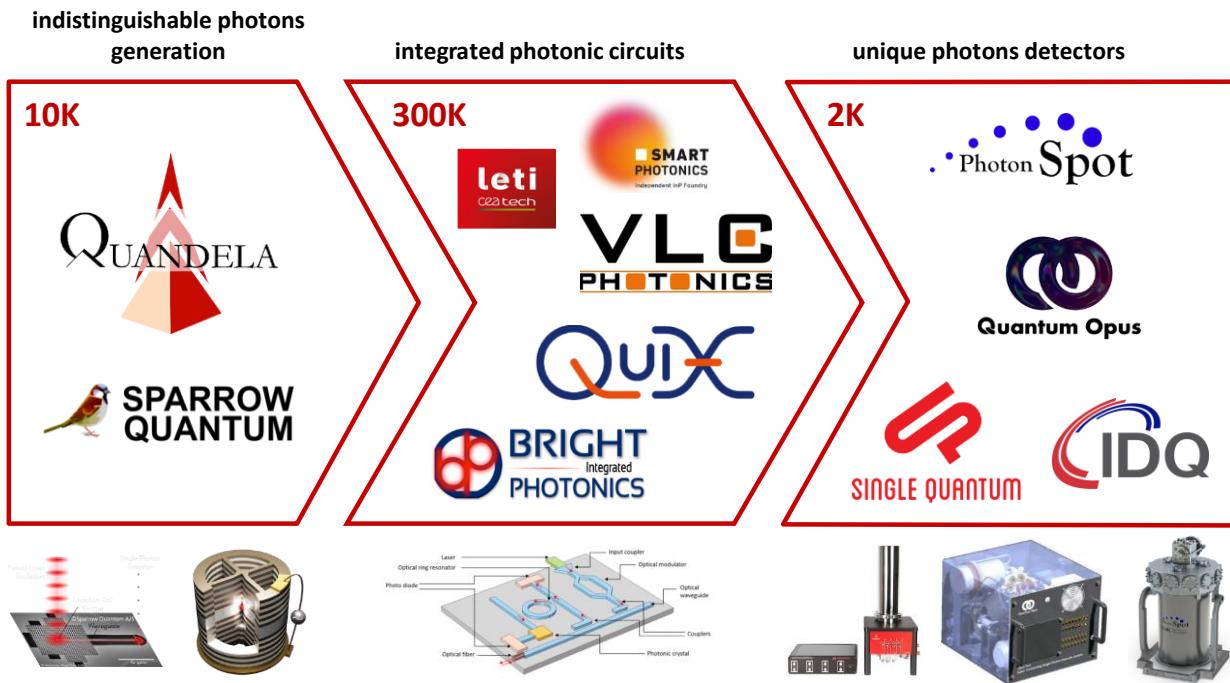
At last, in the integrated photonic circuits, let's mention **LightOn** (France) and their quantum photonic processor announced in 2021. It implements 8 input quantum states onto 19 distinct optical railings, performing 19x19 unitary linear operations with up to 8 entangled photons at minimal loss and a reconfigurability rate of 10Hz. This is based on using multimode fibers. It must be further documented to be fairly evaluated<sup>744</sup>.

Ultimately, a photon qubits quantum computer would consolidate three key components: a single photon generator, integrated photonic circuits and single photon detectors. The first and last ones are integrated with a cryogenic system operating at about 10K and 2K-4K respectively<sup>745</sup>.

<sup>743</sup> See [A 12-mode Universal Photonic Processor for Quantum Information Processing](#) by Caterina Taballione et al, 2020 (11 pages).

<sup>744</sup> See [LightOn Qore, a novel Quantum Photonic Processor](#), June 2021 (2 pages).

<sup>745</sup> Source of inspiration for the diagram: [Photonic quantum bits](#) by Pascale Senellart, June 2019 (31 slides) in slide 11.



source : adapted from Photonic quantum bits by Pascale Senellart, june 2019 (31 slides)

The most active countries in the field seem to be China, the United Kingdom (notably at the Universities of Oxford, Bristol, Cambridge and Southampton)<sup>746</sup>, France (C2N, LKB, ...), Italy<sup>747</sup>, Germany (notably at the Universities of Stuttgart and Paderborn), Austria, Australia, Japan, but the others are not outdone, with of course the USA.

In fact, it is the American "photonicists" from the research and private sector who were the most active in 2018 in their lobbying to trigger what has become the National Quantum Initiative Act. The same was true in Europe for the launch of the Quantum Flagship program the same year.

Photon qubits are the specialty of some startups like **PsiQuantum**, **Orca Computing**, **Tundra Systems Global**, **Quix**, **Quandela**, **Nu Quantum**, and **Xanadu**.

### Boson sampling

In photonics, the simulation of boson sampling is an experiment that is used to showcase the advancement of photon qubits. The idea of boson sampling came from **Scott Aaronson** and **Alex Arkhipov** from the MIT in a paper published in 2010<sup>748</sup>. They devised a linear optics-based experiment that would be impossible to easily emulate on a classical supercomputer<sup>749</sup>.

Boson sampling is about solving a problem of sampling the probability distributions of identical and indistinguishable photons being mixed in an interferometer and reaching single photon detectors. This physical process is impossible to emulate above a certain threshold, which generates yet another so-called "quantum supremacy" or "advantage".

<sup>746</sup> According to [Quantum Age technological opportunities](#) from the UK Government Office of Science in 2016 (64 pages).

<sup>747</sup> Fabio Sciarrino of La Sapienza University in Rome, carried out in 2013 a sampling of bosons with a chip with 13 input ports and 13 output ports, with three photons. See [Efficient experimental validation of photonic boson sampling against the uniform distribution](#), 2013 (7 pages).

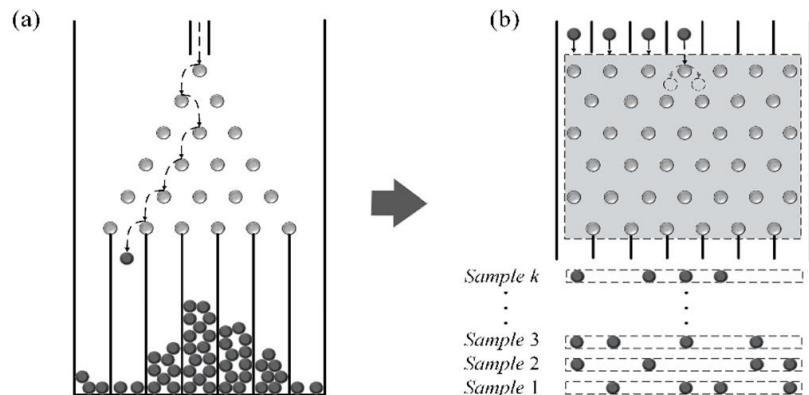
<sup>748</sup> See [The computational Complexity of Linear Optics](#) by Alex Arkhipov and Scott Aaronson, 2010 (94 pages).

<sup>749</sup> In quantum computing, we rely on only one type of boson: the photon. The other bosons are elementary particles such as gluons or Higgs bosons that can only be observed in particle accelerators. There are also composite particles such as the Cooper pairs (double electron) which are at the origin of superconducting currents. But when we talk about boson sampling, we always mean "photon".

A classical emulation requires extremely heavy matrix computing: the evaluation of square matrix permanents<sup>750</sup>. This sits in the "#P difficult" problem class of the complexity theories zoo<sup>751</sup>. The verification of the obtained result can't even be carried out by a classical computer<sup>752</sup>.

Boson sampling is the quantum and photonic analogue of the famous **Galton** plate experiment where balls cross rows of nails in a random way and end up in columns, with a Gaussian distribution<sup>753</sup>.

This experiment is based on various probability concepts: convergence of a binomial distribution law towards a normal or Gaussian distribution, Moivre-Laplace theorem, etc. In the photon-based experiment, photons are injected into a series of interferometers combining them with their neighbor in a random way.



On the other hand, the distribution at the end does not follow a Gaussian curve. It depends on the photons being sent upstream.

The appropriateness of the boson sampling style exercise is questionable. It implements a physical phenomenon with photons that is difficult to emulate in a classical way<sup>754</sup>. However, it is not strictly a form of calculation with some problem input data. There is not even a real notion of qubits, quantum gates and programming, except in the choice of the photons we send into the system. The optical components used are all passive and static, except the photon generators and detectors<sup>755</sup>.

It is a physics experiment generating additive and subtractive interferences and superposition of quantum states<sup>756</sup>. The difficulty of the experiment lies mainly in the complexity of the production of identical and indistinguishable photons. At this stage, nobody has managed to transform (or reduce) a useful algorithm into boson sampling.

<sup>750</sup> If you want to explore the question, see for example [Lecture 3: Boson sampling](#) by Fabio Sciarrino, University of Rome, (63 slides) and [Experimental boson sampling with integrated photonics](#) (33 slides) by the same author who describes laser-based techniques for etching integrated photonic components. As well as [Permanents and boson sampling](#) by Stefan Scheel, University of Rostock, 2018 (21 slides). As for the definition of the notion of permanent in [Wikipedia](#), it uses notions and notations of linear algebra that are not even explained. The permanent of a matrix is a variant of its determinant. If the classical resolution of sampling requires the computation of matrix permanents, its resolution by linear optics system does not allow the computation of matrix permanents.

<sup>751</sup> #P is the class of function problems that counts the number of solutions of NP problems.

<sup>752</sup> In 2018, a Chinese team carried out a numerical simulation of 50 photon boson sampling using 320,000 processors from the Tianhe-2 supercomputer. See [A Benchmark Test of Boson Sampling on Tianhe-2 Supercomputer](#), 2018 (24 pages). With the 20 photons and 60 modes of the Chinese experiment published in October 2019, a supercomputer is no longer able to follow.

<sup>753</sup> Source of illustration: [Quantum Boson-Sampling Machine](#) by Yong Liu et al, 2015.

<sup>754</sup> But this is a valid reality for the simulation of many complex physical phenomena, such as the folding of a protein or the functioning of a living cell, except that these remain in the realm of the living and are not simulated in a machine.

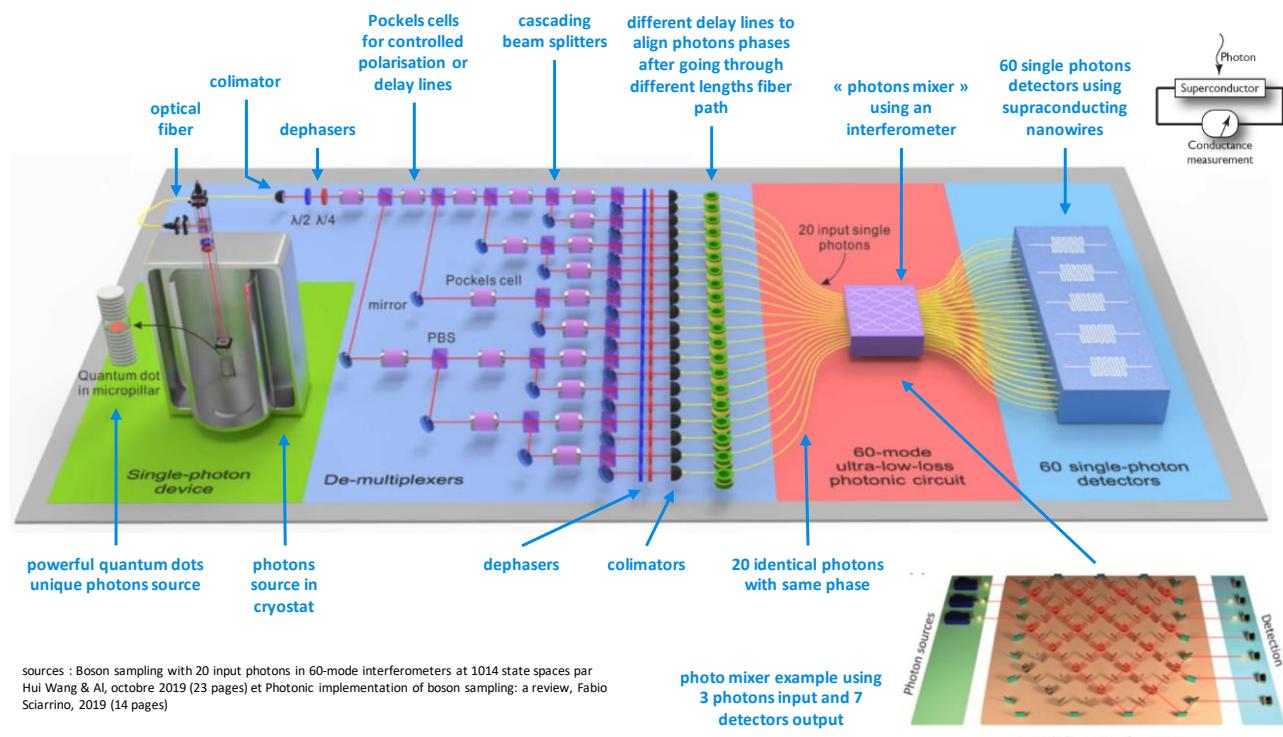
<sup>755</sup> See [An introduction to boson-sampling](#) by Jonathan Dowling et al, 2014 (13 pages) which describes well the issues involved in conducting boson sampling.

<sup>756</sup> See the animation [Boson Sampling with Integrated Photonics](#), 2015 (3mn) which describes the path of photons in a boson sampling experiment as well as [Photonic implementation of boson sampling: a review](#) by Fabio Sciarrino, 2019 (14 pages) which describes in detail this kind of experiment.

However, this could eventually lead to applications in homomorphic encryption and blind computing<sup>757</sup>. There are also some algorithms for simulating molecular vibrations based on boson sampling<sup>758</sup>. In 2020, a Chinese team was conducting an experiment similar to boson sampling to play a variant of the Go game<sup>759</sup>.

Chinese researchers are particularly active in the field<sup>760</sup>. In June 2019, the **Hefei** laboratory created a boson sampling using six photons with three degrees of freedom, therefore, based on qutrits (three-state qubits)<sup>761</sup>. The states of the photons were their traveled path, polarization and orbital angular momentum. With a gate error rate of 29%.

In October 2019, Chinese researchers upgraded the feat to 20 photons with an experiment presented as reaching quantum supremacy, at the same time as the announcement of Google Sycamore<sup>762</sup>. In this experiment described in the diagram *below*, 20 indistinguishable photons were sent in a series of splitters and ended up in 60 photon detectors. The output Hilbert space was limited to 14 detectors, with a size of  $3.7 \times 10^{14}$  or  $2^{48}$ . With the 60 activated detectors, this space should be able to reach a size of  $60^{20}$  or  $2^{118}$ .



<sup>757</sup> Seen in [Introduction to boson-sampling](#) by Peter Rohde, 2014 (34 minutes) which refers to [A scheme for efficient quantum computation with linear optics](#) by Emanuel Knill, Raymond Laflamme and Gerard Milburn, 2001 (7 pages) which theorized that quantum computation based on linear optics was plausible. We owe them the KLM scheme or protocol (their initials), a linear optics quantum computing (LOQC) programming model that has the disadvantage of being very heavy in terms of the number of hardware devices.

<sup>758</sup> See [Boson sampling for molecular vibronic spectra](#) by Joonsuk Huh, Alán Aspuru-Guzik et al, 2014 (7 pages) and [Vibronic Boson Sampling: Generalized Gaussian Boson Sampling for Molecular Vibronic Spectra at Finite Temperature](#) by Joonsuk Huh et al, 2017 (10 pages).

<sup>759</sup> See [Quantum Go Machine](#) by Lu-Feng Qiao et al, July 2020 (16 pages).

<sup>760</sup> See [Chinese researchers on the road to the 'ultimate' quantum processor?](#) by Bruno Cormier, September 2018 which points to [Building Quantum Computers With Photons Silicon chip creates two-qubit processor](#) by Neil Savage, September 2018 which discusses the creation of a two-qubit quantum processor. The original article is [Large-scale silicon quantum photonics implementing arbitrary two-qubit processing](#), September 2018 (23 pages). The researchers involved were Chinese, English and Australian.

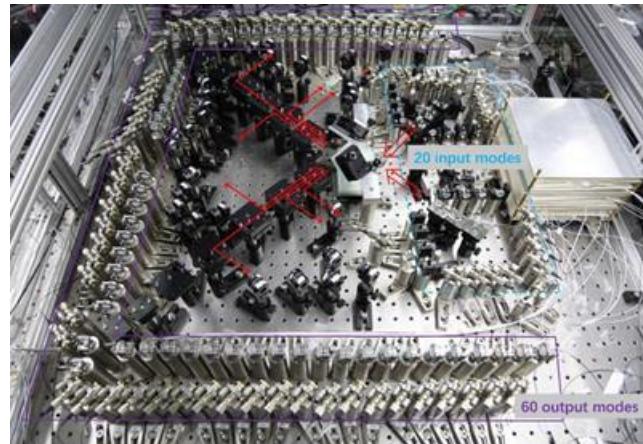
<sup>761</sup> See [18-Qubit Entanglement with Six Photons Three Degrees of Freedom](#) by Xi-Lin Wang et al, June 2019 (14 pages).

<sup>762</sup> See [Boson sampling with 20 input photons in 60-mode interferometers at  \$10^{14}\$  state spaces](#) by Hui Wang et al, October 2019 (23 pages).

The size of Hilbert's space of such a device is evaluated with the size of the Fock space of M modes occupied by N photons. This would give a binomial space  $(\frac{M+N-1}{M})$  so  $(\frac{79}{60})$  which is equal in size to  $\frac{79!}{60!*19!}$  ([source](#)).

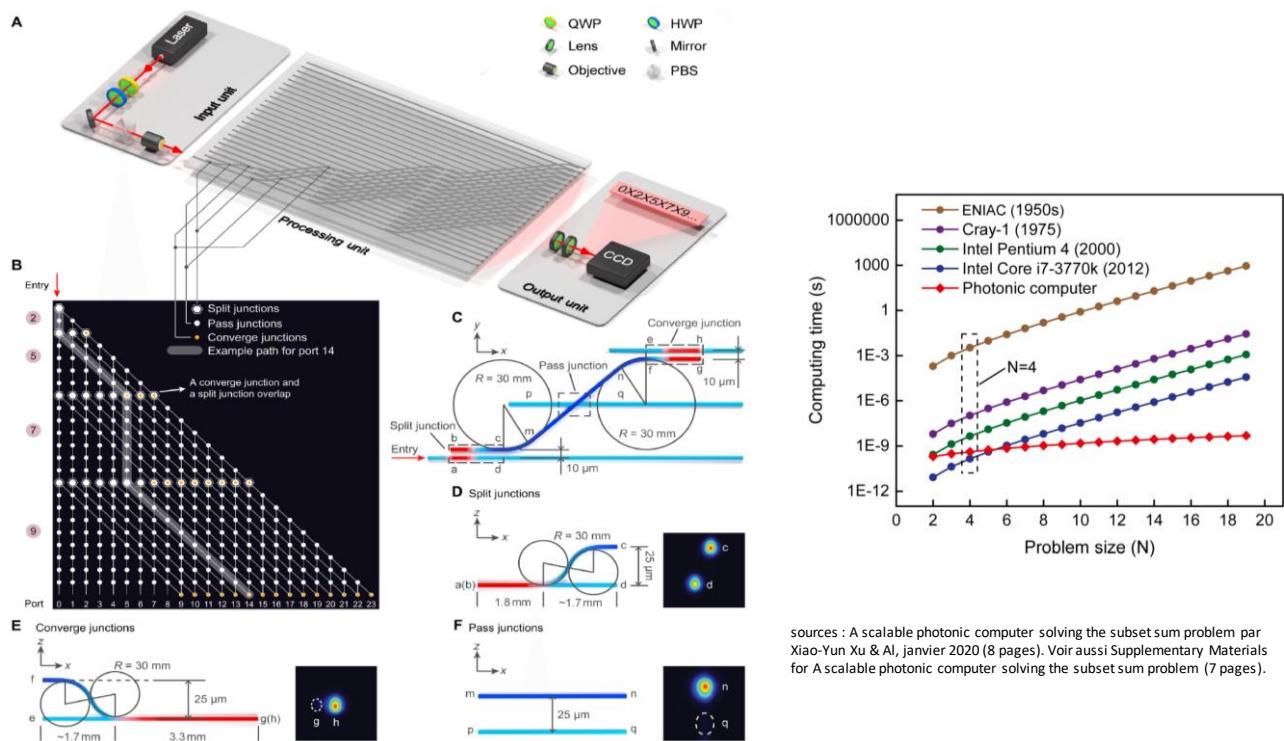
The Chinese researchers indicated that they could use several hundred detectors in output and use a double encoding of photons (polarization and spatial encoding) to multiply the power of their system and thus make it able to create a NISQ (noisy intermediate scale quantum computer) system, except that the ability to program it does not seem obvious, nor its uses.

This represents the number of incoming photon detectors at the power of the incoming photon number. The previous record was 5 photons over 16 modes and the sampling was verifiable on a classical computer whereas with these 20 photons and 60 modes, it is no longer possible. The photon generator was realized with quantum dots in gallium and indium arsenide, placed in a 4K<sup>763</sup> cryostat. The photon mixer used 396 beam splitters and 108 mirrors. For the experiment to work, one photon must arrive at the same time in all the inputs of the photon mixer.



The corresponding probability is very low. They use active demultiplexers with Pockels cells to demultiplex and direct the photons.

In 2020, other Chinese researchers used an optical quantum calculator to solve a useful problem, the subset-sum problem, which is complete NP. The system, *below*, uses a chipset much more miniaturized than the usual boson sampling experiments.

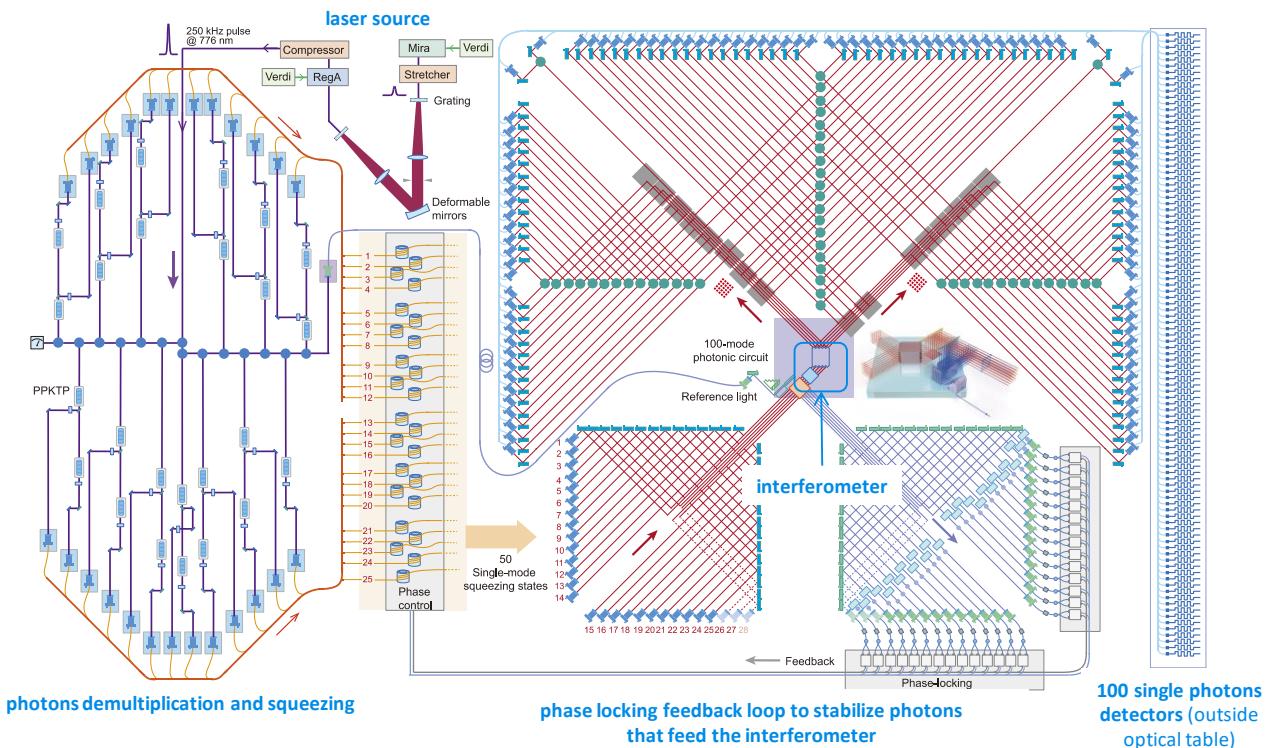


<sup>763</sup> The photon source would come from a German laboratory located in Würtzburg, Bavaria. It is largely inspired by the reference work in the field of Pascale Senellart's team from the CNRS C2N.

The problem is to determine, apart from a set of signed integers, whether it is possible to add a subset of them together to obtain a given integer<sup>764</sup>. The system uses a laser as a source of photons. The benchmark has been realized with N=4 integers. They indicate that by extrapolating, their system would beat all other known methods of solving this kind of problem.

One of the perspectives of photon-based qubits is to bypass their flaws with the use of MBQC and *cluster states*, which we have already defined on page 352. Indeed, these use the implementation of an entangled state between all qubits and then a measurement of the progressive state of the others. This avoids the complexity of optical quantum gates, which are difficult to implement, whereas we now know how to create a set of well-entangled photons.

In December 2020, the stakes went higher with a **gaussian bosons sampling** done with 70 photons modes<sup>765</sup>. The experiment was even more impressive than the previous ones and the publicized quantum advantage reached new heights. But the system was not more programmable than the previous ones (schematic below).



In June 2021, the same China team however upgraded their GBS (Gaussian Boson Sampling) experiment and made it somewhat programmable, ramping it up to 113 detection events extracted from 144 photon modes circuit. The input squeezed photons are phase programmable, before they enter the fixed part of the experiment in the interferometer. They still have to implement some real-world algorithms and benchmarks to demonstrate sort of quantum computing advantage<sup>766</sup>.

<sup>764</sup> See [Photonic computer solves the subset sum problem](#), February 2020 which points to [A scalable photonic computer solving the subset sum problem](#) by Xiao-Yun Xu et al, January 2020 (8 pages). See also [Supplementary Materials for A scalable photonic computer solving the subset sum problem](#) (7 pages).

<sup>765</sup> See [Chinese Scientists Begin Climb Toward Universal Quantum Computer](#) by Matt Swayne, December 2020, [Chinese scientists say they've achieved a quantum computing breakthrough](#) by Shiyin Chen et al, December 2020 and [Quantum computational advantage using photons](#) by Han-Sen Zhong et al, December 2020 (23 pages) and the [supplemental materials](#) (64 pages). See [Benchmarking 50-Photon Gaussian Boson Sampling on the Sunway TaihuLight](#) by Yuxuan Li et al, 2020 (12 pages) for the classical emulation on classical supercomputers.

<sup>766</sup> See [Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light](#) by Han-Sen Zhong, Chao-Yang Lu, Jian-Wei Pan et al, June 2021 (9 pages).

Late 2020, a competing Chinese team implemented another form of boson sampling using “membosonsampling” for which an emulation requires even more complicated Haar-random unitary matrix<sup>767</sup>. But it was not programmable.

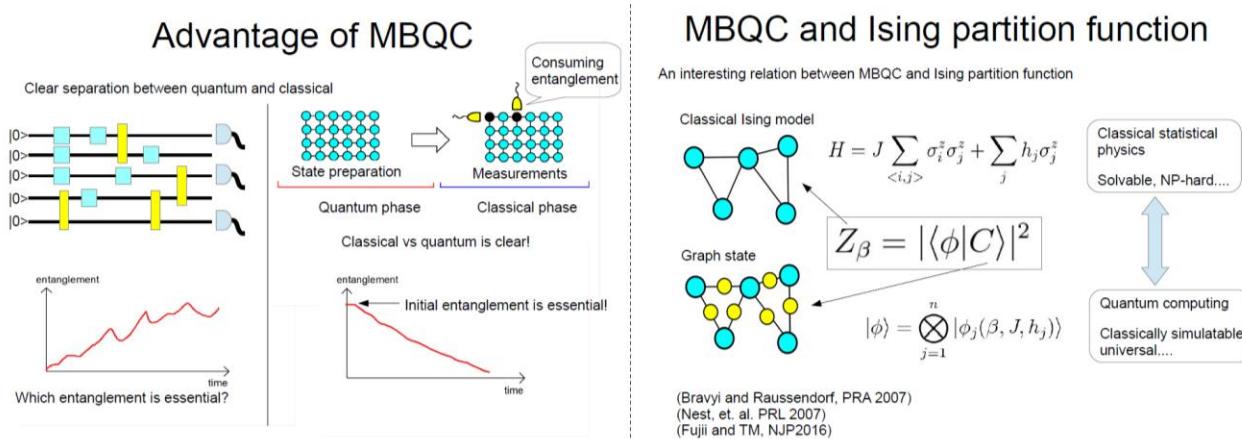
## Measurement Based Quantum Computing

MBQC is a very particular approach to quantum computing. It consists in exploiting the initialization of entangled qubits and then performing step-by-step measurements on certain qubits to obtain a result on the last measured qubits at the end of the run. There are several variants, the *one-way quantum computing* (1WQC<sup>768</sup>) which uses two-dimensional qubits matrices to create cluster states and the *measurement-only QC* which only measures qubits, without prior entanglement. We will focus here on the first method which seems to be the most commonplace.

MBQC allows the execution of classical quantum algorithms with universal gates. Where is it relevant? It is particularly interesting in qubit-based quantum systems where it is difficult to create multi-qubit quantum gates exploiting entanglement and where the number of chained gates is limited for physical reasons.

The model was initially created for cold atoms qubits but it later made more sense with photon qubits for which two-qubit gates are difficult to create. Photons are also indicated because they allow to easily manage rotation angles in the Bloch sphere that are used in the single-qubit quantum gates of the process, via a phase control of the photon qubits.

With MBQC, things are done a bit backwards with respect to classical quantum computing: we first apply single-qubit gates and measure them progressively, whereas in classical quantum computing with universal gates, we only involve qubits progressively and then make measurements at the end of computation.



<sup>767</sup> See [Quantum Advantage with Timestamp Membosonsampling](#) by Jun Gao, December 2020 (30 pages).

<sup>768</sup> MBQC was designed in 2000 by Robert Raussendorf and Hans Briegel. See [A computationally universal phase of quantum matter](#) by Robert Raussendorf, 2018 (41 slides), [Measurement-based Quantum Computation](#) by Elham Kashefi, University of Edinburgh (50 slides) and the extensive [Introduction to measurement based quantum computation](#) by Tzu-Chieh Wei from Stone Brook University, 2012- (88 slides) and a one pager: [Universal measurement-based quantum computation with Mølmer-Sørensen interactions and just two measurement bases](#). Other information sources include [Blind quantum computation](#) by Charles Herder (10 pages), [Cluster-state quantum computation](#) by Michael Nielsen, 2005 (15 pages), [Fault-tolerant quantum computation with cluster states](#) by Michael Nielsen and Christopher Dawson, 2004 (26 pages), [2D cluster state](#) (50 slides), [Quantum Computing with Cluster States](#) by Gelo Noel Tabia, 2011 (18 pages), [Quantum picturalism for topological cluster-state Computing](#) by Clare Horsman 2011 (18 pages) and [Cluster State Quantum Computing](#) by Dileep Reddy et al, 2018 (11 pages). See also [Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments](#) by Stephanie Barz, 2015 (26 pages).

An MBQC calculation is **logically irreversible**, unlike a quantum algorithm based on universal quantum gates. Indeed, the process of measuring qubit states cannot be logically reversed except when the state of the qubits read corresponds exactly to their basis states  $|0\rangle$  and  $|1\rangle$ .

A quantum computation executed with universal gates is the equivalent of applying a unitary transformation embodied by a giant square matrix of dimension  $2^N$  to a set of N qubits initialized in the state  $|0\rangle$ . This matrix can be inverted by scrolling backwards the quantum gates that were used to create it. With MBQC, this is not possible. This irreversibility of MBQC calculations explains why it is also called 1WQC for One Way Quantum Computing. There is no way going back.

This model is also **probabilistic**, due to the probabilistic nature of the state measures of qubits at each step of the calculation. The successive measurements provide information on the state of the qubits, which makes it possible to become deterministic again in the rest of the computation by applying a kind of error correction on the fly. A bit like using 3-qubit error correction codes.

By definition, MBQC is a **hybrid algorithms** method since its implementation depends on interactions between quantum computing and the exploitation of qubits readout data by a classical computer controlling the system.

Qubits used in the cluster state-based MBQC are of four different classes: those that are prepared and measured (the ancilla qubits), those that are only measured during computing, those that are only prepared (but measured at the end of computing) and those that are neither prepared nor measured (and are used for the rest of computing).

The principle is based on the sequencing of so-called NEMC sequences with four steps<sup>769</sup>:

- Using a set of **ancilla qubits** (step N), those of the first type which are measured with a Z projection.
- Creating **entanglement** between some of the qubits (step E) in groups called "cluster states". The system does not entangle all the qubits in the quantum register. It does so group by group, these clusters. Entanglement is, for example, generated by a series of Control-Phase (or control R) gates on qubits initialized in the state  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  with an H gate applied to the state  $|0\rangle$ . As these gates are commutative, the order in which they are executed to prepare entanglement does not matter. This can enable a heavy parallelization of processing using MBQC. A cluster is any graph of entangled qubits, the most common being a 2D matrix of qubits all entangled with their immediate neighbors.
- Measuring **state of intermediate qubits** during computing (M). It is carried out with a variation of projective measurement. It consists in first applying one or more X or Y gates to a qubit to create a rotation in their Bloch sphere and then to measure their state on the computational basis. It is a bit like rotating the Z ( $|0\rangle/|1\rangle$ ) axis in the Bloch sphere to change the reference point.

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

$$|\pm_\alpha\rangle = \frac{|0\rangle \pm e^{i\alpha}|1\rangle}{\sqrt{2}}$$

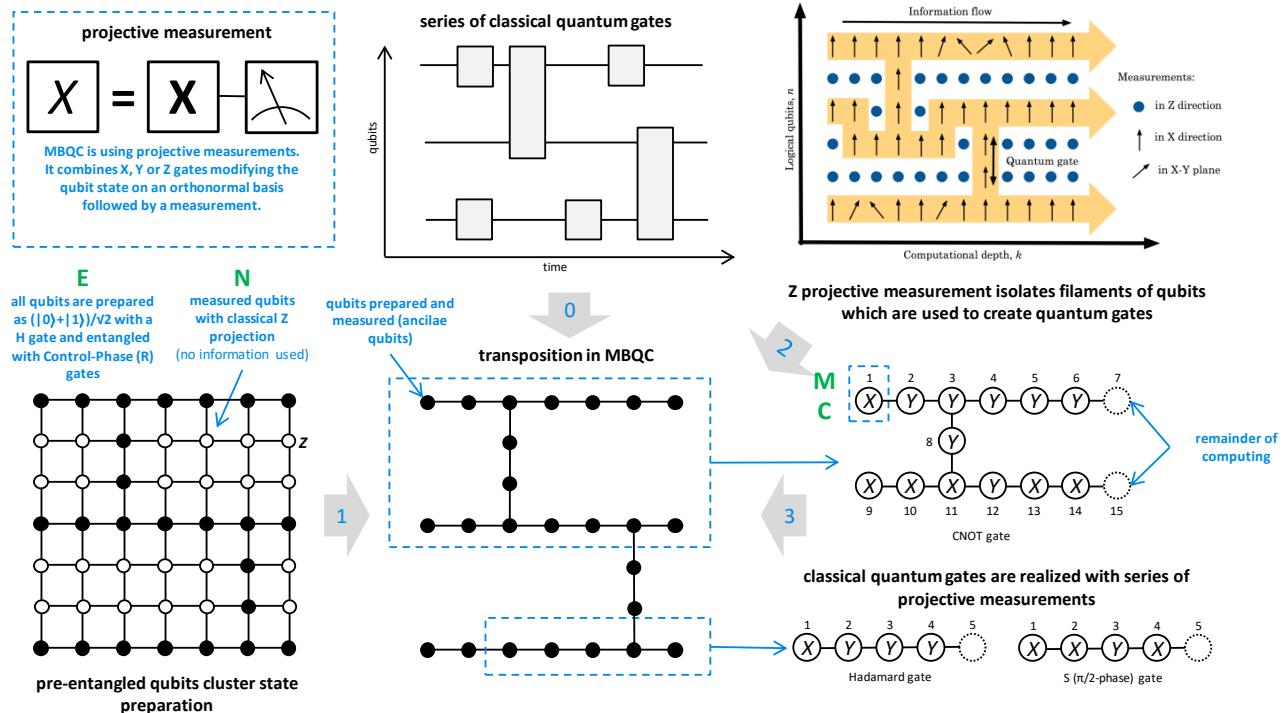
The projective measurement basis is in the form of states of the type  $|\pm_\alpha\rangle$ ,  $\alpha$  being generally a half or quarter turn in Bloch's sphere. A measured qubit is always an intermediate resource and is not an output resource. This helps obtaining an information that can be used to manipulate the qubits afterwards to propagate computation. Projective Z measurements have the effect of removing the measured qubits from the cluster.

---

<sup>769</sup> Information sources: [Advanced Quantum Algorithms](#) by Giulia Ferrini et al, 2019 (30 pages) and [An introduction to Quantum Computing](#) by Elham Kashefi, School of Informatics University of Edinburgh, 2020 (119 slides).

- These successive **corrections** make computing deterministic (step C) with X and Z gates. They are applied according to the result of the projective measurements made in (M). No correction gate acts here on a qubit already measured. This model makes it possible to apply any gate to a qubit which is in fact a combination of  $Rz(\gamma)Rx(\beta)Rz(\alpha)$ , i.e. rotations around the three axis of the Bloch sphere of angles  $\gamma$ ,  $\beta$  and  $\alpha$ <sup>770</sup>.

All this is summarized in the following composite diagram:



What I have just described allows to interpret the lower right-hand part of the *above* illustration which explains how the MBQC equivalents of the CNOT (two-qubit), H or S quantum gate equivalents are realized in MBQC. Each X or Y circle is an X and Y projective measure that combines an X or Y gate followed by a qubit readout. The result conditions the type of projective measurement performed immediately afterwards in the order indicated (1 to 15 and 1 to 5).

Two forms of measurements affect the functioning of the qubit matrix: Z measurements separate the qubits by digging sort of grooves in the qubits matrix, a bit like pacmans, then classical measurements along the "wires" or on the "bridges" between these wires simulate single-qubit gates like Hadamard's and the two-qubit CNOT gates. The sequence of operations depends on the result of each measurement along the wires. The computation result is located in the last qubits whose state is not yet measured and which will be measured last<sup>771</sup>.

This combination of NEMC sequences allows the reproduction of the operation of one- and two-qubit quantum gates. A complete quantum computation is a sequence of multiple NEMCs that ends with the measurement of the state of the remaining qubits!

<sup>770</sup> The decomposition of quantum gates into a computational method that can be used for MBQC has been [patented](#) by Krysta Svore of Microsoft, who leads the QuArC group there.

<sup>771</sup> Illustrations sources: [Basics of quantum computing and some recent results](#) by Tomoyuki Morimae, 2018 (70 slides).

The consequences of what we have just seen are multiple:

- MBQC requires way **more qubits** than in a conventional circuit-based model. We've seen that a single X or Y gate results from the combination of four X and Y gates and as many measurements. This in turn creates a "pressure" on the classical part of the calculation, linked to the measurement. But we catch up (further on) with parallelism.
- MBQC still requires **error correction codes** such as those we have studied in a previous section, page 200. They too will multiply by several orders of magnitude the number of physical qubits necessary for computing any algorithm. It could be facilitated if we could organize the qubits in 3D matrices, the third dimension being used to align the qubits necessary for error correction, especially with surface codes. On the other hand, since MBQC models contains its own error correction mechanisms, it is less demanding in terms of additional qubits for error correction necessary for the creation of "fault tolerant" quantum computers.
- The **temporal dimension** of computing is modified compared to classical gate-based quantum computing. As we can parallelize operations coupling gates and measurements, MBQC is a bit like Nutella on the breadcrumbs: we can spread it out! The depth of the available computation is no longer linked to the ability to chain quantum gates in time as in the middle-high diagram in the previous illustration, but to execute a large number of them in parallel over a very large number of qubits (modulo the required error correction). The sequences of measurements labeled 1, 2 ... n will be carried out simultaneously in groups 1, 2 ... n, n being limited to 15. Therefore, the required physical calculation depth is defined by the maximum number of physical gates to execute to create a CNOT. This is an argument in favor of photon qubits. The depth of an algorithm no longer depends on the ability to chain quantum gates with one and two qubits, but on the entanglement capacity of the qubits at startup in the model's cluster states. In short, sequential quantum computing is replaced by massively parallel quantum computing with a very shallow depth. This is the approach chosen by PsiQuantum.
- An MBQC model is easily exploitable to take advantage of teleportation and **distributed quantum computing** algorithms. Cluster states will be able to be linked together via remote optical links. It is also one of the tools of blind computing<sup>772</sup>.
- Finally, there is a direct link between the MBQC and the **ZX Calculus**. ZX Calculus is a graph model that help formalizing MBQC, its cluster states and the associated error corrections<sup>773</sup>.
- The **algorithms** are specific to this kind of architecture<sup>774</sup>. It is not yet experimental because it requires a large number of qubits that are not yet practically available.

## Startups



**PsiQuantum** (2016, USA/Europe, \$728M) is a startup created by Jeremy O'Brien, a former Stanford and Bristol University researcher, who wants to create a photon-based quantum processor in CMOS silicon technology.

<sup>772</sup> See [Measurement-based and Universal Blind Quantum Computation](#) by Anne Broadbent, Joseph Fitzsimons and Elham Kashefi, 2016 (41 pages).

<sup>773</sup> Seen in [Universal MBQC with generalised parity-phase interactions and Pauli measurements](#) by Aleks Kissinger and John van de Wetering, 2019 (21 pages).

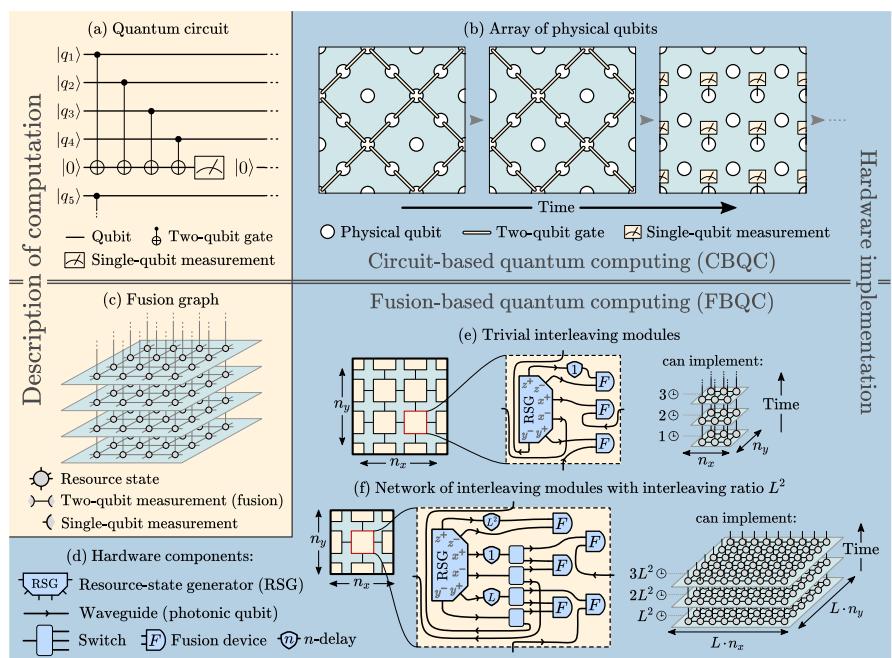
<sup>774</sup> See for example [Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states](#), May 2019 (16 pages). The article describes an MBQC method based on the exploitation of Toffoli (CCZ) and Hadamard (H) gates. They allow to simulate topological quantum computation, reducing the error rate of quantum computation.

He is accompanied by Pete Shadbolt (co-inventor of the VQE algorithm with Jeremy O'Brien and Alán Aspuru-Guzik), Mark Thompson and Terry Rudolph, who discovered when he finished his physics thesis that he was a grandson of Erwin Schrödinger, which may have helped with fundraising! The company already employs over 150 people, most of them in Palo Alto in the USA, but some of them work remotely all over the world, including one person in France.

Early in 2021, the company started to be more open on its technology<sup>775</sup>. It published a paper describing their qubit architecture, using an **FBQC** system, aka Fusion-based quantum computation, a variant of MBQC that we study a bit later. It uses micro-clusters states with groups of 4 qubits connected together and using Resource State Generators (RSGs). It's replacing measurement of entangled states by double measurement of non-connected adjacent qubits to create entanglements between them.

This is what they call dual-rail encoding with lines for photon states  $|0\rangle$  and  $|1\rangle$ .

Two qubit gates use XX nondeterministic and ZZ deterministic measurements (measuring two photons simultaneously with the same polarization basis), implemented with a beam splitter then combining fusions to create small cluster states. With that, the qubits computing depth is quite shallow, avoiding the pitfalls of qubits error rates. It's replaced by a large breadth of computing and commutative operations replacing "depth-computing" by "breadth-computing"<sup>776</sup>.



Their ambition is to produce a system with one million physical qubits generating the equivalent of 100 logical qubits.

Their photonic chipsets manufacturing is handled at the 300 mm wafers **Global Foundries** Luther Forest Technology Campus in upstate New York. They announced having produced a first q1 chip-set sample in April 2021 integrating tens of thousands of single photon sources and detectors<sup>777</sup>.

Their physical architecture is using sandwiches assembling a 22 nm CMOS electronic chipset of 750M transistors using superconducting nanowires bonded with 100K connections to a photonic chipset containing thousands of photon sources, detectors and other optical devices.

The photonic chipset has 200 optical fiber entries and exits that are used to interconnect similar photonic chipsets together in a distributed architecture manner.

<sup>775</sup> See [Silicon Photonic Quantum Computing - PsiQuantum at 2021 APS March Meeting](#) by Jeremy O'Brien, April 2021 (25 mn).

<sup>776</sup> See [Percolation thresholds for photonic quantum computing](#) by Mihir Pant, 2017 (14 pages). The process is also documented in [Towards practical linear optical quantum computing](#) by Mercedes Gimeno-Segovia, 2015 (226 pages). This was the last publication on the PsiQuantum architecture until when they released [Fusion-based quantum computation](#) by Sara Bartolucci et al, January 2021 (25 pages). See also [QIP2021 Tutorial: Architectures for fault tolerant quantum computing](#) by Naomi Nickerson, January 2021 (3h).

<sup>777</sup> See [PsiQuantum partners with GLOBALFOUNDRIES to bring up Q1 quantum system](#) by Mercedes Gimeno-Segovia, PsiQuantum, May 2021.

The final PsiQuantum 1 million physical qubits computer will be made of thousands of computing chips connected together so we can presume each chip is implementing fewer than 1000 physical qubits.

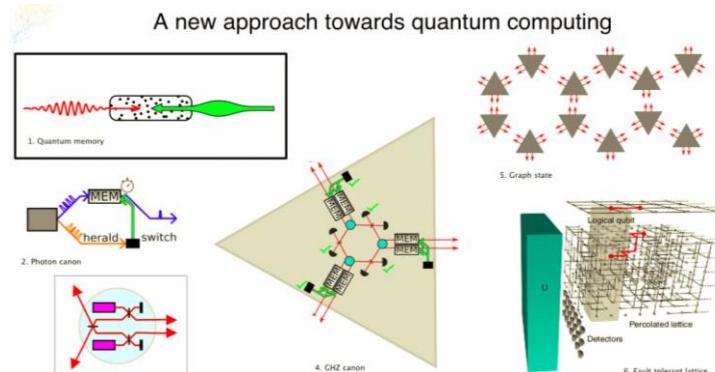
The whole system will run at a temperature of 4K, requiring only a pulse tube refrigeration system, that is much simpler than a dilution system for sub 100mK temperatures and with more cooling power. They are also using fiber delay lines as optical memory thanks to its low loss rate. It is mixed with topological fault tolerance codes. This is supposed to multiply by 5000x the number of usable qubits<sup>778</sup>.

To date, PsiQuantum is the best funded startup in the world in quantum computing, even ahead of D-Wave and Rigetti and on par with IonQ and its 2021 SPAC. Originally from the United Kingdom, it moved part of the team to the USA<sup>779</sup>. They even have Microsoft as investors as well as Pascal Cagni's investment fund, C4 Ventures. Their last funding round of \$450M in July 2021 cemented this funding lead.



**ORCA Computing** (2019, UK, \$3.7M including some UK public funding) is developing a quantum computing platform based on photons and photonic memory<sup>780</sup>. It's also relying on MBQC, a quantum computation management method which consists in starting by creating a cluster state of entangled qubits (in this case GHZ states) and progressively reading the qubit states to carry out its computations progressively. They also use optical frequency combs and continuous variables. Their chipset is manufactured by **Ligentec** in Switzerland.

The startup was co-founded by Richard Murray (CEO, former head of the UK quantum program), Josh Nunn (CTO, former Oxford University, also working for VeriQloud) and Cristina Escoda (COO), an entrepreneur with a background in finance and deep tech<sup>781</sup>. Their roadmap consists in creating 3 qubits by 2024 and hundreds of qubits by 2026. Quantonation is one of their investors.



**TundraSystems** (2014, UK) is developing a linear optics quantum processor operating supposedly at room temperature. They seem to create a photonic microprocessor and not necessarily, a quantum computer with qubits using linear optics.

Their Advisory Board includes two Chinese scientists, Xinliang Zhang and Pochi Yeh who are specialized in optronics ([site](#)).

<sup>778</sup> See [Interleaving: modular architecture for fault-tolerant photonic quantum computing](#) by Hector Bombin et al, 2021 (22 pages).

<sup>779</sup> See the presentation [Measurement-based fault tolerance beyond foliation](#) by Naomi Nickerson of PsiQuantum in September 2019 and [Quantum Computing With Particles Of Light: A \\$215 Million Gamble](#) by Paul Smith-Goodson, April 2020.

<sup>780</sup> See [One-Way Quantum Computing in the Optical Frequency Comb](#) by Nicolas C. Menicucci, Steven T. Flammia and Olivier Pfister, April 2018 (4 pages) and [High-speed noise-free optical quantum memory](#) by K. T. Kaczmarek et al, April 2018 (12 pages).

<sup>781</sup> See some details on their approach in [Photonic quantum processors](#), Orca Computing, April 2020 (27 slides).



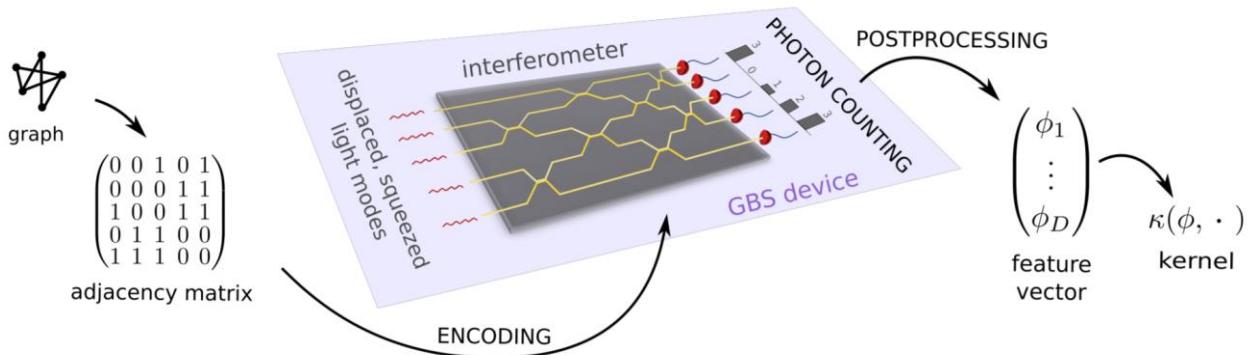
X  $\wedge$  N  $\wedge$  D U

**Xanadu** (2016, Canada, \$135.6M) is a startup created by Christian Weedbrook, a [prolific researcher](#) having started at MIT and the University of Toronto, among others. The startup is developing a photon qubit quantum computer that should also theoretically operate at room temperature and would become a FTQC (fault tolerant quantum computer).

This is, as usual, a questionable assertion given photon generators and detectors in this kind of system are usually using a cryostat.

In September 2020, they launched a cloud-based testing platform of 8 and 12 qubits, to be upgraded to 24 qubits. Their qubits are qumodes based on squeezed states using continuous variables encoding<sup>782</sup>. The 8-qubit silicon-nitride chipset is 4mm x 10 mm wide. It's fed by infrared laser pulses and generates "squeezed states" superposing multiple photons, then flowing through an interferometer made of beam splitters and phase shifters performing quantum gates, and exiting to superconducting photon detectors. They don't specify the detailed characteristics of these qubits, particularly in terms of fidelity<sup>783</sup>.

In 2021, a team of Xanadu and Canadian researchers published a blueprint with more details on the Xanadu FTQC architecture. It's based on MBQC and three-dimensional resource states comprising both GKP bosonic qubits and squeezed states of light. This hybridization enables the implementation of both Clifford and non-Clifford gates. All of this will be implemented on 2D photonic chipsets<sup>784</sup>. In August 2021, Xanadu announced that their FTQC silicon-nitride chipsets would be manufactured by IMEC in Belgium.



Xanadu develops the software platform **Strawberry Fields** and **PennyLane** in Python<sup>785</sup> (wondering about the inspiration...). It includes the Blackbird language and targets chemistry use cases, graph theory problems and quantum machine learning. All this is distributed in open-source.

Their main application is the analysis of similarities between graphs to identify those that are similar and/or separate them into several classes of similarity. Classical methods for solving this kind of problem are similar to finding a matrix determinant<sup>786</sup>.

<sup>782</sup> Their process is documented in [The power of one qumode for quantum computation](#), 2016 (10 pages) with an example of implementation in [Continuous-variable gate decomposition for the Bose-Hubbard model](#), 2018 (9 pages). See also [Optical hybrid approaches to quantum information](#) by Peter van Loock, 2010 (35 pages). See also [Quantum computing with multidimensional continuous-variable cluster states in a scalable photonic platform](#) by Bo-Han Wu et al, 2020 (22 pages).

<sup>783</sup> See [In the Race to Hundreds of Qubits, Photons May Have "Quantum Advantage"](#) by Charles Q. Choi, March 2021.

<sup>784</sup> See [Programmable optical quantum computer arrives late, steals the show](#) by Chris Lee, March 2021 referring to [Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer](#) by J. Eli Bourassa et al, February 2021 (38 pages).

<sup>785</sup> This is documented in [Strawberry Fields: A Software Platform for Photonic Quantum Computing](#), 2018 (25 pages).

<sup>786</sup> See [Measuring the similarity of graphs with a Gaussian Boson Sampler](#) by Maria Schuld et al, 2019 (11 pages).



**Quandela** (2017, France, €35M) is expanding its historical single photon source activity to create photon qubits computing systems as part of their project ROQC (Reconfigurable Optical Quantum Computer). Their initial goal is to reach 10 qubits and more afterwards.

The targeted use cases are certified QRNGs using Bell states, hybrid quantum machine learning algorithms and chemical simulations. The Quandela team plans to deploy a platform that will handle a few digital qubits in the cloud in 2022.



**QBoson** (2020, China) was founded by Wen Kai, who has a PhD in quantum computing from Stanford and worked before at Google AI in the USA.

The company is creating photon-based quantum computers with, in sights, an hybrid AI applications approach. They claim to have completed the construction of a laboratory and of a 1,000 photon-based qubit quantum computer with a plan to reach 1 million-qubits in 3 to 4 years.

The first part is probably a little oversold even if the second part is not far from PsiQuantum promises<sup>787</sup>. Another promise is that this computer works at ambient temperature, which is a highly dubious claim whether it's based on photons or on cold atoms. In both cases, you need some form of cooling for your light sources and photon detectors.

On the left, the only visual of the laboratory that was inaugurated in July 2021. Go guess the type of qubits they are working on with this ([source](#))!



**Duality Quantum Photonics** (2020, UK) is a Bristol-based startup created in February 2020. Its founder is Anthony Laing, from the Department of Physics at the University of Bristol where he developed a quantum simulator based on lithium niobate generated photons.

He targets drugs design for the pharmaceutical industry. They were supposed to create a prototype in 2021.



HP conducts research in quantum computing at its laboratory in Bristol, UK, covering quantum computing, cryptography and quantum communications.

They invested in "The Machine", conceptually far from a universal quantum computer and uses an optical bus to link the different components of a supercomputer.

<sup>787</sup> Wen Kais thesis is [Experimental study of tune-out wavelengths for spin-dependent optical lattice](#) in <sup>87</sup>Rb Bose-Einstein condensation by Kai Wen et al, September 2021 (9 pages). It relates to cold atoms qubits, not photons. But QBoson's communication is about photonic qubits controlled by lasers ([source](#)). All in all, one thing is sure: these guys don't want you to know what they are doing exactly.

In partnership with HP, American and Japanese scientists proposed in 2008 the creation of an HPQC, High Performance Quantum Computer, with 3D qubit arrays realized in linear optics containing 7.5 billion physical qubits allowing to accumulate 2.5 million logical qubits<sup>788</sup>. This project was left aside. HPE abandoned quantum computing entirely and explained it in 2019. They said they preferred to focus on neuromorphic processors and memristors<sup>789</sup>.

Their photonics specialist is **Ray Beausoleil**, based in Silicon Valley. He was specialized in photonics and NV centers and abandoned this track, becoming a quantum computing skeptic. Somewhat along the lines of Gil Kalai, he believes that errors would increase faster than the growth in the number of qubits. Still, HPE invested in **IonQ** in October 2019 to show that it didn't entirely leave the quantum stage.

### Quantum computing hardware key takeaways

- Superconducting qubits are the most common nowadays, implemented by IBM, Google and Rigetti among others. But they are noisy and do not scale well. One solution may be cat-qubits which combine trapped microwave photons in cavities and superconducting qubits for their manipulation and readout (Alice&Bob and Amazon).
- Electron spin qubits could scale well due to their small size, the reuse of classical CMOS semiconductors manufacturing known-how, their higher working temperature enabling the usage of control cryo-electronics. They have been however demonstrated at a relatively low scale at this stage.
- NV centers qubits have the benefit to be stable and to work potentially at ambient temperature but there are not many vendors involved there, besides Quantum Brilliance (Australia).
- Topological qubits would bring the benefit of being resilient to quantum errors and to scale better than other solid-state qubits. But, it doesn't really exist yet, particularly the Majorana fermions species looked after by Microsoft.
- Trapped ions qubits have the best fidelities so far, but they are hard to scale beyond 32 qubits, at least with their main vendor, IonQ. Honeywell may have a solution to scale it.
- Cold atoms qubits are mostly used in quantum simulation where it could scale up to a thousand qubits but it could potentially also be used in gate-based quantum computing although it's not really demonstrated. Pasqal (France) and Cold Quanta (USA) are the main players in this field.
- Photon qubits are flying qubits, moving from a source to detectors and traversing optical devices implementing quantum gates. There are many investigated techniques, with the distinction between single/discrete variable photons and continuous variable photons. Scalability is also an issue, particularly with photon sources and the probabilistic nature of photons generation. Their limited quantum gates computing depth requires the implementation of specific computing techniques like MBQC and FBQC, this last one being used by PsiQuantum, the best funded quantum computing startup with IonQ as of mid-2021. Quandela (France), Xanadu (Canada) and Orca (UK) are other key players in that space.

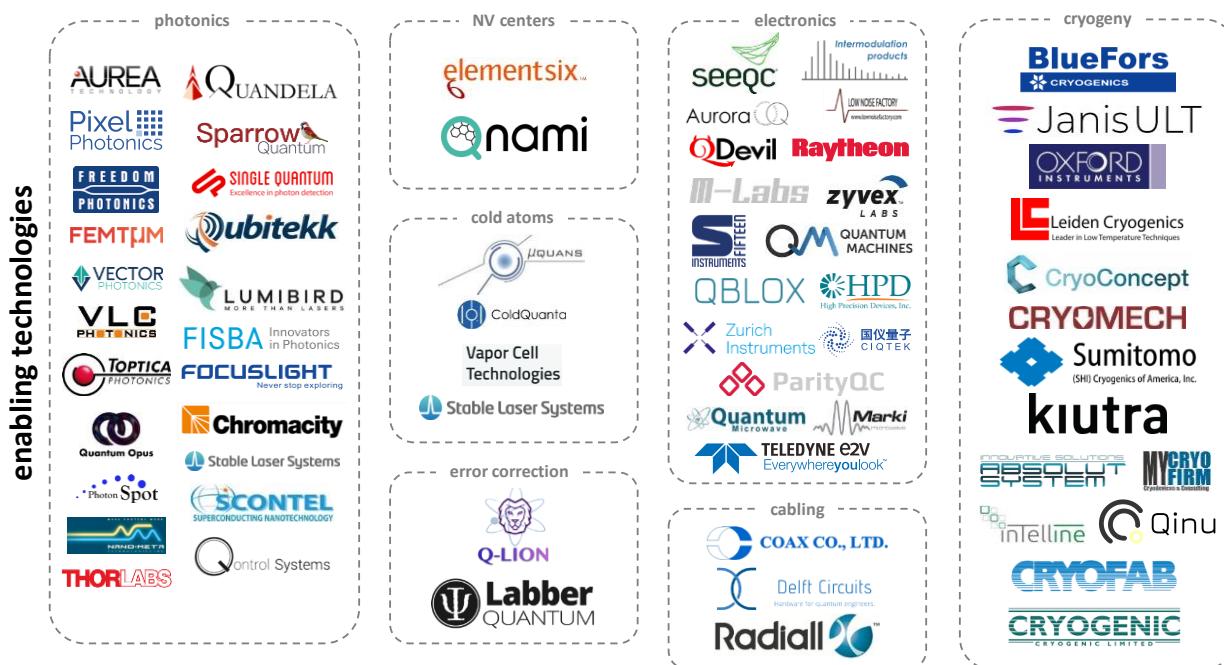
<sup>788</sup> See [High performance quantum computing](#) (7 pages).

<sup>789</sup> See [Why HPE abandoned quantum computing research](#) by Nicole Hemsoth, April 2019.

# Quantum enabling technologies

Building a quantum computer and other second quantum revolution related products involve assembling a lot of various technologies, some being classical and others quantum-related themselves. This part of this ebook is dedicated to these various important enabling technologies. These are “enabling” in a sense that their characteristics and performances frequently have a direct impact on the performance and scalability, particularly with quantum computing. We’ll see this with cryogenics, cabling, classical electronics, lasers and photonics.

We’ll also look at the raw materials needed in quantum technologies, where it comes from, is it rare or not and how is it transformed. At last, we’ll have a look at other unconventional computing technologies. They can both compete and, in some cases, complete quantum computers. Whatever happens, this cooptition is also enabling innovation.



## Cryogenics

Cryogenics is an important enabling technology used with most types of qubits, the most demanding being the very low operating temperatures of superconducting qubits, at 15 mK. Other technologies like photon qubits require lightweight cryogenics operating at 4K to 10K for their photon sources and detectors<sup>790</sup>. Detectors must be cooled to avoid the photon dark count effect, when thermal noise originated photons are detected instead of useful photons.

In this part, we’ll focus on the 15mK dry dilution refrigeration systems used by superconducting qubits. These qubits must be cooled to this low temperature to avoid noise sources from the environment, particularly when compared with the microwave pulses used to control qubits and handle their readout<sup>791</sup>.

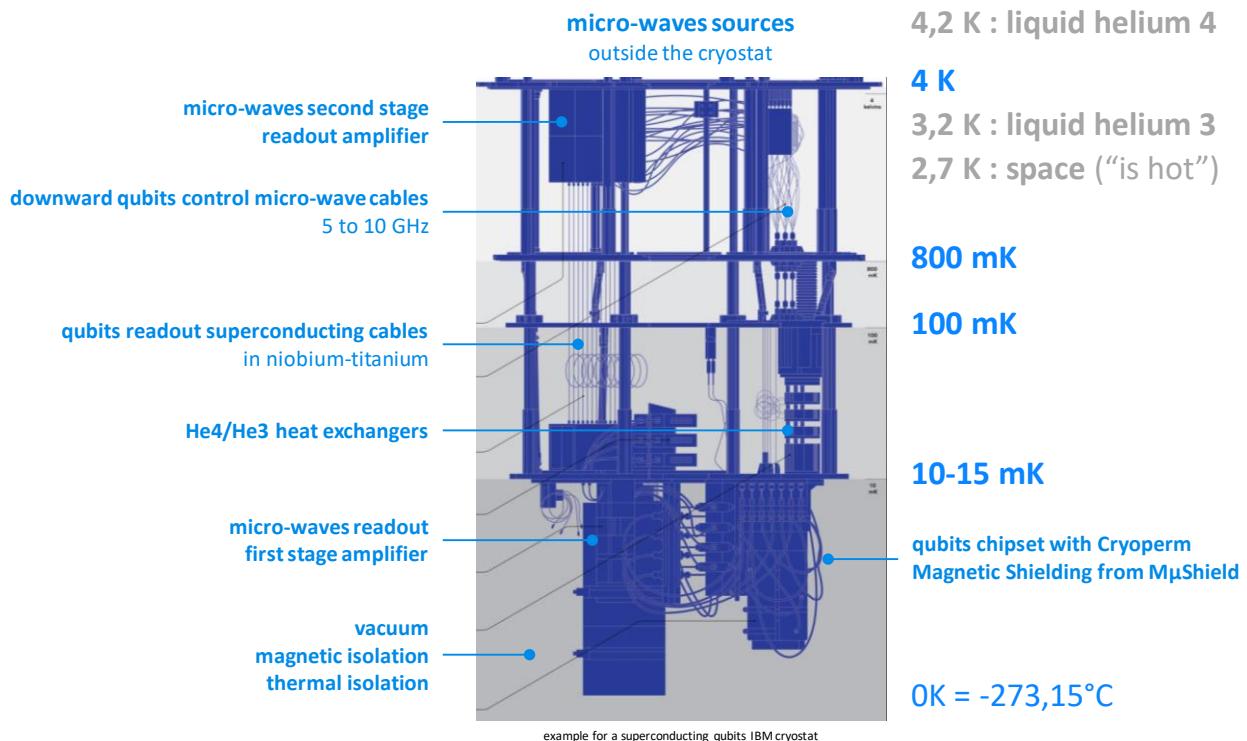
<sup>790</sup> By definition, cryogenics operates below 123K or -150°C. Bearing in mind that -153.15°C is the temperature below which permanent gases, i.e. gases in the ambient air, all condense into liquid at ambient pressure.

<sup>791</sup> It is governed by the equation  $k_B T < \hbar\omega$ . The Boltzmann constant multiplied by the temperature must be inferior to the product of the Dirac constant and the microwaves frequency in Hz. This leads us to adopt a temperature of about 15 mK for superconducting qubits.

These are the most complicated systems and also, those requiring some scalability in cooling power to accommodate the growth in number of physical qubits.

### Wet and dry dilution refrigeration

Superconducting quantum computer from IBM, Google and others are frequently presented with these mysterious gold chandeliers where the processor is housed, surrounded by an unlikely set of wires, devices and several layers of circular plates. This system is a mix of passive and active control electronics reaching the qubits processor and low temperature cooling system<sup>792</sup>. The chipset must be as isolated as possible in terms of temperature, magnetism, vacuum and even mechanical vibrations.



The above diagram is taken from [Quantum Computers Strive to Break Out of the Lab](#), 2018.  
However, legends are from the author.

The refrigerated part of a quantum computer with superconducting qubits or silicon is generally organized in stages, knowing that the lower you go down in the stages, the colder it gets:

- On the upper level, a plate that is not usually seen in diagrams and picture is thermalized at 50K. This is where both the electronic cables for controlling and reading the qubits as well as the fluids used for refrigeration arrive in the cryostat.
- One level below, running at 4K, i.e. 4°C above absolute zero (273.15°C)<sup>793</sup>. That's where sits the lower part of the so-called pulse tube.
- The below plate is at around 800 mK. Between these two floors is the lowest temperature in space, which is 2.7 K and also corresponds to the cosmic background radiation.
- Another plate is generally located at a temperature of 100 mK.

<sup>792</sup> A tour of the IBM Q Lab is available in the 2016 video [A Tour of an IBM Q Lab](#).

<sup>793</sup> The Kelvin scale starts at absolute zero. This temperature where atoms literally no longer move is unreachable. If it were, Heisenberg indeterminacy would be broken! It is approached asymptotically. The lowest temperature record is 450 pK (pico-kelvin), which is reached thanks to Doppler effect laser-based atoms cooling, already described on page 68.

- The lowest stage plate is where the quantum processor sits, and is cooled between 10 and 25mK, usually around 15mK. It is also called the "mixing chamber cold plate". A cold plate is a one-stage copper plate and the mixing chamber is the last level at the bottom of the dilution refrigeration system that we will explore later<sup>794</sup>.

We will now study the detailed characteristics of the very low temperature cryogenics used in these superconducting quantum computers<sup>795</sup>.

It uses a **dilution refrigeration**, which is based on the association of two helium isotopes: helium 4 and helium 3, which have different and complementary physical properties<sup>796</sup>. They have respectively a boiling temperature of 4.2K and 3.2K. Helium 4 is superfluid at 2.17K while helium 3 is superfluid at a much lower temperature of 2.5 mK, at ambient pressure.

The cryostat exploits the combination of three phases: a gaseous  $^3\text{He}$  phase and two liquid phases, one with  $^3\text{He}$  and the other with a mixture of  $^3\text{He}$  and  $^4\text{He}$ , with evaporation of the  $^3\text{He}$  in a mixed chamber<sup>797</sup>.

Let's explain first why helium is so important for low temperature cryogenics. Hydrogen becomes liquid at 20.3K<sup>798</sup>, nitrogen at 77.4K and oxygen at 90.2K. These gases are useless for low temperature cryogenics.

On the other hand,  $^4\text{He}$  liquefies at 4.2K at room temperature and a  $^4\text{He}$  cryostat can reach 1K while  $^3\text{He}$  cryostats can go as low as 300 mK. The mix of  $^4\text{He}$  and  $^3\text{He}$  is used in so called dilution refrigerators reaching 15 mK<sup>799</sup>. Note the low density of  $^4\text{He}$  which is 125g/L at 4.2K. There are two types of dilution refrigerators: "dry" and "wet".

In **wet dilution refrigerators**, a first system cools the enclosure to 4K with liquid  $^4\text{He}$ . A second so-called dilution system uses a mixture of liquid  $^4\text{He}$  and  $^3\text{He}$  with a flow circulating in ducts connecting the metal plates down to less than 15 mK in the bottom stage.

<sup>794</sup> In [Top 5 Trends in Quantum Technologies to Look for in 2020](#) by QuantumXchange, January 2020, we find: "Interestingly, IBM and Google are taking different approaches in the infrastructure of quantum computers. IBM's hardware resembles a chandelier with rings whereas the Google device looks like a chip". Which shows that they did not understand at all that IBM and Google had both a candlestick and a chipset. So they did not explore the hardware architecture of a superconducting quantum computer!

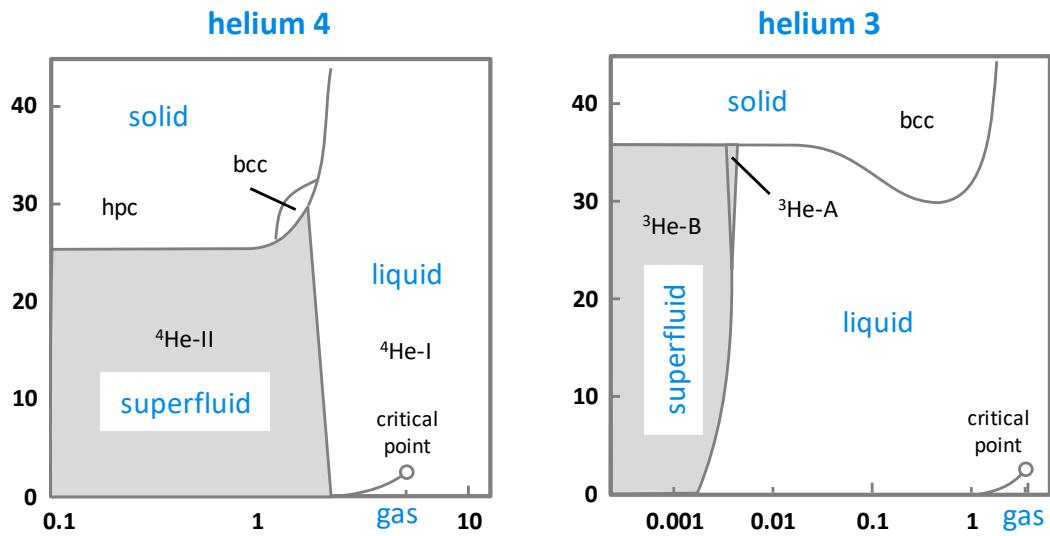
<sup>795</sup> See [Cryostats Design  \$^4\text{He}\$  and  \$^3\text{He}\$  cryostats](#) by Guillaume Donnier-Valentin, CNRS Institut Néel, 2011 (91 slides), [Some Fundamentals of Cryogenic and Module Engineering with regard to SRF Technology](#), Bend Petersen, ESY Cryogenic Group MKS (95 slides) and [Development of Helium-3 Compressors and Integration Test of Closed-Cycle Dilution Refrigerator System](#), 2016 (5 pages).

<sup>796</sup> Helium was discovered indirectly in 1868 through the discovery of an unexplained spectral line in the light spectrum of the sun by astronomers Pierre Jules Janssen (1827-1907, France) and Joseph Norman Lockyer (1836-1920, United Kingdom). It was then isolated for the first time in 1895 by the Scottish chemist William Ramsay (1852-1916).

<sup>797</sup> See the video [Quantum Cooling to \(Near\) Absolute Zero](#) by Andrea Morello of UNSW which explains very well how dilutions work, 2013 (10 minutes). This illustration is inspired from a schema seen in inspired by [Cryostat design below 1K](#) par Viktor Tseplin, October 2018. Bcc means body-centered cubic and hpc, hexagonal close-packed. These are two states of solid helium which are of no interest in dilution refrigerators. A phase diagram shows the phase of the element as a function of temperature (in X in logarithmic scale) and pressure conditions (in Y, 1 bar = atmospheric pressure). It shows that in the regime used below 1K, helium 3 is liquid and helium 4 is superfluid. This difference makes it possible to operate refrigeration at these low temperatures.

<sup>798</sup> Liquid hydrogen cryogenics uses spin variations of hydrogen, instead of isotopic ones.  $\text{H}_2$  molecule exists in two forms, with both hydrogen atoms having the same spin (orthohydrogen) or an opposite spin (parahydrogen). At 300K, the ratio is 75% orthohydrogen and 25% parahydrogen. At low temperature, the ratio is different and the conversion between orthohydrogen and parahydrogen is exothermic, used in the refrigeration process.

<sup>799</sup> The first liquefaction of helium was achieved in 1908 in Leyden, Netherlands, by Kamerlingh Onnes. The dilution cryostat concept was proposed by Heinz London in 1951 and was tested in 1965 at the University of Leiden, when it reached 220 mK. The record temperature went down to 60 mK in 1972 and then to 1.75 mK in 1999.



Inspired by Cryostat design below 1K par Viktor Tsepelin/October 2018.

similarities between  $^4\text{He}$  and  $^3\text{He}$ :

- absence of triple point
- critical point at low temperature
- high-pressure to form solid
- existence of superfluidity

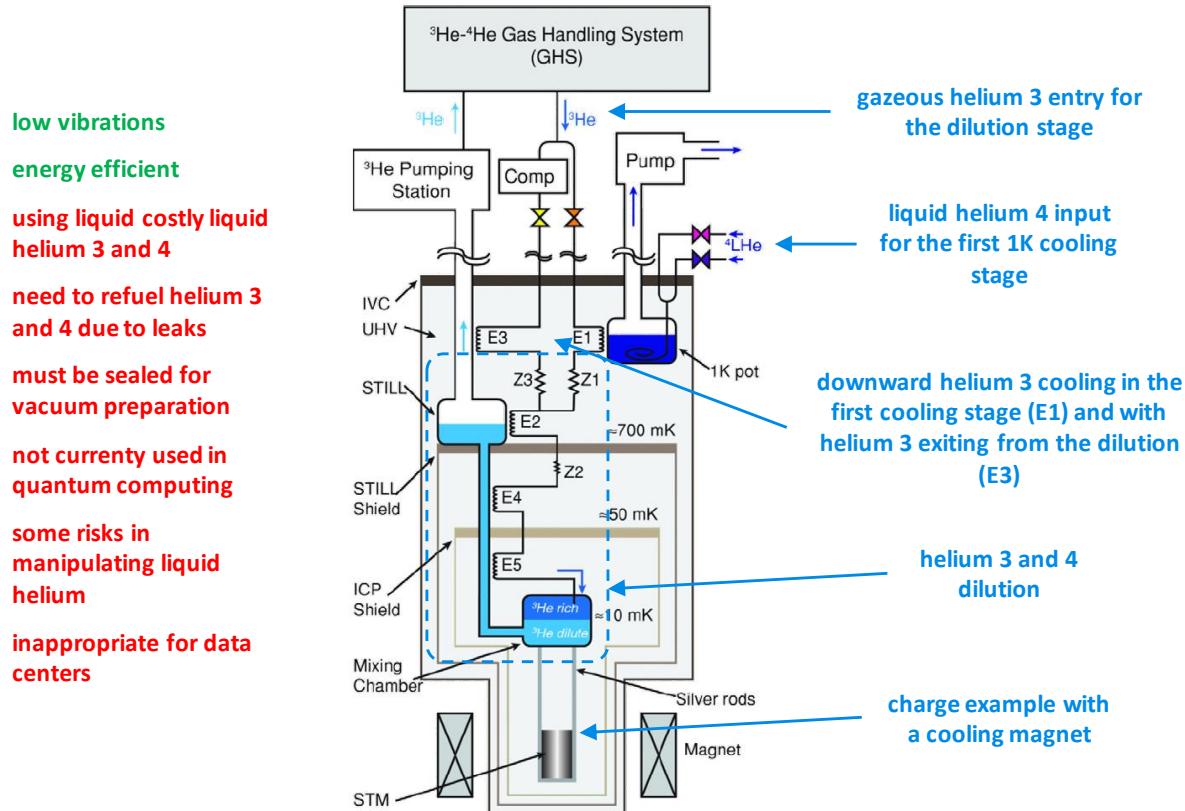
differences between  $^4\text{He}$  and  $^3\text{He}$ :

- different statistics (Boson vs Fermi)
- $^3\text{He}$  has magnetic field dependence
- superfluidity has different origin
- $^3\text{He}$  100x more expensive than  $^4\text{He}$

Wet dilution system was used until the early 2000s. It was then replaced by dry dilution systems that are simpler to operate, especially to create quantum computers that are easy to install at customer sites, thanks to avoiding liquid helium.

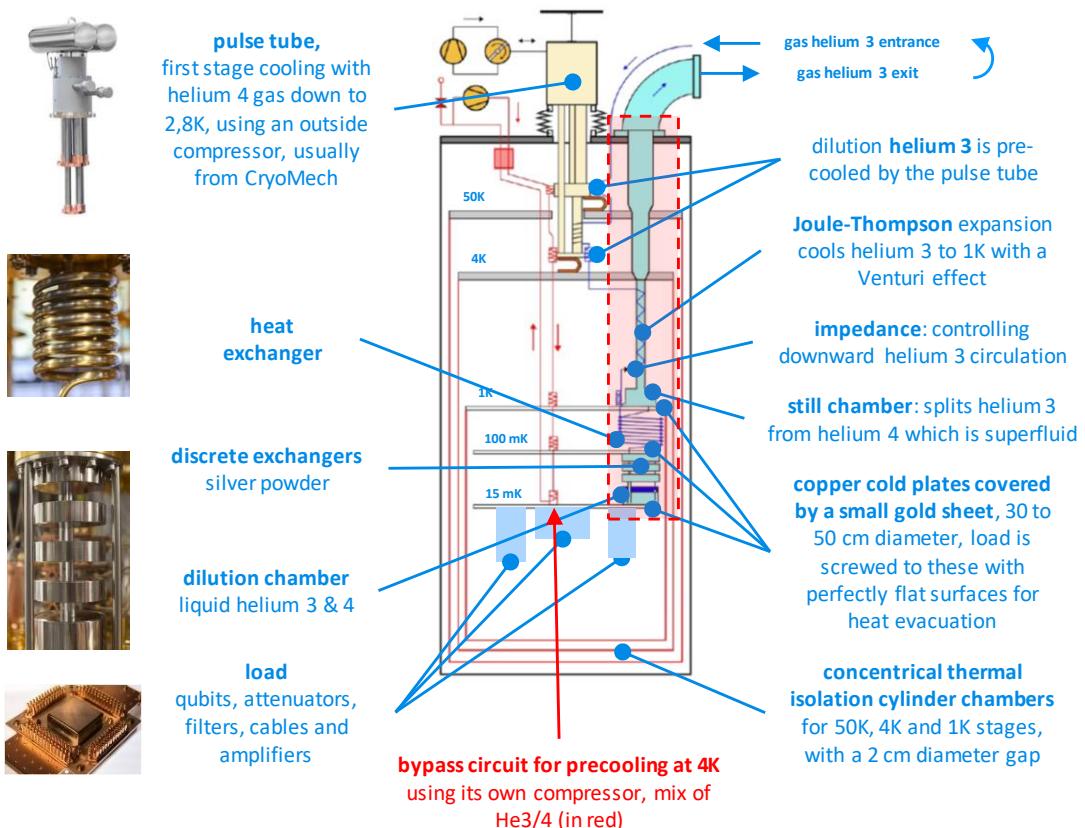
However, wet dilution systems are still used for various physics experiments where the dry system is not appropriate, but not for quantum computing.

## wet dilution refrigeration



**Dry dilution refrigerators** or so-called cryogen-free refrigerators do not use liquid helium. They are using only gaseous helium 3 and 4. Like wet systems, they have two stages: the lower dilution stage is about the same with controlled expansion of helium 3 which is bathed at the bottom in liquid helium 4 in a dilution chamber. This covers cooling to temperatures lower than 1K.

The upper stage relies on the pulsed tube technique that manages cryogenics down to about 2.8K with helium 4 gas and a large external water-cooled compressor. This technique has been mastered for about twenty years and has been progressing incrementally since then. Its arrival coincides with the first experiments with superconducting qubits. Dry dilution refrigerators are generally used for the cryogenics of qubits requiring to go down to less than 1K. The following diagram explains how it works.



schematic inspired from [Cryostat design below 1K](#) by Viktor Tsepelin, October 2018 (61 slides), illustrations from CryoMech documentation, Janis, [Dry dilution refrigerator with 4He-1K-loop](#) by Kurt Uhlig, 2014 (16 pages) and IBM.

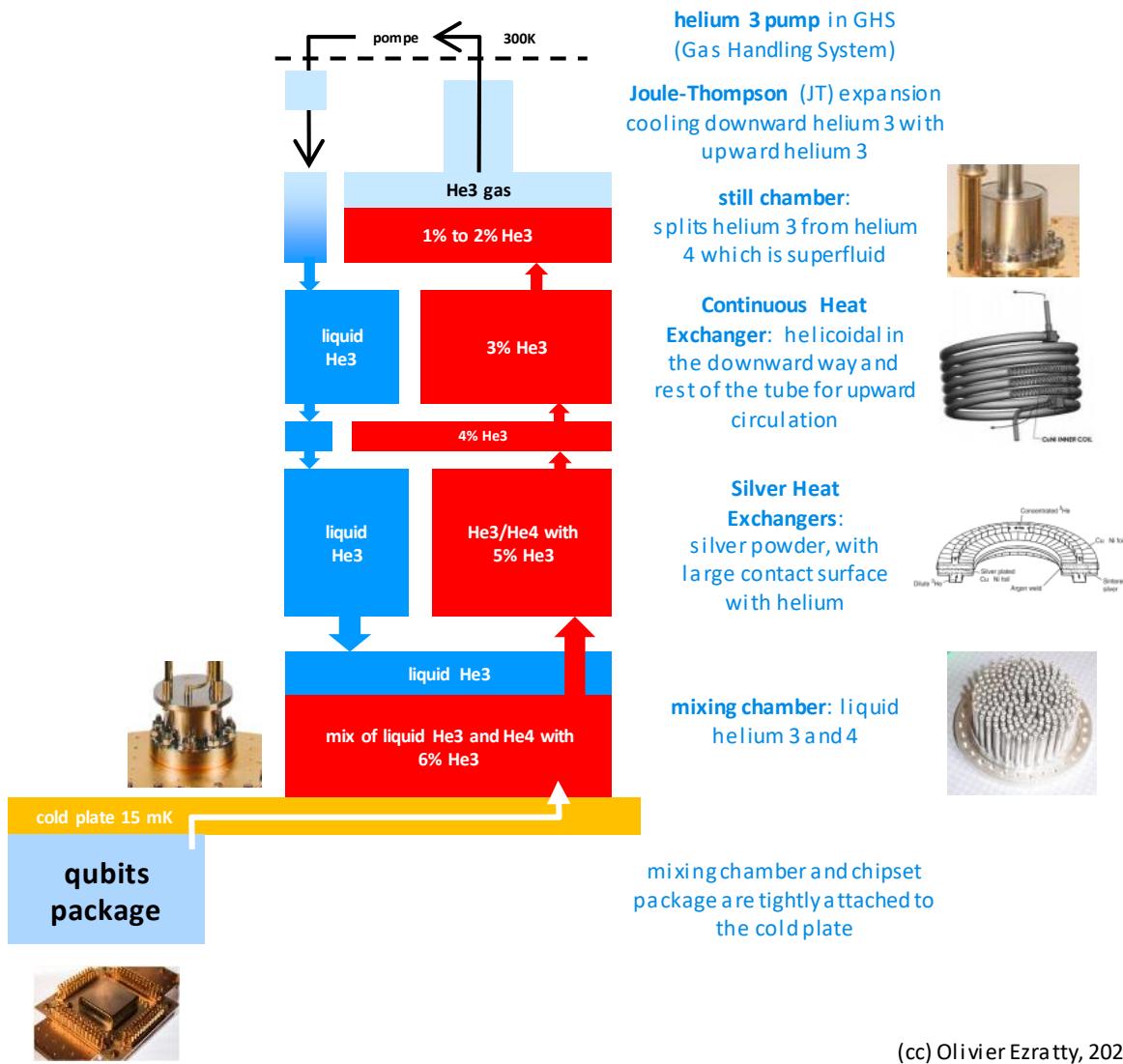
The pulsed tube is associated with a **Stirling** or **Gifford-McMahon** type compression and expansion system. The latter seems to be the most frequently used, particularly at **CryoMech<sup>800</sup>**. It uses a piston. Stirling engines are used to cool infrared devices but not in dilution systems.

It can be seen in the curve on the right that the available cooling power decreases rapidly with temperature. It is currently around 1W at 4K<sup>801</sup>. There are no moving mechanical parts inside the cryostat, both in the pulse tube and in the dilution.

<sup>800</sup> See [Lecture 2.2 Cryocoolers](#), University of Wisconsin (25 slides) which is the source of the schematics used to describe the Stirling and Gifford-McMahon systems.

<sup>801</sup> With larger liquid helium cryogenic installations like Helial SF from Air Liquide, a cooling power of 100W to 1kW can be generated at 4K.

This avoids the generation of unwanted vibrations that could disturb the wiring and the qubits which are very sensitive beasts. The flow of gases and liquids produces very little disturbance in the dilution process.



(cc) Olivier Ezratty, 2021

A refrigeration system is often evaluated in % of the Carnot cycle. This cycle describes a perfect thermodynamic cycle using four perfectly reversible thermodynamic processes involving work-heat exchange<sup>802</sup>. The efficiency of a thermal machine is never perfect with 100% of this cycle.

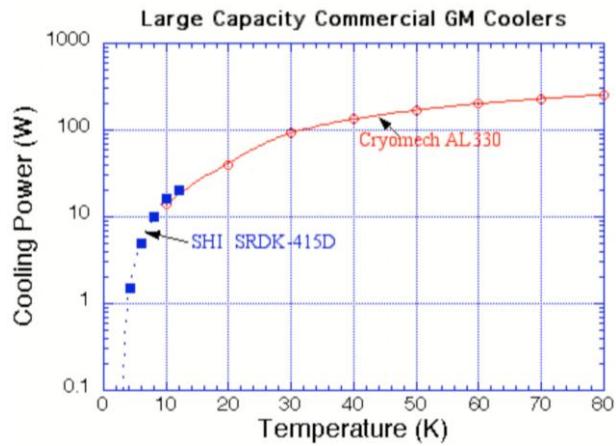
For a pulsed tube, a perfect Carnot efficiency would be about 1.4%, i.e. it would take 70W of energy to extract 1W at 4.2K<sup>803</sup>! In practice, it requires about 10 kW, i.e. 152 times more! We thus obtain a **Carnot efficiency** of less than 1%. That's <1% of 1.4% ! Indeed, we spend more than 10 kW to get 1W of power at 4.2K. So... at 15 mK to get 10  $\mu$ W ? We do not evaluate the efficiency of the 15 mK stage of Carnot because it operates isobarically, i.e. at constant pressure, the thermal cycle being linked to a phase variation of helium 3. This stage is powered by heat exchanges between the pulsed tube and the helium 3 gas circuit.

<sup>802</sup> See Cryogenic Systems by Pete Knudsen, 2018 (71 slides) which describes well the Carnot cycle principle.

<sup>803</sup> See [Lecture 5 Refrigeration & Liquefaction \(Part 1\)](#) by J. G. Weisend II (17 slides).

## Pulse Tube Cryocoolers

- Two general types
  - Stirling type
    - High frequency ~ 60 Hz
    - High efficiency: 25% of Carnot
    - Operation down to 10 K
  - GM type
    - Low frequency ~ 1-2 Hz
    - Split design = very low vibration
    - Ideal for 4 K operation ( $\leq 1$  watt)



There is a circuit, shown in red in the diagram *above*, that is used to pre-cool the cryostat in the thermalization preparation. This is done in three steps: first, by starting the pulse tube which cools the 50K and 4K stages with helium 4 gas and the external compressor of about 12 kW<sup>804</sup> (in yellow in the diagram). Then by using the pre-cooling circuit which will circulate a helium 3 and 4 mixture to the lower stages, and which will have been cooled by the pulse tube, in the circuit in red in the diagram.

Finally, the dilution system takes over from the second one and is launched to be able to go down to 15 mK in the lower cold plate (in light blue in the diagram).

By adopting a rocket analogy, the pulsed tube and its 7 to 12 kW compressor are the equivalent of the first stage of a Saturn V rocket. The pre-cooling system is the analogue of the rocket second stage and the dilution system is the equivalent of the third stage that sends the lunar module and the LEM to the moon, here, the chipset. Extracting the Earth's gravity over a large mass is equivalent to cooling a large metal mass inside the cryostat to 50K and 4K. While the dilution system is responsible for cooling a smaller mass from 4K to 15 mK, the lower cold plate and the payload attached to it.

These systems require optimization with a large number of parameters. The modeling of a cryostat could one day benefit from quantum computation, especially since the fluids used are in a superfluid quantum state.

A good part of the power is used to lower the temperature to 1K, because the mass to be cooled is the most important. The cylinder that protects the part cooled at 4K receives the thermal radiation from the part at 50K. This makes a big thermal difference to absorb.

In a cryostat of about 16 kW, only about one third of this power is used in the dilution system, which is used to lower to 15 mK. It corresponds to the pumps in the GHS, the Gas Handling System, which contains all the pumps and gas circuits outside the cryostat, and to the share of the energy spent in the pulse tube to cool the dilution system.

The dilution system does not use a compressor. The helium 3 circulating outside is just driven by a pump located in the GHS. The reason is that the helium 3 that returns to the cryostat is cooled by the pulse tube. In practice, all the cryostat heat is evacuated by the compressor of the pulse head which is itself cooled by water.

<sup>804</sup> At CryoMech, the compressors adapted to these dilution systems consume from 7.9 to 12kW; from PT410 to PT420. About 4kW must be added for the GHS (Gas Handling System) which manages the dilution circuits with their pumps and controls as well as for the computer and the assembly dashboard.

The diagram *above* details the operation of the dilution system as well as the phase (liquid or gaseous) and the concentration of helium 3 and 4 in each stage and component. It shows the descending circuit of helium 3 which becomes liquid from the condensation at the boiler.

In the circuit going up from the mixing chamber, a liquid mixture of helium 3 and 4 rises and the concentration of helium 3 goes down as the stages go up. It is only in the boiler that helium 3 becomes gaseous. Helium 4 remains liquid and is evacuated downwards. It has moreover a tendency to rise due to superfluidity. A trick is to cut this rising film and send helium 4 back down.

The helium 3 landing in the dilution chamber at the bottom must end up there at a temperature barely above 1mK of the chamber temperature. It is pre-cooled by the helium 3 that is moving upward. The only way to achieve this is to increase the contact surfaces, which is done in the discrete heat exchangers just below the cold plate at the 100 mK level.

These dry cryostats still use a cryogen, liquid nitrogen at 77K, to filter helium gas and remove impurities<sup>805</sup>. This filtration is based on zeolite powder, made of microporous aluminosilicate crystals.

The liquid nitrogen tank used for this pre-cooling is called a "cold trap"<sup>806</sup>. This filtering is completed in the cryostat 4K stage by another filtering system based on activated carbon powder which works better at low temperatures and increases the contact surfaces with the gas to better filter it.

As a general rule, the complete thermalization of a quantum computing cryostat takes about 24 hours. The so-called "1K" stage was actually cooled at about 1.2K in wet cryogenics and is around 800 mK for dry cryogenics. The power consumption is identical between the thermalization phase and the temperature maintenance of the instruments once the thermalization is completed.

Cryogenics at 10-20 mK is specific to quantum computers whose qubits must be cooled at very low temperatures, mainly those based on electrons (superconductors, electron spin, Majorana fermions). Theoretically, silicon qubits should only be cooled down to 1K but for the moment, they are still cooled down to about 15mK. An Australian team created a proof of concept of silicon qubits running even at 1.5K and another one from Intel and Qutech at 1.1K<sup>807</sup>.

To reach **even lower temperatures**, below 3 mK, a complementary technique is used, adiabatic nuclear demagnetization (ADR or Adiabatic Demagnetization Refrigeration)<sup>808</sup>. It is not necessary for quantum computing. This type of refrigeration can be added to a wet or dry dilution cryostat.

The principle consists in using a paramagnetic salt which is magnetized with a strong enough field, of 6 Tesla or more. This will heat the salt. The heat is evacuated via a 4K liquid helium bath. The suppression of the magnetic field cools the salt by expansion.

The process complexity lies in the heating-cooling cycle which can disturb the cooled equipment. It is treated by combining several devices that take turns to smooth the temperature curve of the system. The process has been tried and tested for a long time, but the cooling power available is very low.

---

<sup>805</sup> LN<sub>2</sub> for liquid nitrogen, gaseous nitrogen being a molecule of two nitrogen atoms.

<sup>806</sup> Liquid nitrogen is also sometimes used to pre-cool the metallic structure of the cryostat during the warm-up. This is unrelated to the helium circuit. This can save up to five hours for the cryostat thermalization. But this process is not commonly used for quantum computer cryostats. It is used for precooling heavier payloads for physics experiments using equipment weighing up to several hundred kilograms, including superconducting magnets. This technique is not used for quantum computing.

<sup>807</sup> See [Hot qubits made in Sydney break one of the biggest constraints to practical quantum computers](#) by UNSW, April 2020 related to [Operation of a silicon quantum processor unit cell above one kelvin](#) by Andrew Dzurak et al, April 2020 (in nature) and in February 2019 on Arxiv. The test was performed on 2 qubits with a unit gate reliability rate of 98.6% quite average but in line with what is currently obtained with silicon qubits. See also [Universal quantum logic in hot silicon qubits](#), 2019 (11 pages).

<sup>808</sup> We owe the creation of the process to William Giauque (1895-1982, USA) in 1927. He was awarded the Nobel Prize in Physics in 1949.

# kiutra

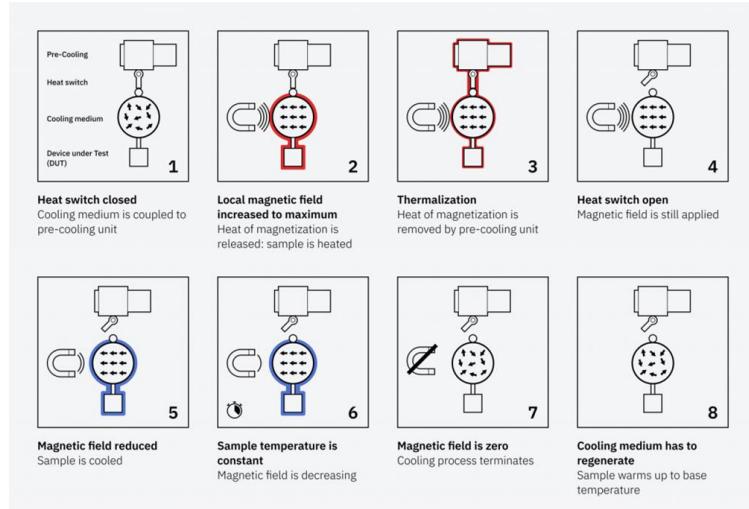
**Kiutra** (2017, Germany) uses this technique to obtain more classical temperatures of a few hundred mK, one of its advantages being that it does not generate vibrations<sup>809</sup>. These temperatures are interesting for cooling silicon qubits.

It is a startup from the TUM (Technical University of Munich) launched by Alexander Regnat. It was seed financed by APEX Ventures and German investors, but the amount is not known.

Their cryostat range goes down to 100 mK (in pulsed mode) or 300 mK (in continuous mode), which is insufficient to cool superconducting Josephson effect quantum computers but could possibly be suitable for electron spin silicon chipsets that can theoretically be satisfied with a temperature of 1K. Their system uses the magnetocaloric effect which was discovered in stages in 1881, 1917 and demonstrated in 1933 to reach a temperature of 250 mK.

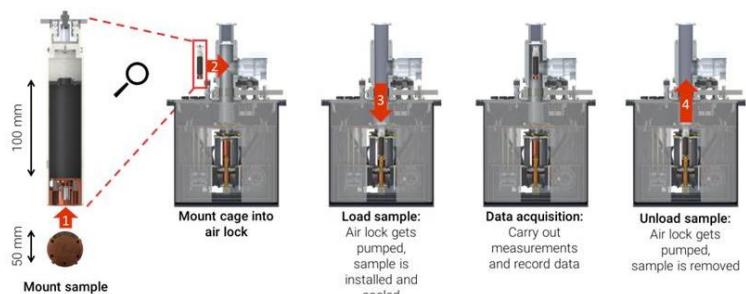
The Kiutra process is based first on this classical effect also called adiabatic demagnetization. It consists in magnetizing a solid material with magnetocaloric properties.

This makes it rise in temperature. This temperature increase is evacuated by a conventional heat transfer fluid, which is not specified. It may be helium 4 if it is a question of going down to a temperature of less than a few Kelvins. Then, the magnetization is stopped which leads the material to cool down.



In order to smooth in time and space this heating/cooling cycle, they combine several cooling units with what they call cADR (continuous Adiabatic Demagnetization Refrigeration)<sup>810</sup>.

The apparatus proposed by Kiutra seems to be mainly designed to cool small samples and does not seem to be yet adapted to the usual architectures of quantum computers with their cooling stages stacked between 4K at the top and 15 mK at the bottom. On the other hand, some dry cryostats can reach temperatures situated between 5 and 10 mK.



They are dedicated to physics experiments unrelated to quantum computing such as the search for dark matter (for the detection of WIMP, Weakly Interacting Massive Particles) and the analysis of cosmic radiation using calorimeters operating between 5 mK and 7 mK<sup>811</sup>.

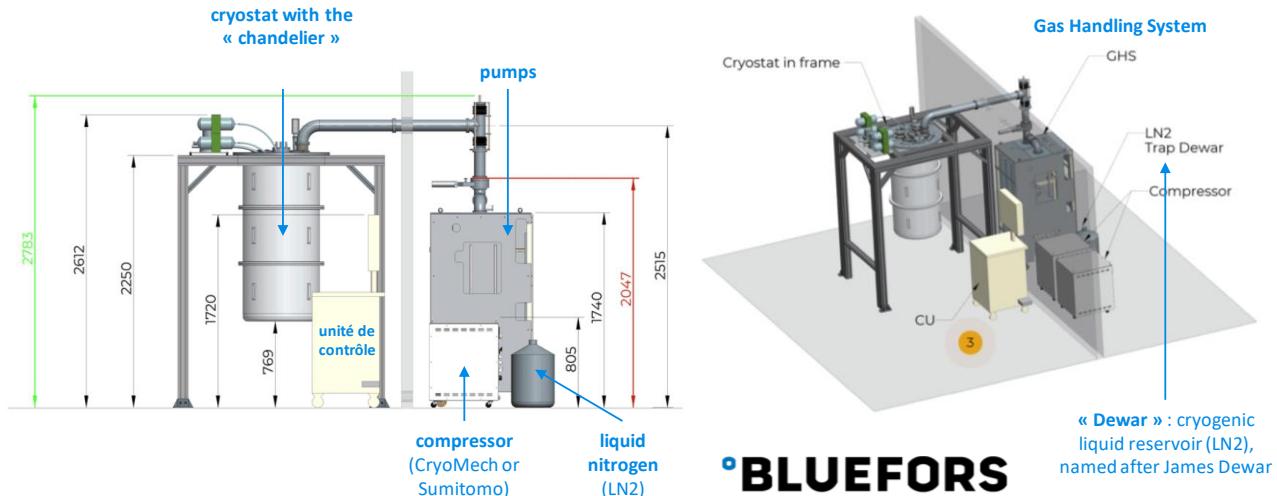
<sup>809</sup> See also [Cryogenic Fluids](#) by Henri Godfrin (now retired), 2011 (50 slides), from Institut Néel in Grenoble, which includes a leading research team on cryogenics. With a record of 100 μK obtained with the DN1 cryostat using nuclear demagnetization.

<sup>810</sup> I discovered in passing that this technique was also being explored at the Institut Polytechnique de Grenoble. See in particular the thesis [Magnetic Refrigeration: Conceptualization, Characterization and Simulation](#) by Morgan Almanza, 2015 (160 pages).

<sup>811</sup> This is the case, for example, of the **CUORE** (Cryogenic Underground Observatory for Rare Events) bolometer installed in Italy. The cryostat comprises five pulse tubes and cools a 750 kg payload of tellurium dioxide to 10 mK. It was looking for signs of beta decay that could prove the existence of Majorana fermions. In the end, it did not find any.

## Dry dilution installation

A dry dilution refrigeration system is divided into two large parts with the compressor, pumps, liquid nitrogen and helium gas reservoirs positioned in one room, and the refrigerated enclosure in another room. This is quite logical since the compressor will generate heat that will have to be dissipated, via an incoming and outgoing water pipe.



With dry dilution refrigerators, the safety constraints are quite light compared to wet versions. Wet dilution uses up to 80 liters of liquid helium which could explode if heated too abruptly because the expansion of the gas is important compared to its liquid state, with a ratio of 1 to 700. It was necessary to handle liquid helium canisters and fill tanks with protective equipment against splashes<sup>812</sup>.

The wet dilution installation below is from CEA-IRIG in Grenoble, which deployed in June 2019 two systems from **BlueFors**. I visited it at the end of June 2019. These systems cost about €1 million each.

The CEA teams installed a device that allows the tested sample to be changed in just 7 hours. Thermalization can thus be planning at night, and in the early morning, the experiments can be resumed.

The phenomena of materials **expansion and compression** are significant at very low temperatures. This has an impact on the design of the whole device and the choice of materials.

The materials that can be used are special steels with nickel, chromium, aluminum, bronze, copper, composite materials, niobium-titanium for wiring, nickel-copper alloys, indium for joints, kapton and mylar for insulation.

The refrigerated system is usually placed in **vacuum**. The management of high vacuum and ultra-high vacuum (Ultra High Vacuum) are industrial specialties. Knowing that cryostats of superconducting and silicon quantum computers only require high vacuum between 5 and 10 mBar. They use commercially available pumps from e.g. **Pfeiffer** (Germany). Pumping only takes place when the system starts up and is deactivated once the system is thermalized at low temperature. Cooling down to 15 mK does not require ultra-vacuum pumping because in practice, at this temperature, all the gases become solid and settle on the walls of the material, generating a very good vacuum.

<sup>812</sup> The oxygen level in the room could also dangerously decrease due to the accidental evaporation of nitrogen or liquid helium. Contact with cryogenic materials, particularly metals, should also be avoided. Rooms must be large enough and care must be taken of in the higher zones in the room where helium can be concentrated since it is lighter than air.



Using too much pumping to generate ultra-high vacuum could propagate dust from these solidified gases, damaging the qubits or the rest of the equipment in the cryostat. Ultra-high vacuum is used for cold atom-based computers.

Thermal leaks are coming from cables entering and leaving the enclosure or radiation. Numerous layers of thermally insulating materials are integrated in the cryostat. They are cylinders stacked upside down like Russian dolls. It is made of aluminum, copper and steel. Each cylinder and plate acts as a thermal insulator vs the lower cylinder.

The quantum chipset is **magnetically isolated** from the outside. Magnetic isolation uses several Russian doll enclosures made of various alloys, including **Mu-metal**, an alloy of nickel, iron and molybdenum, aluminum alloys and other superconducting alloys. The quantum processor can also be magnetically shielded. IBM uses a Cryoperm Magnetic Shielding from **MuShield**.

Apart from this magnetic isolation, cryostats in research laboratories may be supplemented by **superconducting magnet** systems that occupy the lower part of the cryostat cylinder. They have a cylindrical shape that surrounds a measuring instrument. These magnets are also supplied with liquid helium to guarantee the superconducting effect that is used to generate intense magnetic fields of several Teslas.

These fields are used to set up various experiments, particularly in astronomy or fundamental physics. They are sometimes used in quantum computing, especially with silicon qubits for electrons spin control<sup>813</sup>. At D-Wave, the magnetic field is reduced to one nano-Tesla (nT) in the computer enclosure, compared to the Earth's magnetic field, which can reach 65 micro-Teslas, giving us a ratio of 1 to 65,000. D-Wave communicates on a ratio of 1 for 50,000.

---

<sup>813</sup> At CryoConcept, 8 or 14 Tesla magnets can be installed on the 4K stage next to the dilution unit.

The **cold plates** at each stage of the cryostat are generally made of 99.99% pure copper with very low oxygen content to maximize their thermal conductivity<sup>814</sup>. It is covered with a thin a few microns thick layer of gold which serve as a protection against oxidation and radiation. It also has good thermal conductivity and is soft, which is very useful for solidly anchoring and cooling all the attached components.

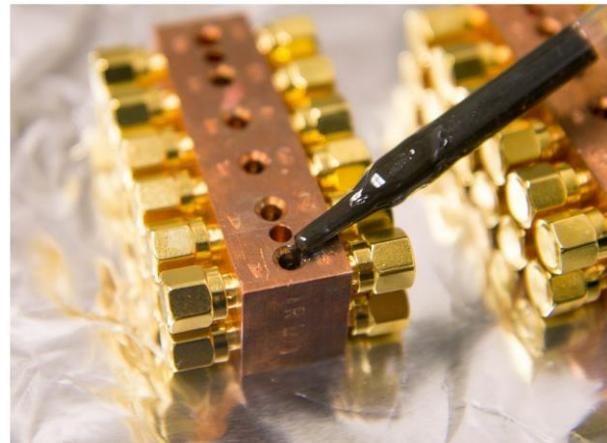
On the right, an example of a BlueFors cryostat cold plate. These plates are custom perforated to allow all the cables to pass through, not including the cryostat components. All the holes must be used to avoid thermal leaks between the bottom and top of these cold plates.

Infrared rays must be prevented from passing from one level to another and generating downward heat leakage.

These plates must be optically totally watertight screens so as not to let a single photon pass through!

The trend is to increase the size of the cold plates, with a diameter reaching 50 cm. Knowing that their size is slightly decreasing from the top to bottom cold plates because of the concentric cylinders shields surrounding them.

In cryostats for quantum computers, the current standard for the bottom plate is 30 cm to 40 cm for research and 50 cm in production, to accommodate more electronic components. It could soon reach 100 cm. Infrared photons are filtered with an **Eccosorb** resin that surrounds the superconducting cables in the lowest stage of the system. This resin is a mixture of epoxy and metal powder. It is injected into copper filters (OFHC) that surround the cables in the coldest stage of the cryostat (*opposite*)<sup>815</sup>. The resin is usually supplied by **Laird Performance Materials (UK)**.



(A) ECCOSORB injection. Inject slowly and at a flat angle such that the liquid creeps onto the edge of the fill opening and into the cavity. Injecting too fast or steep will cause a planar bubble to form which blocks the opening (see Figure 3.8b).

<sup>814</sup> It is OFHC for oxygen-free high thermal conductivity. Source of this information: [Flying Qubit Operations in Superconducting Circuits](#) by Anirudh Narla 2018 (219 pages).

<sup>815</sup> See some explanations of the Eccosorb resin in [Improving Infrared-Blocking Microwave Filters](#) by Graham Norris, 2017 (114 pages) and [Development of Hardware for Scaling Up Superconducting Qubits and Simulation of Quantum Chaos](#) by Michael Fang, 2015 (56 pages).

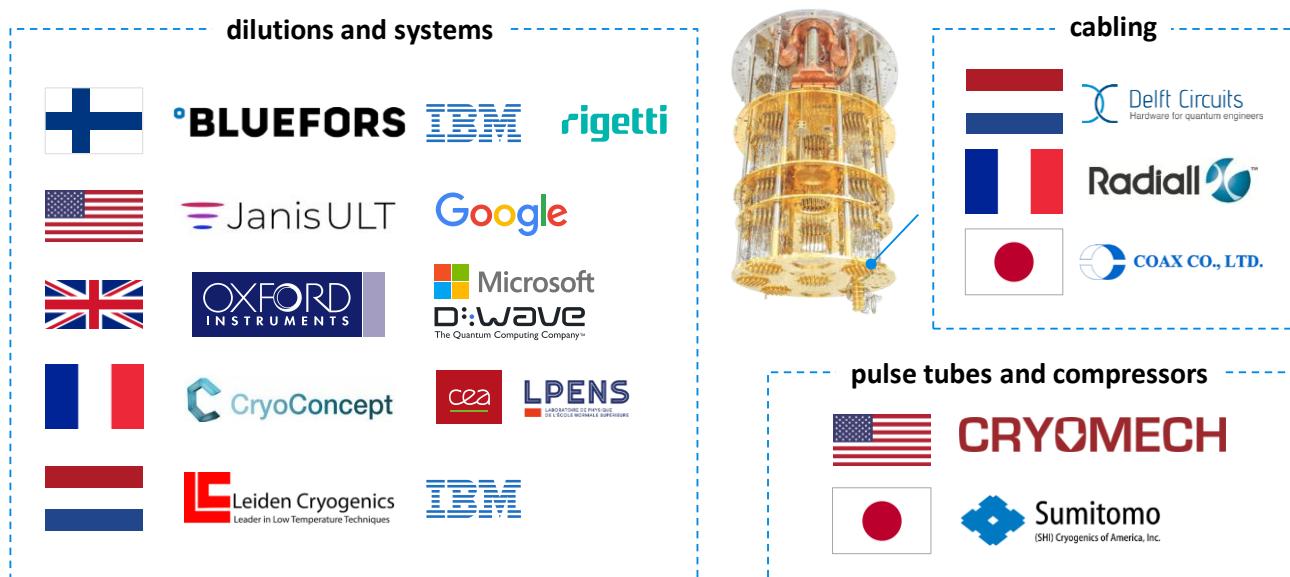
To reach ultra-low temperatures of 1 mK, the **Continuous Nuclear Demagnetisation Refrigerator** technique can also be used, in complement with dry refrigeration<sup>816</sup>. This temperature is required for some physics experiments but not with solid-state based quantum computers (superconducting or electron spin qubits). At such a low temperature, the cooling budget is equally super low, at just 20 nW.

## Cryostats vendors

The main suppliers of cryostats for quantum computers are **BlueFors Cryogenics** (Finland), which equips IBM and Rigetti, **Oxford Instruments** (UK), which is used by D-Wave and Microsoft, **Janis ULT** (USA), used by Google, **Leiden Cryogenics** (Netherlands)<sup>817</sup>, which manufactures the most powerful cryostats on the market, used mainly for physics experiments, and **CryoConcept** (France), a branch of Air Liquide since 2020.

Finally, the world market for cryogenic systems, all categories combined, is expected to be about \$1.8B in 2020<sup>818</sup>.

Let us recall that the science of low temperatures used in quantum computing has benefited from numerous advances from other fields: space and especially space telescopes where a large part of the instruments needs to be cooled such as infrared sensors or bolometers, particle accelerators with their superconducting magnets and finally, medical imaging, especially MRI, which also needs low temperatures to cool its superconducting magnets.



## BlueFors

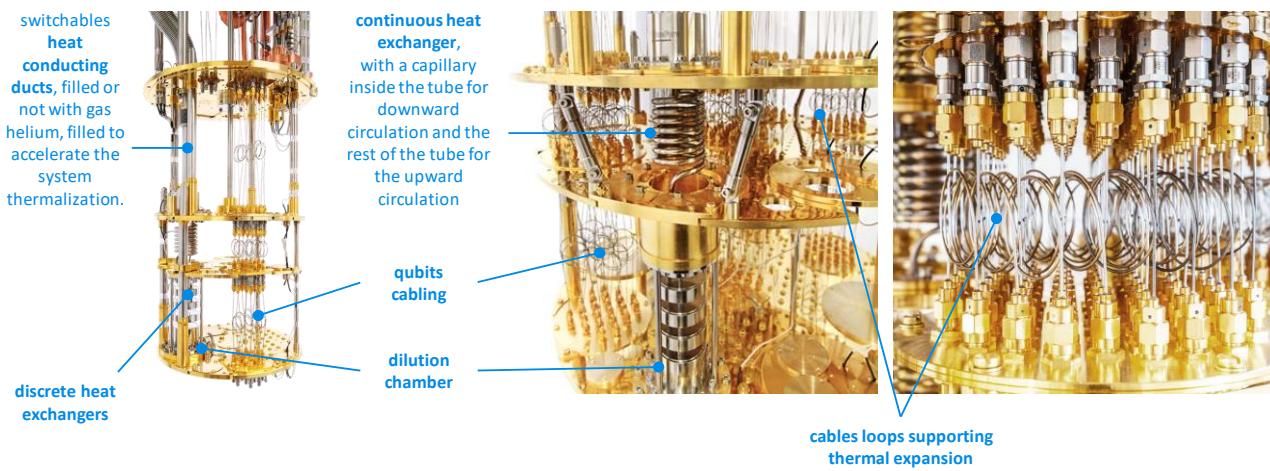
**Bluefors** (2007, Finland) is the worldwide leader of low temperature cryogenic systems, using dry dilution. It's focused on the quantum computing market.

<sup>816</sup> See [Development of a sub-mK Continuous Nuclear Demagnetization Refrigerator](#) by David Schmoranzer, Sébastien Triqueneaux et al, Institut Néel, 2020 (7 pages).

<sup>817</sup> See [Leiden Cryogenics BV](#) brochure (28 pages).

<sup>818</sup> See [Cryocooler Market by Type \(GM, PT, JT, Stirling, and Brayton Cryocoolers\), Services \(Technical Support, Repair, Preventive Maintenance\), Heat Exchanger Type \(Recuperative and Regenerative\), Application, and Geography - Global Forecast to 2022](#), December 2019. This market represented \$1.4B in 2018 and is expected to grow 9.3% annually by 2027. But beware, the market for quantum computers cryostats is a rather small share of this market.

The spin-off from Aato University delivered 600 systems with its 250 employees. It has a broad range of dry dilution systems, with some cabling (coaxial, ribbon, optical) and filters, QDevil X, codeveloped with **QDevil**.



details of a BlueFors cryostat ([source](#)) with custom comments

In March 2021, Bluefors announced a partnership with **Linde** (Germany) to create high-capacity cryogenic systems dedicated to scalable quantum computers. Linde is a gas producer competing with Air Liquide!

They also developed with **Afore** (Finland) a Cryogenic Wafer Prober, a system used for the characterization of 300 mm wafers at 15 mK temperatures. It was acquired by **CEA-Leti** in 2021 to test the quality of their silicon qubits wafers. **Intel** acquired a similar tool as well, for their own silicon qubits development efforts in their D1D fab in Hillsboro, Oregon, USA.



**JanisULT** (1961, USA) was initially Janis, a generalist cryostat manufacturer. In 2020, they sold their 'classical' laboratory cryostats business to Lake Shore.

They kept their ultra-low temperature cryostat business under the brand Janis ULT. They have an offering of wet and dry dilution refrigerators for various use cases, including quantum computing. Their high-end wet dilution refrigerator is the JDry-500-QPro with a 508 mm cold plate and >450  $\mu\text{W}$  of cooling power at 100 mK achieved with a single pulse tube, coming from Sumitomo SHI.

**Oxford Instruments** (1959, UK) is an established British company, listed on the London Stock Exchange since 1999, specializing in scientific instrumentation including cryogenic systems capable of down to 5 mK.

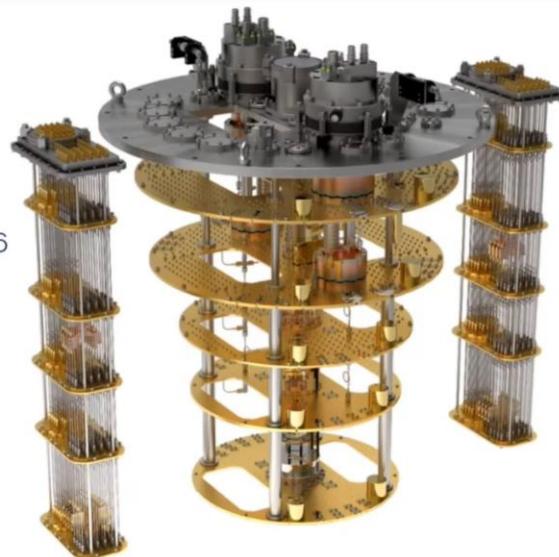
They also provide CCD cameras to detect the state of trapped ion qubits, electron microscopes, vacuum deposition systems, X-ray sources and cameras, and nuclear magnetic resonance spectrographs. The company had acquired VeriCold Technologies (Germany) in 2007 to gain control of pulsed tubes used in the first stage refrigeration for dry dilution cryostats. Their last product is the Proteox, a high-end and flexible dry dilution system with removable cabling.

## ProteoxLX – Maximise experimental capacity



### Enabling the future of Quantum Computing scale-up

- Exceptional capacity for signal lines and cold electronics
  - 530 mm diameter mixing chamber plate
  - Two large Secondary Inserts with 117 mm x 252 mm fully customisable space – up to 256 UT85 SMA lines per system
  - 10 KF50 non line of sight ports for DC wiring
- Highest cooling power system
  - 25  $\mu$ W at 20 mK
  - Twin pulse tubes at 1.5 W or 2.0 W per Pulse Tube Refrigerator (PTR) provide up to 4.0 W cooling power at 4 K
- Low base temperature < 7 mK



In March 2021, they launched the ProteoxLX. It expands the qubits hosting capacity with a larger sample space and coaxial wiring capacity, low vibration and integration of cryo-electronics components. It offers a cooling power of 25  $\mu$ W at 20 mK and 850  $\mu$ W at 100 mK with twin pulse tubes providing up to 4 W cooling power at 4 K.

They also designed a Q-LAN, a cryogenic link that could be used to connect two dilution fridges. The payload can reach 20 kg at 20 mK and 125 kg at 4K.



**CryoConcept** (2014<sup>819</sup>, France, acquired by Air Liquide in July 2020) stands out with cryostats ensuring a very low-level of vibration via their UltraQuiet technology.

They have deployed more than 120 cryostat in 13 countries for various players such as the CEA in Saclay and the ENS<sup>820</sup>. Since 2018, CryoConcept has been collaborating with CEA-Leti to deliver two large cryostats to equip the QuCube project for silicon qubits. They sell worldwide including in the USA, Japan and South-Korea in a market driven by dark matter research and bolometry. The unique low-level of vibrations of their cryostat is related to the absence of mechanical contact between the pulse tube and the cryostat.

<sup>819</sup> CryoConcept was in fact created in 2001 by technology transfer from the CEA where Olivier Guia had worked. The company has had several different owners including French company Segula Technologies and American company CryoMagnetics. Olivier Guia took over the company in 2014. They then reintegrated the in-house R&D and in particular recovered the technological mastery that was at the CEA.

<sup>820</sup> See the quantum equipment of the ENS (Ecole Normale Supérieure, in France) in their [Labtour](#).

By this mean, vibrations are reduced in the range from 1Hz to 1KHz. This absence of vibration is useful to preserve qubits coherence as for cryostats installations containing bolometers that are used to perform physics experiments such as in dark matter research. This experience in bolometry enabled Cryoconcept to develop highly reliable dilution fridges, with systems running for more than one years without interruption. This reliability is a key attribute sought after to operate future quantum data centers.

Historically, CryoConcept started by manufacturing wet cryostats and kept an expertise in this field even though dry systems are now the most commonly manufactured dilutions. Now associated with Air Liquide, CryoConcept is working on coupling helium liquefiers with dilution refrigerators in order to overcome the current cooling power limitation at 4K, thanks to their cryocooler technology and with an increase of the cooling power available at lower level down to 20mK. This will ensure cooling power adapts as the number of qubits in the related quantum processors is growing.



**Leiden Cryogenics** (1992, Netherlands) was founded by Giorgio Frossati and Alex Kamper. The former had been working on dilution refrigeration since the 1970s. Among other things, he invented silver powder heat exchangers.

He started to work at the Centre de Recherche sur les Très Basses Températures in Grenoble, which became the research center on Condensed Matter and Low Temperatures (MCBT) of the Institut Néel of the CNRS. He then became a professor at the University of Leiden in the Netherlands. He designed there a dilution refrigerator reaching a record temperature of 1.85 mK with a cooling power of 25 μW at 10 mK. The heat exchanger technologies he developed were licensed to Oxford Instruments. At last, BlueFors was created by Georgio Frossati's post-docs! What a small world!



**Absolut System** (2010, France) was created by Alain Ravex, former head of the low temperature department of the CEA in Grenoble in the 1980's and 1990's, then a consultant for Air Liquide.

The company develops custom cryostats running at temperatures higher than 1.8K and targets a wide range of applications in research and in the industry, particularly for the production of liquid nitrogen. Their customers include CEA-Leti, Thales and Air Liquide. They are based near Grenoble.

They developed the ACE-Cube (Advanced Cryogenic Equipment), a cryogen free helium cryostat using a remote cooling technique. It is implemented for specific infrared detectors and semiconductors characterization and above 10K.

They also launched AFCryo (2017), a joint subsidiary in New Zealand, with Fabrum Solutions (2004) also based in New Zealand<sup>821</sup>.

**MyCryoFirm** (2013, France) also produces cryostats, but running only down to 3K and therefore, unsuitable for the uses of quantum computing in general. They rather target the field of research in fundamental physics as well as that of quantum sensors.



**Cryomech** (1963, USA) is a supplier of components for cryostats and in particular dry cooling systems comprising a pulsed tubes and a compressor which are integrated in the cryostats of most market players such as BlueFors and CryoConcept.

---

<sup>821</sup> See [Commercial Cryocoolers for use in HTS applications](#) by Christopher Boyle, Hugh Reynolds, Julien Tanchon and Thierry Trollier, 2017 (29 slides).

These pulse tubes and compressors are the first stage of dry dilution refrigeration systems. They use an expansion system of compressed gas outside the cryostat with no rotating parts in the cryostat<sup>822</sup>. The compressor is water-cooled, with a flow rate of 5 to 12 liters per minute depending on the incoming temperature. But this water must also be cooled, and it can require up to an additional 10 kW of electric power unless the computer is located in a cool region.

Their pulse tubes range includes the PT415 and PT420 (*right*). Its main competitor is the SHI Cryogenics Group subsidiary of **Sumitomo** (Japan, *left*)<sup>823</sup>. These compressors are sold combined with their related pulsed tubes.



**High Precision Devices** (1993, USA) develops cryogenic instruments adapted to superconducting quantum computers and in particular sensors. It is very specialized low-level instrumentation. They also develop ADR (Adiabatic Demagnetization Refrigeration) type cryogenic systems. It was acquired by **FormFactor** (1993, USA) in 2020, an advanced SoC and memory probe cards designer for the semiconductor industry.

**Intelline** (2018, Canada) produces customized cryogenic refrigeration systems that are expected to be more affordable than those of its competitors. But they seem to target markets other than quantum computer cryogenics, at least at temperatures below 1K.

**CryoFab** (USA) provides liquid helium containers and related accessories.

**Cryogenic Limited** (1991, UK) provides a various set of cryogenic systems and superconducting magnets. It includes liquid helium systems and ultra-low temperature systems using their own magnet and an off-the-shelf cryostat from Leiden.

**Qinu** (Germany) is a new company selling mK and 4K cryostats. It was created by a former researcher from Institut Néel in Grenoble, which has its own cryostats design laboratory.

<sup>822</sup> These pulsed tubes are used in particular in the semiconductor industry, in vacuum deposition machines (CVD, MOCVD) and plasma deposition machines. They are down to 10K, which is sufficient for semiconductor production.

<sup>823</sup> There are other pulse head and compressor manufacturers such as Fabrum Solutions (New Zealand) but the latter only targets temperatures of 77K for liquid nitrogen production.

One of their added value is to reduce the vibrations coming from the pulse tube. They cover temperatures ranging from 3.2K to 4.9K.

There are many other cryostats and cryogenic devices vendors around but they are less specialized in serving the needs of quantum technologies providers<sup>824</sup>.

### Cooling budgets

The level of cooling power at ultra-low temperature is quite low. This limits the energy that can be released by the qubits themselves and by the microwave attenuation and amplification circuits used to read the state of the qubits. On the right, a comparison of these cooling power budgets by supplier.

	cryostat	pulse tubes	minimum temperature	20mK stage	100mK stage	MC cold plate
°BLUEFORS	LD250	1	10 mK	12 µW	250 µW	30 à 50 cm
	XLD400	2	8 mK	14 µW	450 µW	30 à 50 cm
	XLD1000	2	8 mK	34 µW	1000 µW	30 à 50 cm
JanisULT	JDry-500-QPro	1	7 mK	14 µW	500 µW	50 cm
	TritonXL	2	5 mK	25 µW	1000 µW	43 cm
	TritonXL-Q	2 ou 4	7 mK	25 µW	850 µW	50 cm
CryoConcept	Proteox	1	10 mK	?	500 µW	36 cm
	HD200	1	10 mK	11 µW	350 µW	30 à 50 cm
	HD400	1	10 mK	10 µW	400 µW	30 à 50 cm
Leiden Cryogenics Leader in Low Temperature Techniques	CF2400 Maglev	2	4 mK	?	2000 µW	49 cm
	CF1400 Maglev	2	8 mK	?	1000 µW	49 cm

The **BlueFors**' refrigeration thermal budget ranges from 12 µW (LD250) to 30 µW (XLD1000) at 20 mK, and from 250 µW (LD250) to 1000 µW (XLD1000) at 100 mK.

**Oxford Instruments**' TritonXL also has a thermal budget of 1000 µW at 100 mK but with two pulsed tubes, while the new Proteox reaches 500 µW ... with only one pulsed tube. It is completed by a removable system for qubit control cables supporting up to 140<sup>825</sup>.

The **Janis** JDry-500-QPro has a thermal budget of 14 µW at 20 mK and 450 µW at 100 mK (*above, in-house compilation*).

The current record can be found at **Leiden Cryogenics** with a recent cryostat with a thermal budget of 2000 µW on the 100 mK stage, but the budget at 20 mK is not indicated in their literature. On the 4K stage, the available thermal budget is around 1W. But beware, these extreme performances above 500 µW are often obtained with two pulsed tubes instead of one and thus, double the external compressor and power drain. All this with a double dilution refrigeration system to go below 1K. It is also possible to have systems with a single pulse tube and two dry dilution systems.

<sup>824</sup> See [61 Ice Hot Companies Transforming The Cryogenics & Alternative Cooling Systems Industries](#), January 2021.

<sup>825</sup> See the very interesting presentation [50 years of dilution refrigeration](#), by Graham Batey of Oxford Instruments, 2015 (26 slides).

The thermal budget of the coldest stage is conditioned by the equation:  $Q_m = 84\dot{n}_3 T^2$  where  $Q_m$  is the cooling power in W,  $\dot{n}_3$  is the flow velocity in mol/s of helium 3 in the cryostat at this stage and  $T$  is the temperature of the stage in Kelvin. This law that can be simply called "Q=84NT<sup>2</sup>" explains that the thermal budget at 15 mK is very low compared to the cooling budget available at the upper stages (up to 25 μW at 15 mK, 1 mW at 100 mK and 1.5W at 4K).

There is another constraint related to the Kapitsa resistance. It limits heat exchanges between helium 3 and the heat exchanger. These exchanges are proportional to  $T^4$ . If we therefore want to multiply heat exchanges by 10, the exchange surfaces in the lower parts of the dilution system would have to be multiplied by 10,000! This is done with using silver powders integrated into the discrete heat exchangers above the dilution chamber. These powders are structured to maximize the heat exchange surface area with the helium gas flowing through them. Their deposition process must maximize the flat contact surface with the small tanks where they are located.

### Other cryogenics

For the other types of qubits, the cooling requirements are different: trapped-ion qubits are not theoretically refrigerated, but Honeywell's prototype ion trapped processors announced in early March 2020 are cooled to 12.6K, a temperature that can be obtained with helium 4 based cryostats.

In photon-based quantum processors, the optical components traversed by the photons (mirrors, prisms, interferometers, whether miniaturized in nanophotonics or not) are not refrigerated, but the photon sources and photon detectors are, at temperatures between 1K and 10K. The associated cryogenics is much lighter and consumes less energy compared to dilution cryostats.

Other techniques allow very localized cooling. This is the case of the **Doppler effect** which works on cold atoms suspended in a vacuum. Another solution developed by researchers from the VTT Technical Research Centre in Finland would cool silicon components with a phonon-based electronic cooling technique. It seems that this cooling's capacity is very low, very localized, and still requires pre-cooling the system to at least 244 mK. It is therefore still necessary to operate a helium 3 and 4 dilution cryostat<sup>826</sup>.

On the other hand, quantum technologies also use **other forms of cryostats** than those presented here for quantum computing. For example, Thales' NV centers-based quantum sensors use miniaturized cooling using liquid nitrogen and occupying only half a cubic decimeter<sup>827</sup>. The required temperature is lower, around 70K. That's hot compared to 15 mK!



### Cabling and filters

In current quantum systems based on superconducting qubits, copper coaxial cables carry **microwave photons** at frequencies between 5 and 10 GHz to act on the qubits (reset and quantum gates).

---

<sup>826</sup> See [Thermionic junction devices utilizing phonon blocking](#) by Emma Mykkänen et al, 2020 (9 pages). It reads: "The cooling power for this sample is about 2 pW/μm<sup>2</sup> at 300 mK". "Our best-performing sample is S2 (subchip with 1-mm diameter and 0.4-mm height). Its maximal absolute and relative temperature reductions are 83 mK (at 244 mK) and 40% (at 170 mK), respectively". Therefore, it is already necessary to reach 244 mK before starting, and it is therefore necessary to use a helium 3 and 4 cryostat.

<sup>827</sup> Image source: [Closed Cycle Refrigerator](#) by John Wilde, 2018 (11 slides). These are usually systems using a Stirling engine. Thales Cryogenics produces such miniaturized refrigeration systems. The [RM2](#) cools a payload to 77K for a mass of 275g and a thermal budget of 400 mW at this temperature. It is notably used for cooling infrared cameras in embedded systems. This type of small cryostats can also be found at SunPower (USA), capable of cooling down to 40K and with a larger mass of 1.2 kg. Ricor (1967, USA) is another manufacturer of this kind of mini-cryostats.

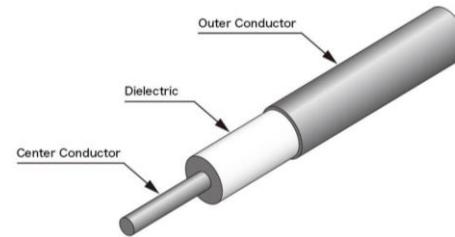
Microwaves are generated by devices generally located outside the refrigerated enclosure. Frequencies below 5 GHz and above 10 GHz are filtered out. These microwaves are also attenuated and filtered at the input on the 4K cold plate. An attenuation of 60db, carried out in three steps of 20 db which each time divide by 100 the transmitted power. It is used to limit the thermal noise that is conveyed in the cables. It is reduced so as not to represent by more than one thousandth of the photons that end up in the qubits. Each filter absorbs energy that must be dissipated at the stages where they are placed.

The thermal conductivity of a cable Q is calculated as follows, using the product of the cable conductivity k, its cross-section A, the temperature gradient T<sub>2</sub>-T<sub>1</sub> and L the length of the cable.

$$Q = kA \frac{T_2 - T_1}{L}$$

**Coaxial superconducting cables** - having theoretically zero resistance at low temperature - connect the qubits to their reading system (thus, in the upward direction in the diagrams). They are made of niobium and titanium alloy (NbTi). They include loops to absorb the metal contraction that occurs during cooling<sup>828</sup>. Their signal is amplified before leaving the cryostat.

These cables come from various vendors including **Coax Co** (Japan). This company is the only one in the world able to produce NbTi cables<sup>829</sup>. The 2 mm diameter cable consists of a conductive outer jacket and a central conductor, both made of niobium-titanium ([source](#)) which are separated by a Teflon (PTE) or Kapton insulation.

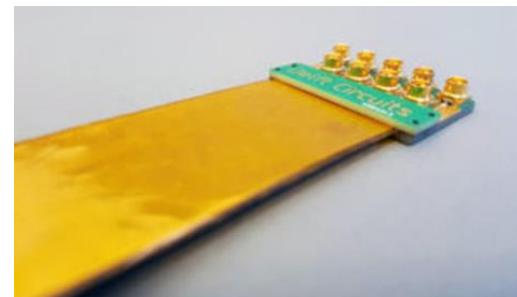


Other vendors like Delft Circuits are also proposing superconducting cables but they seem to rely on CoaxCo for the base cables they're then integrating in their own solutions.



**Delft Circuits** (2016, The Netherlands) provides various superconducting components that can be used in Josephson superconducting quantum computers.

In particular, they offer cables and flexible mats used to carry the control microwaves of superconducting qubits such as CF3 (Cri/oFlex, *opposite*) and supporting frequencies ranging from 2 to 40 GHz with 8 embedded cables.



**Radiall** (France) is an industry company specialized in connectors and cabling, very active in the aerospace vertical. They are now addressing quantum technologies needs.

<sup>828</sup> See [Challenges in Scaling-up the Control Interface of a Quantum Computer](#) by D. J. Reilly of Microsoft, December 2019 (6 pages) which states that superconducting cables have resistance and capacitance when microwaves are passed through them and therefore have a thermal release that must be taken into account.

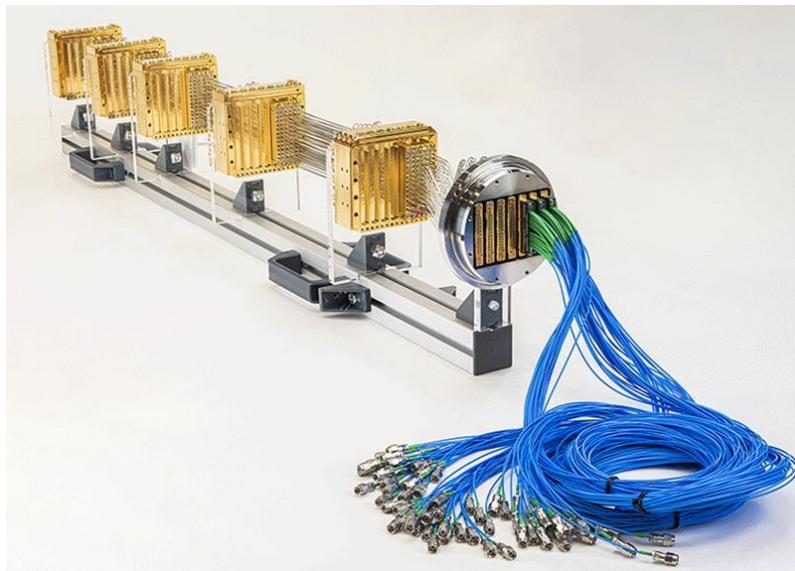
<sup>829</sup> See [We'd have more quantum computers if it weren't so hard to find the damn cables](#), by Martin Giles, January 2019.



They developed special very low magnetism coaxial connectors for D-Wave and cryogenic multiport switches working at 18 GHz for CQT (Singapore). They work on optical connectors and optoelectronic couplers and sell nickel-tantalum attenuators. They also collaborate with various other research labs like Institut Néel in Grenoble.

Microwave qubit control downlink cables are made of various materials including copper-nickel, copper-beryllium or bronze alloys. After passing through the 4K stage, they are replaced by superconducting versions to limit their heat conduction. Between the two, 20 dB attenuators are inserted. In addition, conventional twisted pair cables carrying direct current are used to power the active electronic components integrated in the cryostat, in particular the qubit state readout amplifiers.

This creates significant **wiring clutter**. The picture *below on the right* shows a Google cryostat with its bunch of cables and wires connecting the different cold plates. This is the wiring for only 53 qubits (actually, you need to add the 88 coupling qubits). It seems that it is possible to miniaturize some of this, especially with flat ribbon cables.



These various cables have another disadvantage: they are very expensive. The unit is several thousand dollars. For today's 53-qubit superconducting quantum computer, this cabling costs more than the entire cryostat, more than half a million dollars. This explains why cryostat manufacturers such as **Bluefors** also offer their own optimized cabling system, such as their 168-cable High-Density Wiring, which appears to be sized to support 56 qubits. This allows more value per machine to be sold! The same is true with the removable cable system of the recent Proteox from **Oxford Instruments**.



**QDevil** (2016, Denmark, 1M€) sells filters used in cryostats including the QFilter, based on a collaboration between Harvard University and the University of Copenhagen. It's a cryogenic filter reducing electron temperatures below 100 mK.

They also sell the QDAC, a 24-channel low noise DAC, the QBoard, a PCB-based fast-exchange cryogenic chip carrier system, and the QBox, a 24-channel breakout box. They are partnering with Bluefors.



**Atem** (1990, France) is a coaxial cables designer and manufacturer. It wants to enter the quantum computers space with its Qryolink project to propose superconducting coaxial cables.

# Qubits control and readout electronics

Most of the times, driving qubits with quantum gates requires sending them some sort of photons. For superconducting qubits and electron spin qubits, these photons are in the microwave spectrum. In a counterintuitive fashion, these microwaves are transmitted in coaxial cables and not over the air like radio waves. This is due to their frequencies, between 4 and 8 GHz for superconducting qubits and between 18 and 26 GHz for electron spin qubits.

These are in between higher-frequencies photons that can be transmitted in optical fiber and lower frequencies signals which are transmitted as classical electrical current in wires. We'll look into two sorts of microwave generation technologies: those coming from room temperature electronics and those generated within the cryostat at cryogenic temperature, including cryo-CMOS, superconducting electronics and other discrete electronic components working at these low temperatures.

Direct current signals are also used to drive qubits, like with Z gates with some superconducting qubits and to drive some amplifiers<sup>830</sup>.

	Microwave Control	Baseband Control
Superconducting (Transmon)	1Q XY gates, 2Q gates Carrier: 4-8 GHz Pulse duration: 10-30 ns $\pi$ -pulse Pav: -80 to -60 dBm Shaped envelope	1Q Z gates, 2Q gates 0.01-1mA static/pulsed Pulse Duration: 10-500 ns Resolution: ~nA
Semiconductor Spin	Single spin Q: 1Q XY gates Carrier: 0.1-50 GHz Pulse duration: 10 ns to 1 $\mu$ s $\pi$ -pulse Pav: -60 to +0 dBm Shaped envelope	Single spin Q: 2Q gates S-T Q: XY gates, 2Q gates E-O Q: XY gates, 2Q gates $\mu$ V-mV level signals Pulse Duration: ns-ms 1 ns rise/fall
Trapped Ion	1Q XY & Z gates, 2Q gates Carrier: 5-20 MHz, 1-12.6 GHz Pulse duration: 1-500 $\mu$ s $\pi$ -pulse Pav: 0 to 45 dBm Rectangular envelope	Qubit state control typically not performed at baseband

**FIGURE 11.** Summary of microwave/baseband control requirements for each of the qubit technologies. Abbreviations: Q—qubit,  $P_{av}$ —available power at qubit drive port.

## Room temperature electronics

This field is covered by industry vendors addressing research and commercial quantum computing markets. Beforehand, many quantum computing research laboratories were relying on generic microwave generator and readout systems coming from electronics vendors like **Rohde & Schwarz** and **Tektronix**. And large shops like **Google** developed their own electronics.



**Zurich Instruments** (2008, Switzerland, \$112K) is a manufacturer of electronic test and measurement equipment, including a range of microwave generation and analysis tools. The company was acquired by Rohde & Schwarz in July 2021.

Their offer is built around their Quantum Computing Control System, which bridges the gap between the quantum computer software control tools and the associated electronic instrumentation. This system consists of several components.

<sup>830</sup> This excellent review paper [Microwaves in Quantum Computing](#) by Joseph Bardin et al, January 2021 (25 pages) provides an excellent overview of the challenges of microwave based qubit controls for superconducting, electron spin and trapped-ions qubits. The table/chart in this page comes from this document. Z gates are driven by direct currents with Google's Sycamore qubits while IBM's are driven by microwaves, like the XY gates. See also [Engineering cryogenic setups for 100-qubit scale superconducting circuit systems](#) by S. Krinner et al, 2019 (29 pages) which makes a good inventory of energy consumption sources in the cryostat.

First, the PQSC (Programmable Quantum System Controller, *below top left*) which is used to program and control all the devices. It is equipped with a Xilinx UltraScale+ FPGA that can be driven by the LabOne software using Python, C, MATLAB, LabVIEW and Microsoft's .NET framework. It controls up to 18 HDAWG (High-Density Arbitrary Waveform Generator, *below in blue*) microwave generators and manages up to a hundred qubits. These are sold at 23K€. These generators create microwave pulses that combine a waveform (Gaussian or other, *below right*) modulated by a high-frequency signal, usually between 5 and 10 GHz, adapted to superconducting qubits drive and readout (result *below right*). It can control up to 8 channels.

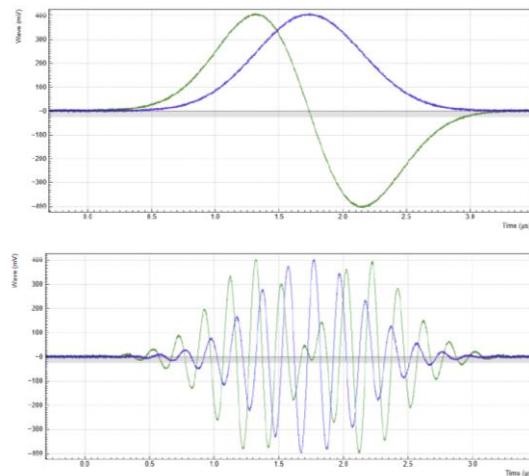
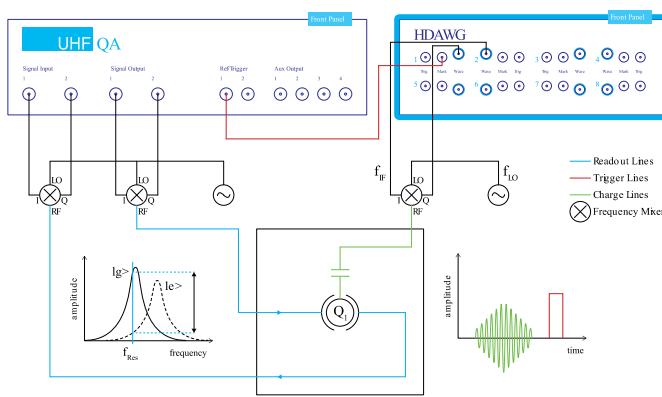


Figure 3.15. Dual-channel signal generated by the AWG and captured by the scope. The top figure shows two envelope waveforms played without modulation, the bottom figure shows the same envelope waveforms played with enabled modulation.

These microwaves are sent to the qubits to reset them to zero, activate quantum gates or handle state readout. The single-qubit quantum gates are generated by sending a modulated microwave that modifies the energy level of the qubits and change its state.



This is complemented by the UHFQA (Ultra-High Frequency Quantum Analyzer) which can analyze the readout state of 10 qubits. In the diagram,  $F_{\text{LO}}$  is the frequency of the microwave signal to be modulated and  $F_{\text{IF}}$  is the modulation waveform.

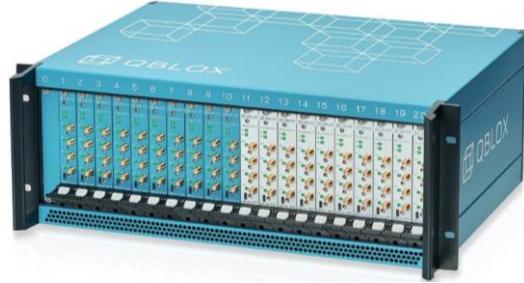
On the UHFQA side, the system detects the modulation or phase modification of the signal recovered through a resonator associated with the qubits,  $l_g$  and  $l_e$  respectively for ground states and excited states.

In April 2021, Zurich Instruments launched a new signal generator, the SHFSG with better micro-waves signal spectral purity and stability. It can handle up to 144 qubit control channels and is accommodated with 4 or 8 channels, controlling up to 8 qubits.

# QBLOX

**Qblox** (2018, Netherlands, \$5M) is a spin-off from QuTech that develops scalable control electronics for superconducting qubits. Their latest generation controls up to 20 qubits with a 4U rackable system.

It consumes about 1 kW. The device contains both micro-wave generators for qubits gates (QCM module, blue) and qubits readout and electronics for qubit readout (QRM module, white). Each unit relies on small custom FPGAs. In a classical manner, it creates waveforms mixed with a microwave carrier signal after DAC conversion. Readout uses an ADC and a phase detection system.



Their DACs/ADCs have a high sampling rate of 16 bits. A high sampling rate is important to create precise waveform microwaves. This precision is a way to ensure a good fidelity for qubit gates generated by these generated microwave pulses.

Their architecture could scale up to controlling 1000 superconducting qubits. Calibration is done with the help from **Orange Quantum Systems** and cabling comes from **Delft Circuits**, two other spin-offs of Qutech in the Netherlands.

The company was [distinguished](#) at CES 2021 by being nominated in the innovation awards of the show, taking place entirely in virtual mode in January 2021.



**Quantum Machines** (2018, Israel, \$73M) provides a qubit control layer for superconducting quantum computers that combines hardware and software<sup>831</sup>. It is a spin-off from the Braun Center for Submicron Research Laboratory at the Weizmann Institute.

They developed their own classic qubit control processor, an FPGA operating at room temperature, which generates the pulses for controlling qubits and measuring their states either with microwaves and lasers<sup>832</sup>. It supports superconducting, electron spin, NV centers, trapped ions and cold atoms qubits.



They already have more than a dozen clients, including, in France, ENS Paris, ENS Lyon, Alice&Bob and Pasqal. Their co-founder and CEO Itamar Sivan did a Master's degree at the ENS between 2009 and 2011. They also partner with Q-CTRL which develops qubits firmware level control software. Their processor is integrated into their "Quantum Orchestration Platform", which also combines a software layer<sup>833</sup>. In June 2020, they announced the creation of the **QUA** language, positioned as a language for creating hybrid quantum and classical algorithms, such as VQE and QAOA, which need rapid feedback between classical and quantum processors. This programming language works with all types of qubits, superconductors, silicon, cold atoms and trapped ions. The compiler thus takes into account the differences in the implementation of qubits: their connectivity, the homogeneity or heterogeneity of their coupling, the coherence times, the error rates, etc.

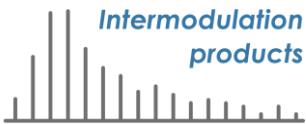


**CIQTEK** (2016, China, \$15M) develops high-precision pulse generator (ASG) and arbitrary waveform generator (AWG) used in qubits control. They also manufacture NV centers-based magnetometers.

<sup>831</sup> See [The Story of the First Israeli Quantum Computing Startup](#) by Eliran Rubin, December 2018.

<sup>832</sup> See the video [MLQ2021 Session Th2: Quantum Machines](#), March 2021 (46 mn) explaining their process.

<sup>833</sup> See [Quantum Machines raises \\$17.5M for its Quantum Orchestration Platform](#) by Frederic Lardinois, March 2020, [Israel gets ready to join global quantum computing race](#) by Amitai Ziv, December 2019 and [The quantum computer is about to change the world. Three Israelis are leading the revolution](#) by Oded Carmeli, February 2020.



**Intermodulation Products** (2018, Sweden) is a spin-off company of KTH, the Royal Swedish Institute of Technology. They market Viva ce, a microwave generator in the 4 GHz band used to drive superconducting qubits.

**Quaxys** (2020, USA) provides hardware and software solutions for superconducting and spin qubits electronic control, including Quantuware 4840, a compact qubit control and measurement unit.

**Low Noise Factory** (2005, Sweden) designs and produces low-noise amplifiers operating at ambient or cryogenic temperatures as well as circulators. They are part of the European OpenSuperQ project, led by the University of Saarlandes in Germany, to create quantum computers based on superconducting qubits.

**Teledyne E2V** (USA/UK/France) is a designer, manufacturer and provider of DACs and ADCs circuits used for microwave processing with superconducting qubits, noticeably with IBM. These are designed and manufactured near Grenoble, France.

We can also mention a Chinese project, a superconducting microwave generator for the control of superconducting qubits based on a Xilinx FPGA<sup>834</sup>.

## Cryo-electronics

Cryo-electronics sit inside the cryostat, control the qubits and manage their readout in place of the external electronic devices we're just covered, totally or partially depending on the systems generation. Many research team and industry vendors are working on this strategic set of technologies which are some of the key gatekeepers of qubits scalability. We have among others the **University of Sidney**, **TU Delft** in the Netherlands, **VTT** in Sweden, **CEA-Leti** and **CNRS Institut Néel** in France and US vendors like **Intel** and **SeeQC**.

Cryo-electronics help save a lot of quite expensive and embarrassing cabling, filters, attenuators, amplifiers, and reduce thermal losses in the cryostat. It can also contribute to shorten the qubit gate to qubit readout cycle which can fasten the execution of quantum correction codes that will be required when operating large scale quantum processors.

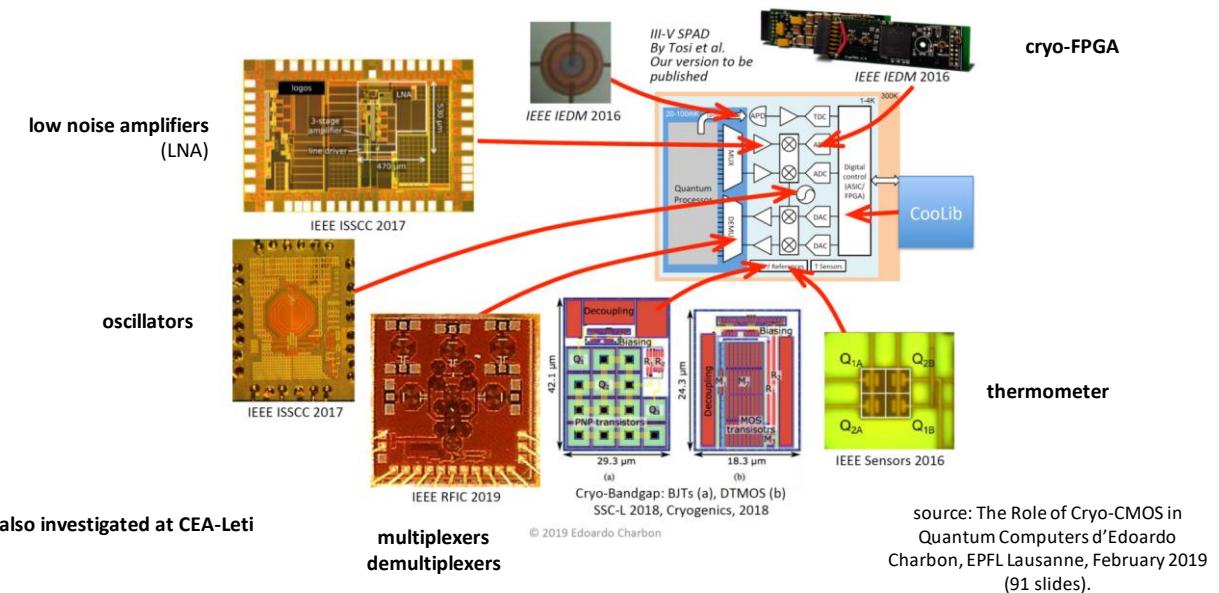
It must meet rigorous specifications<sup>835</sup>. The example *below* describes the variety of component functions that can be integrated in the 1K-4K stages and even, when possible, at the qubit chipset stage at less than 20 mK<sup>836</sup>.

These components must be certified to operate at these temperatures. These are data multiplexers, frequency oscillators, arbitrary waves microwave pulse generators, low-noise amplifiers, readout electronics, DC/AC square signals pulse generators (for spin qubits), thermometers and other various sensors.

<sup>834</sup> See [Scalable and customizable arbitrary waveform generator for superconducting quantum computing](#) by Jin Lin, 2019 (9 pages).

<sup>835</sup> See [Engineering cryogenic setups for 100-qubit scale superconducting circuit systems](#) by S. Krinner et al, 2019 (29 pages) which describes the issues with superconducting qubit control. In 2018, they proposed an optimized approach of wiring and electronics allowing up to 150 superconducting qubits to be embedded in a cryostat.

<sup>836</sup> Source of the diagram: [The Role of Cryo-CMOS in Quantum Computers](#) by Edoardo Charbon, EPFL Lausanne, February 2019 (91 slides). See also an earlier work from Purdue University and Australian colleagues: [Cryogenic Control Architecture for Large-Scale Quantum Computing](#) by J. M. Hornibrook, 2014 (8 pages) which describes well what should be done where in the cryostat.

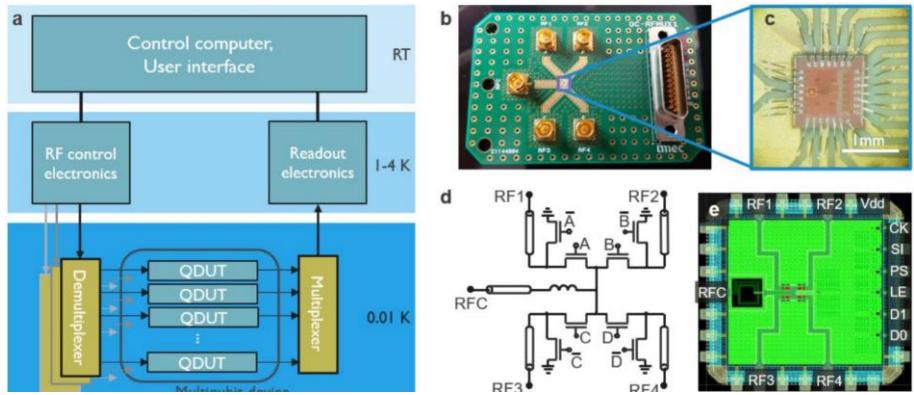


The trend is to put within the cryostat a maximum of these electronic components. However, the heat they released is limited by the dilution refrigeration system cooling power<sup>837</sup>. It also conditions at which cold-plate stage these components can operate.

The available cooling power currently barely reaches 25  $\mu\text{W}$  at the 10-20mK stage and 1 W at 4K. Starting in 2016, separate solid-state electronic components started to be designed and tested at cryogenic temperatures.

For example, Chalmers University of Technology (Sweden) created a **cryo-LNAs** (low noise amplifier) using **HEMTs** (high-electron-mobility transistors) and indium phosphide (InP) transistors which are very efficient at 4K. These amplifiers were designed for the readout microwaves reflected by the qubits. Still, these microwaves were analyzed outside the cryostat<sup>838</sup>.

IMEC (Belgium) developed in 2020 a cryo-CMOS RF MUX multiplexing the in and out microwave signals used in qubit readouts and operating at 32 mK. Working at up to 10 GHz, it is suitable for superconducting qubits readouts and not yet for all electron spin qubits<sup>839</sup>.



It greatly simplifies the cabling between RF control and readout electronics that sit at 4K and the qubit chipset sitting at below 20 mK.

<sup>837</sup> See [Cryogenic Control Beyond 100 Qubits](#) by Ian Conway Lamb, 2017 (103 pages) which describes the technological challenges of components operating at cryogenic temperature, here for superconducting qubits. And the short version: [Cryogenic Control Architecture for Large-Scale Quantum Computing](#) by Ian Conway Lamb et al, 2017 (8 pages). See also [Semiconductor devices for cryogenic amplification](#) by Damien Prêle, 2013 (30 slides) and [Cryo-CMOS Circuits and Systems for Quantum Computing Applications](#) by Bishnu Patra et al, 2018 (14 pages).

<sup>838</sup> See [InAs/AlSb HEMTs for cryogenic LNAs at ultra-low power dissipation](#) by Giuseppe Moschetti et al, 2020, Solid State Electronics (7 pages).

<sup>839</sup> See [Millikelvin temperature cryo-CMOS multiplexer for scalable quantum device characterisation](#) by Anton Potočnik et al, IMEC, November 2020 (35 pages).

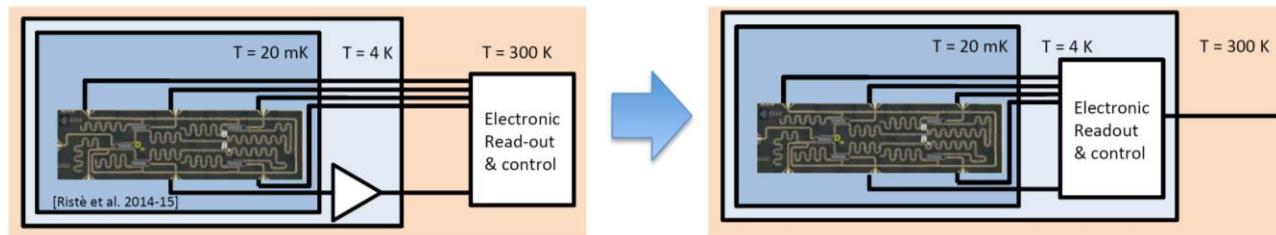
Even better, **CEA-Leti** prototyped in 2020 a low-noise cryo-CMOS amplifier that operates as low as 10 mK<sup>840</sup>. All this is used to handle the first stages of qubits state readout within the cryostat.

The trend is to integrate all these components in a minimum number of chipsets, preferably one, and working as close as possible to the qubits chipset. The best level of integration so far was reached with **Intel** HorseRidge 2 announced in 2021 and the coldest operation was achieved with the Gooseberry chipset from **Microsoft** and the **University of Sidney** as well as with a cryo-CMOS from **CEA-Leti**.

The first approach was to miniaturize these circuits at the 4K stage of the cryostat. It was studied in 2019 at **TU Delft** for silicon qubits state readout with their QuRO, for Quantum Read-Out<sup>841</sup>. The readout was using microwaves photon reflectometry.

It sent an unmodulated RF frequency and evaluated the amplitude and phase of the reflected RF photon. The technique allows multiplexing qubits readout before sending the information out of the cryostat. This simplifies the output wiring. The prototype was based on a CMOS low noise amplifier (LNA) supplemented by a SiGe (silicon-germanium) transistor amplifier, followed by an analog-to-digital converter (ADC) implemented in a Xilinx Artix 7 FPGA.

This FPGA made it possible to multiplex the readout state of several qubits. They use some copper cooling radiator in the 4K stage of the dilution refrigeration. They relied on standard market off-the-shelf passive and active components operating correctly at 4K.



This prototyping did not deal with the waveform generation and DAC circuits driving qubit gates. The energy saving of this kind of system is related to the quantum error correction load on qubit measurement. Bringing readout electronics closer to qubits speeds up error correcting codes. It's also interesting for simplifying the connectivity and improving quantum computers scalability.

A similar approach was initially adopted by **Intel** in collaboration with **QuTech** for its 2020 Horse-Ridge superconducting and silicon qubits driver component capable of handling the microwave pulses of this frequency driver from 2 to 20 GHz. This component is placed in the 4K stage of the cryostat<sup>842</sup>.

Introduced in 2021, **HorseRidge 2** improved cryo-electronics integration to an unprecedented level. It added multigate pulsing making it possible to control several qubits simultaneously, qubit readout and a programmable microcontroller. Gate pulsing create multi-qubit gates with square DC signals controlling the barrier and plunger gates of the quantum dots while single-qubit gates use modulated RF signals and qubit readout use regular RF signals. The chipset uses frequency multiplexing to reduce the number of RF cables for qubits drive and readout. It drives up to 16 spin qubits with frequency ranges between 11 and 17 GHz. It reads the state of up to 6 qubits simultaneously.

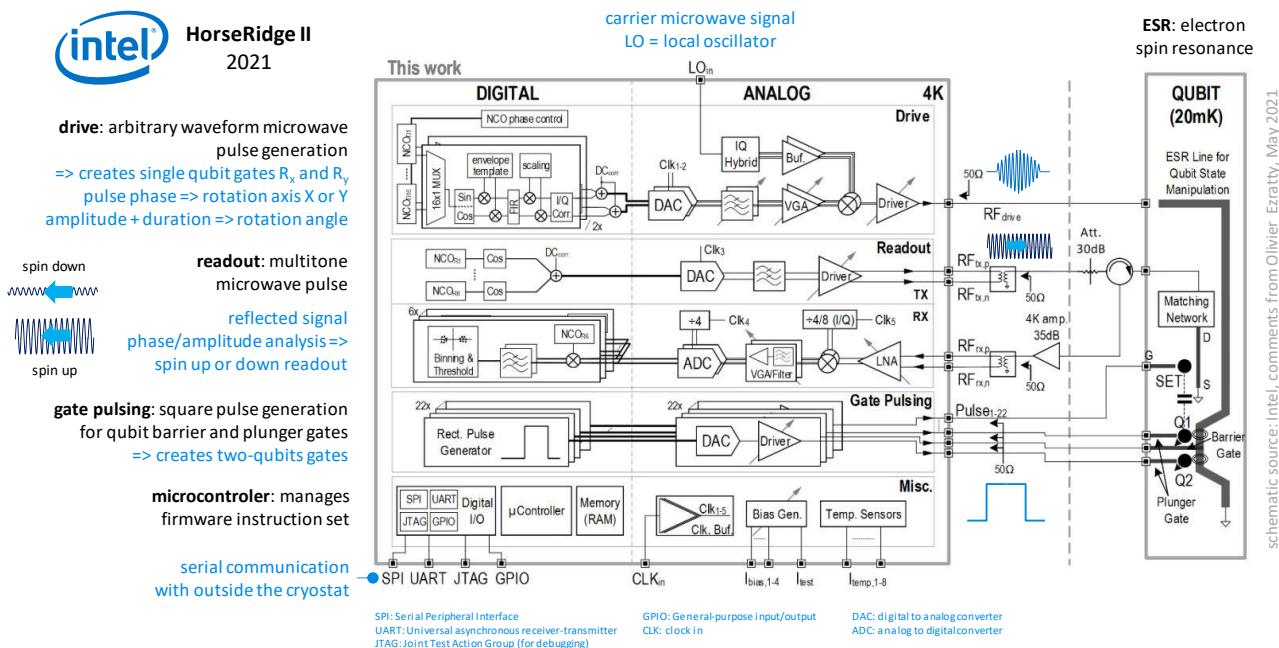
---

<sup>840</sup> See [Low-power transimpedance amplifier for cryogenic integration with quantum devices](#) by L. Le Guevelet al, March 2020 (13 pages).

<sup>841</sup> See [Cryogenic electronics for the read-out of quantum processors](#) by Harald Homulle, TU Delft, 2019 (185 pages).

<sup>842</sup> See [Cryo-chip overcomes obstacle to large-scale quantum computers](#) by QuTech, February 2020.

The control chip contains 22 DACs to simultaneously control the gate potentials for many qubits. The chipset is manufactured in a 22nm low-power FinFET technology (22FFL), operates at 4K and contains 100 million transistors<sup>843</sup>.



In May 2021, Intel and Qutech demonstrated high-fidelity two-qubit control with this HorseRidge 2 control chipset.

While HorseRidge 2 operates at 4K, others are trying to put its features at a lower cryostat level, 100 mK or even 10-20 mK, in 2019, an American-Australian team from **University of Sydney**, **Purdue** and **Microsoft Research** designed Gooseberry, a CMOS circuit to control superconducting, electron spin or (the yet to be seen) Majorana fermion qubits<sup>844</sup>. It is operating at the 100mK stage, just next to the qubit circuit on the same PCB support (in that case, only for silicon qubits since superconducting qubits would sit at the 15 mK cold plate stage). The circuit is using a microwave carrier signal source outside the cryostat. It is using a round-robbing scheme to distribute modulate micro-waves to each and every qubit in a sequential way.

Qubit readout is done here with external circuits (ADC and FPGA). It is a bit the opposite of Harald Homulle's solution from TUDelft. The test CMOS is realized in FDSOI in 28nm. The chipset greatly simplifies the control circuitry coming from outside.

This low-power chipset is generating control pulses of 100 mV at 18 nW per cell. The control of the qubits can also use superconducting microwave generation and reading circuits, their interest being a much lower thermal dissipation<sup>845</sup>.

<sup>843</sup> See [A Fully Integrated Cryo-CMOS SoC for Qubit Control in Quantum Computers Capable of State Manipulation, Readout and High-Speed Gate Pulsing of Spin Qubits in Intel 22nm FFL FinFET Technology](#) by J-S. Park et al, February 2021 (3 pages) and 41 slides.

<sup>844</sup> See [A Cryogenic Interface for Controlling Many Qubits](#) by D.J. Reilly et al, December 2019 (7 pages). It was then published in [Nature](#) in January 2021.

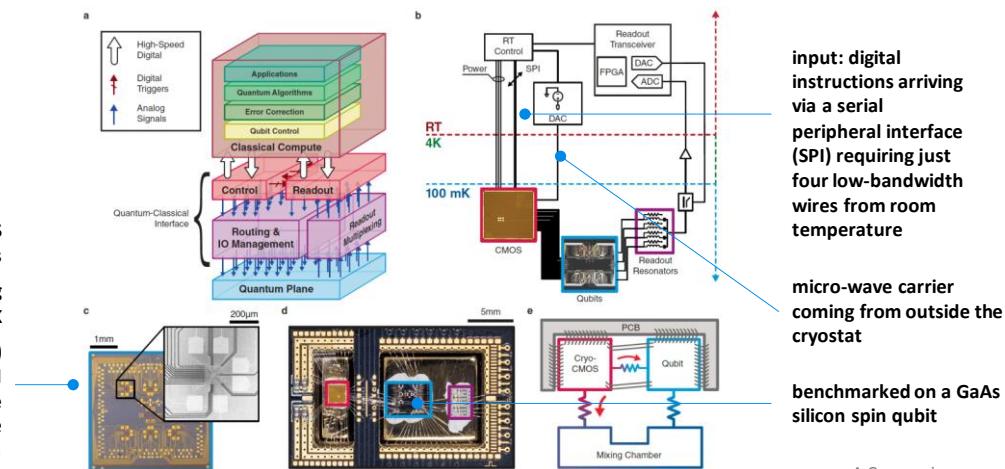
<sup>845</sup> See [Quantum Computer Control using Novel, Hybrid Semiconductor-Superconductor Electronics](#) by Erik P. DeBenedictis of Zettaflops, 2019 (15 pages), which describes an approach for controlling qubits mixing superconductors (JJ) and adiabatic circuits, Cryogenic Adiabatic Transistor Circuits (CATCs). The paper gives an overview of the energy efficiency of CryoCMOS components and various known superconductors (RQL, AQFP, ...).

**mixed analog/digital CMOS with low-leakage transistors**

**28 nm FDSOI CMOS operating at 100 mK**

**charge lock fast-gate (CLFG) multiplexing command voltage to many variable outputs**, with sequential time multiplex qubits activation

contains master oscillator, wave form memory, configurable ring oscillator



**input: digital instructions arriving via a serial peripheral interface (SPI) requiring just four low-bandwidth wires from room temperature**

**micro-wave carrier coming from outside the cryostat**

**benchmarked on a GaAs silicon spin qubit**

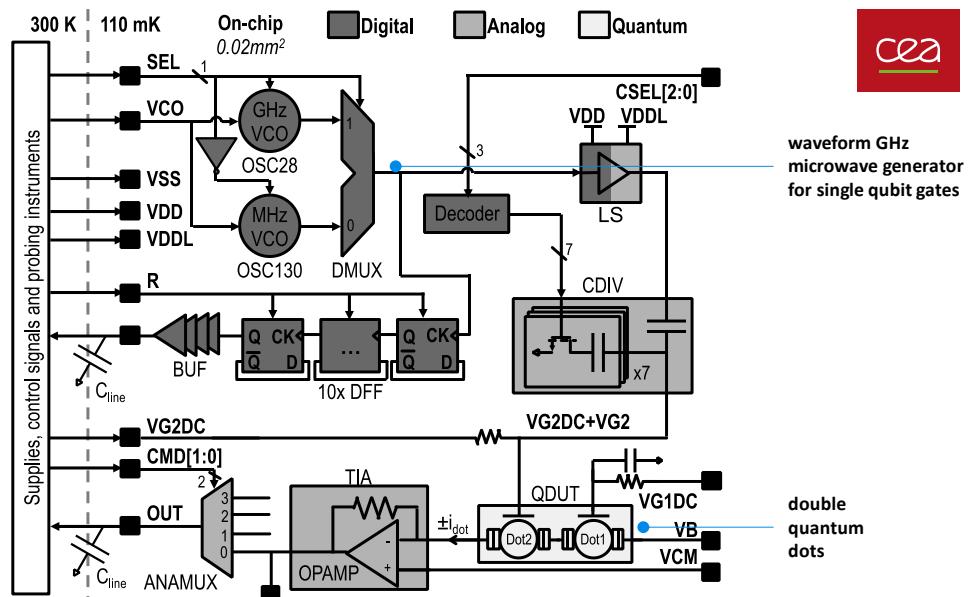
source: A Cryogenic Interface for Controlling Many Qubits by J.D. Reilly et al, December 2019 and published in Nature in January 2021.

In 2020, **CEA-Leti** in Grenoble created a mixed analog, digital and quantum cryo-CMOS circuit manufactured in 28 nm FDSOI and operating at 110 mK. It handles all the qubits driving and readout cycle with charge pumping, generating GHz microwaves and measuring the induced current with a multiplexed transimpedance amplifier (TIA)<sup>846</sup>.

**mixed digital-analog circuits including biasing, signal generation and qubit manipulation, and read-out.**

source: A 110mK 295μW 28nm FD-SOI CMOS Quantum Integrated Circuit with a 2.8GHz Excitation and nA Current Sensing of an On-chip Double Quantum Dot by Loick Le Guevel, Silvano de Franceschi, Yvain Thonnart, Maud Vinet et al, February 2020, ISSCC.

**readout signals passing through a parametric amplifier**



At this experimental stage, it drives only a couple qubits but looks promising with regards to the ability to control qubits at their operating temperature, at least for silicon qubits working between 100 mK and 1.5 K depending on their type and experimental settings.

One key technology to master when assembling electronic components at the qubit level is packaging and connectivity. That's where a French team from **CEA-Leti**, **CEA LIST** and **CNRS-Institut Néel** made progress in February 2021 with building a prototype interposer enabling the integration of quantum and control chips fabricated from different materials, processes and sources.

<sup>846</sup> See [A 110mK 295μW 28nm FD-SOI CMOS Quantum Integrated Circuit with a 2.8GHz Excitation and nA Current Sensing of an On-chip Double Quantum Dot](#) by Loick Le Guevel, Silvano de Franceschi, Yvain Thonnart, Maud Vinet et al, February 2020, ISSCC (12 pages).

Named QuIC (Quantum integrated circuits with CryoCMOS), the prototype demonstrator controls quantum chipsets with integrated control electronics and operating at below 1K. The integration uses a 3D flip-chip process. The control electronics are made on standard FDSOI 28nm by STMicroelectronics. Passive elements and filter devices will be integrated in future versions.

The integrated packaging increases the number of qubits that can be controlled with reducing the number of coaxial cables flowing through the cryostat from the upper stages. It also avoids chipset wire bonding since qubits and control electronics are coupled by routing lines on the interposer. The packaging allows thermal decoupling between the quantum chipset and the electronics control chip-set. They also use a die-to-wafer process from CEA-Leti that are used to build interconnects working at under 1K.

CEA is also replacing indium bumps with other materials that are compatible with existing CMOS manufacturing processes, like SnAg microbumps and directly bonded Cu pads from Cu/SiO<sub>2</sub><sup>847</sup>.

At last, let's deal with cryo-electronics using superconducting components based on the Josephson effect. This technique has been operational in **D-Wave** chipsets since its inception. Its contains both flux superconducting qubits and superconducting SFQ circuits for signals control generation, control and qubit state readout, now for 5000 qubits! This is a little-known technological feat for D-Wave. It allows them to greatly simplify the wiring that leads to the quantum processor. The only shortcoming is that these electronics may be a significant source of noise affecting the qubits quality. These SFQ circuits only create DC signals and ramp currents with DACs (digital-to-analog converters) to configure the annealer Ising model and drive the magnetometers used for qubits readouts. They don't generate microwaves signals.

**CNRS-Institut Néel-UGA** and the **LPMMC** in Grenoble developed a cryogenic amplifier based on SQUID superconducting Josephson effect superconductors, a TWPA - *travelling wave parametric amplifier*, aka "two-pa"<sup>848</sup>. The test components were manufactured in the Nanofab at Institut Néel in Grenoble. They might be used for qubit readouts by Qilimanjaro. In Finland, **VTT** is also manufacturing such amplifiers using 1600 Josephson junctions to handle superconducting qubits readouts.

Still, the most amazing work in superconducting electronics can be found with SeeQC.



SeeQC (2017, USA, \$34,2M) is a subsidiary of Hypres, an American company specialized in the creation of superconducting electronics, created by John Levy, Matthew Hutchings and Oleg Mukhanov<sup>849</sup>. Its parent company Hypres (1983, USA, \$50K) is already a long-time specialist in superconducting electronic circuits.

Its name stands for "Superconducting Energy Efficient Quantum Computing". It focuses on the creation of control circuits for superconducting qubits, which are themselves superconducting circuits equipped with spintronic technology memories<sup>850</sup>. The company was initially funded under IARPA's C3 project launched in 2016. On top of New York, they have established research labs in Rome, Italy and in the UK. They are partnering with Martin Weides's team from the University of Glasgow and with Oxford Quantum Circuits. They even got two grants totaling £1.8M from Innovate UK's Industrial Challenge Strategy Fund as part of two consortiums.

<sup>847</sup> See [Die-to-Wafer 3D Interconnections Operating at Sub-Kelvin Temperatures for Quantum Computation](#), September 2020.

<sup>848</sup> See [A photonic crystal Josephson traveling wave parametric amplifier](#) by Luca Planat et al, October 2019 (17 pages).

<sup>849</sup> See [Seeqc Cuts Its Own Path to the Quantum Era With Integrated Circuit Approach](#) by Matt Swayne, The Quantum Daily, September 2020. By setting up offices in Milan and the UK, the startup found a way to secure European funding for its research. Otherwise they collaborate with Robert McDermott's team at the University of Wisconsin and the Syracuse team in upstate New York.

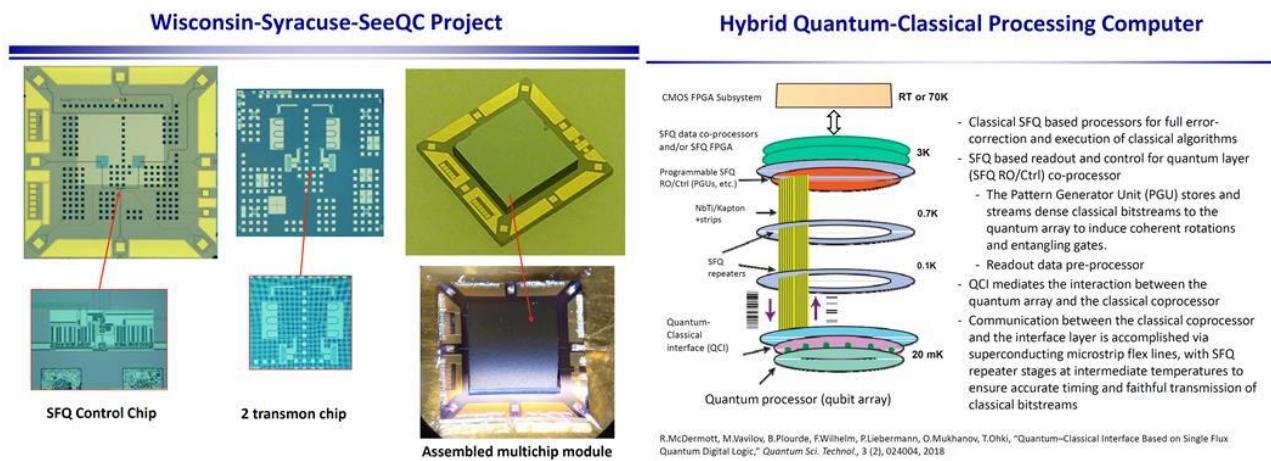
<sup>850</sup> See [Single Flux Quantum Logic for Digital Applications](#) by Oleg Mukhanov of SeeQC/Hypres, August 2019 (33 slides).

The first includes Oxford Quantum Circuits, Oxford Instruments, Kelvin Nanotechnology, University of Glasgow and the Royal Holloway University of London, to create a superconducting qubit computer. The second, named NISQ.OS, is focused on building an operating system with Riverlane, Hitachi Europe, Universal Quantum, Duality Quantum Photonics, Oxford Ionics, Oxford Quantum Circuits, arm and the UK National Physical Laboratory, another SeeQC partner in the UK.

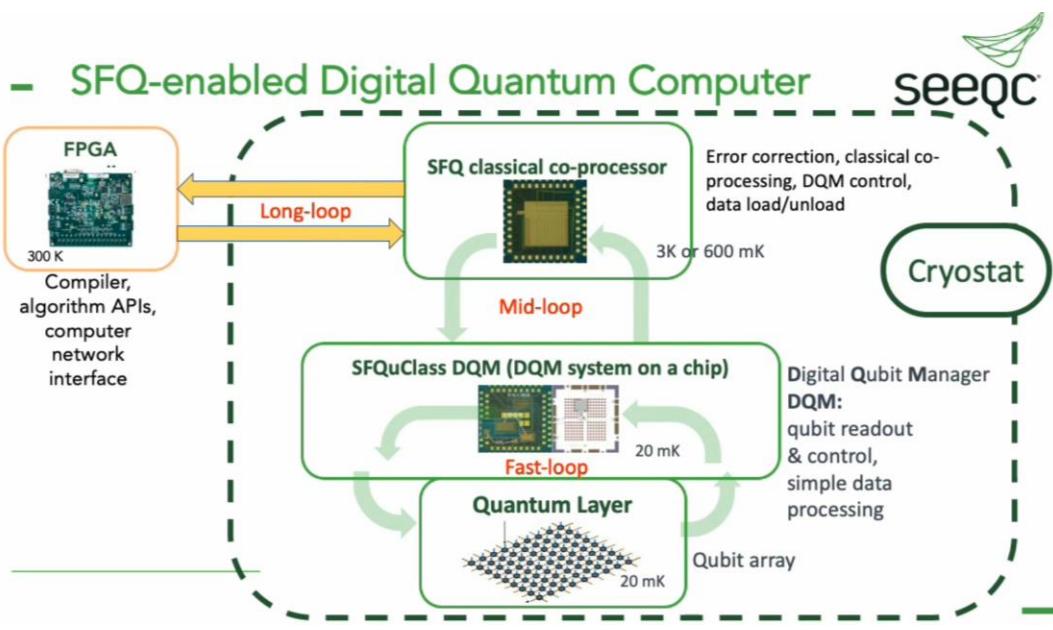
As a result, SeeQC and Riverlane announced in June 2021 announced that they had integrated Riverlane's operating system Deltaflow.OS with SeeQC's qubit driving components.

Their current architecture is based on two chipsets: a classical SFQ control chipset and the SFQu-Class DQM, both using Josephson junctions in SFQ superconducting circuits.

The first chipset runs at 3K or as low as 600 mK. It controls the DQM and handle error corrections without requiring an external computer.



The SFQuClass DQM (Digital Quantum Management) includes the microwave generators used to drive the qubits (with DACs, digital-to-analog signal converters) and for qubits readouts (with ADCs, analog to digital microwave signal converters)<sup>851</sup>.



<sup>851</sup> See [Single Flux Quantum Logic for Digital Applications](#) by Oleg Mukhanov, August 2019 (33 slides) and [Quantum-Classical Interface Based on Single Flux Quantum Digital Logic](#) by Robert McDermott et al, 2017 (16 pages). See also [Accurate Qubit Control with Single Flux Quantum Pulses](#) by Robert McDermott and M.G. Vavilov, 2014 (10 pages) and [Scalable Hardware-Efficient Qubit Control with Single Flux Quantum Pulse Sequences](#) by Kangbo Li, Robert McDermott and Maxim G. Vavilov, 2019 (10 pages).

Its power drain is only 0,0002 mW per qubit when it could reach 2 mW per qubits with cryo-CMOS. Another advantage of SFQs is that their clock speed can reach 40 GHz when classical cryo-CMOS are limited to 2 GHz.

The mid-loop between the SFQ co-processor and the DQM also reduces the latency for qubits controls and is particularly interesting for implementing error correction codes<sup>852</sup>.

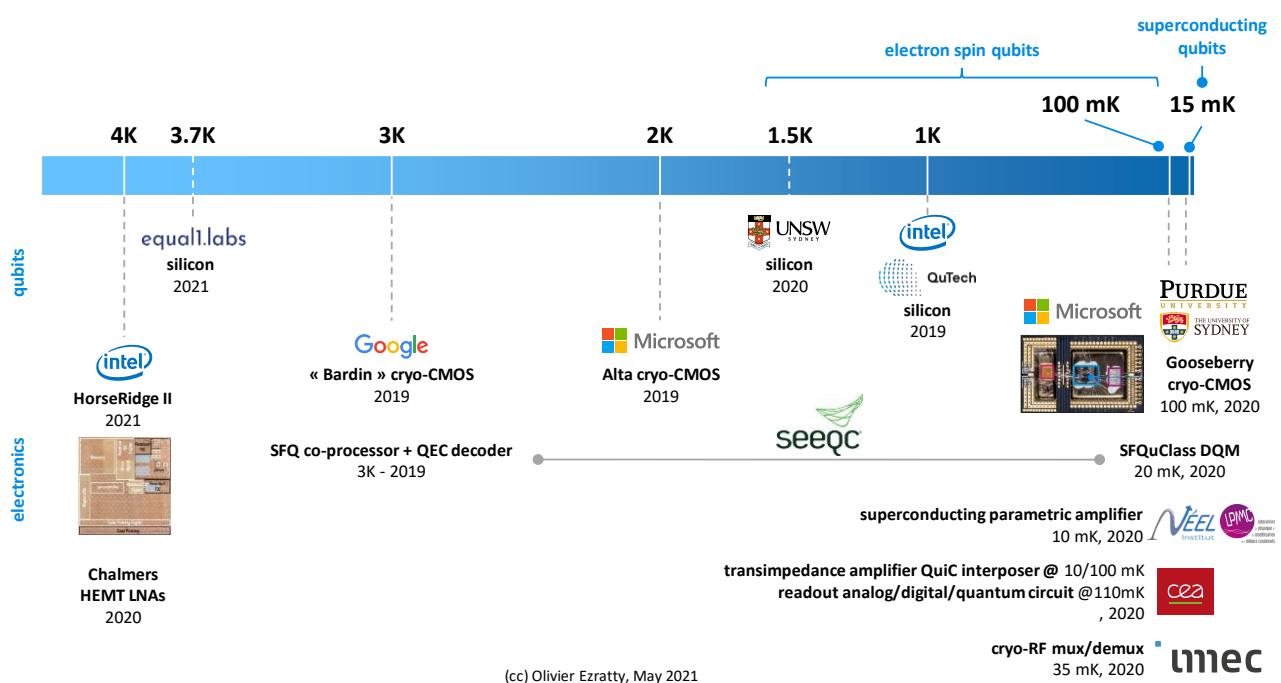
When we can generate all microwave signals inside the cryostat, it still must be exchanged both ways digitally with the outside of the cryostat. This can be done through signals multiplexed on copper, fiber optics, or even, it is under study, radio waves at very high frequencies (in THz). It also helps maximizing the thermal and vacuum insulation with the outside.

An optical fiber has the advantage of being made of glass, which does not generate thermal expansion and is a weak heat conductor.

Still, SeeQC has scalability plans that will require using a growing number of wires with the number of qubits.

"Quantum" Rent's Rule			
Qubit Count	Qubit Control Wiring Overhead		Application
2	4	<b>3</b>	Prototype
10	20	<b>3</b>	Prototype
100	200	<b>31</b>	Prototype
1k	2,000	<b>76</b>	Optimization / chemistry
10k	n/a	<b>330</b>	Optimization / chemistry
100k	n/a	<b>~1,600</b>	Big data / ML
1m	n/a	<b>~6,000</b>	Encryption

To be fair, all these cryo-CMOS and superconducting chipsets must be compared with detailed specifications.



<sup>852</sup> See [Quantum-classical interface based on single flux quantum digital logic](#) by Robert McDermott, 2018 (19 pages), [Digital coherent control of a superconducting qubit](#) by Edward Leonard Jr. et al, 2018 (13 pages). The diagram on page 10 suggests that microwave generation is always performed outside the cryostat. This is related to the fact that the experiment contains a double control of the qubits: by direct current to drive the microwave generation by the SFQ near the qubits, and in the traditional way outside the cryostat. This allows them to compare the fidelity of the two methods. And then [Digital coherent control of a superconducting qubit](#), by Oleg Mukhanov (CTO and co-founder of SeeQC), Robert McDermott et al, September 2019 (39 slides) and [Hardware-Efficient Qubit Control with Single-Flux-Quantum Pulse Sequences](#) by Robert McDermott et al, 2019 (10 pages).

The generated microwave quality depends on the sampling rates used in their DAC and ADCs, on the number of points used in generating the wave envelope (16,384 points for HorseRidge 2), their power consumption per qubit, their frequency range (targeting superconducting and/or electron spin qubits), their clock, their noise level and their real scalability potential with a large number of qubits. These electronic components must also be as isolated as possible from the qubits chipsets.

Let's now look at other commercial vendors in the cryogenic electronics area, given they don't create any cryo-CMOS at this point.



**Atlantic Microwave** (1989, USA) produces and markets radio-frequency and microwave components operating at cryogenic temperatures.

They are used to control superconducting and silicon qubits in cryostats. This includes microwave attenuators, filters, microwave amplifiers and bias tees. It is a subsidiary of the British group ETL Systems, founded in 1984.



**Marki Microwave** (1991, USA) is a supplier of microwave control components: amplifiers, bias tees, couplers, mixers and filters.



**Quantum Microwave** (2016, USA) creates microwave components operating at cryogenic temperatures for quantum computers, including pre-amplifiers, attenuators, frequency couplers, multiplexers, bias tees, diplexers, filters, image reject mixers and directional couplers.



One main applied research domain for **Raytheon** is related to superconducting qubits controls. They work on arbitrary pulse sequencers (APS) creating superconducting qubits control microwaves and an FPGA readout system using low noise parametric amplifiers.

They are also exploring SFQ based control logic (Josephson gate-based logic) and spintronics based low-power memories. They are mainly found in superconducting qubits quantum computers (IBM, Google, Rigetti, D-Wave). However, they do not push forwards the miniaturization of these components like SeeQC does. In October 2021, they announce a technology partnership with IBM, with not much details<sup>853</sup>.



**Diramics** (2016, Switzerland) is a spin-off from ETH Zurich creating ultra-low noise transistors in III-V materials (InP, indium-phosphorus) with a technology named pHEMT (pseudomorphic high-electron-mobility transistor, using junctions with two semiconductors with different band gaps).

It can be used in low temperature electronics. It is currently mostly used in astronomy applications.

At last, let's mention **Cosmic Microwave Technologies** (USA) which produces cryogenic LNAs (low noise amplifiers) used for qubits readouts.

## Thermometers

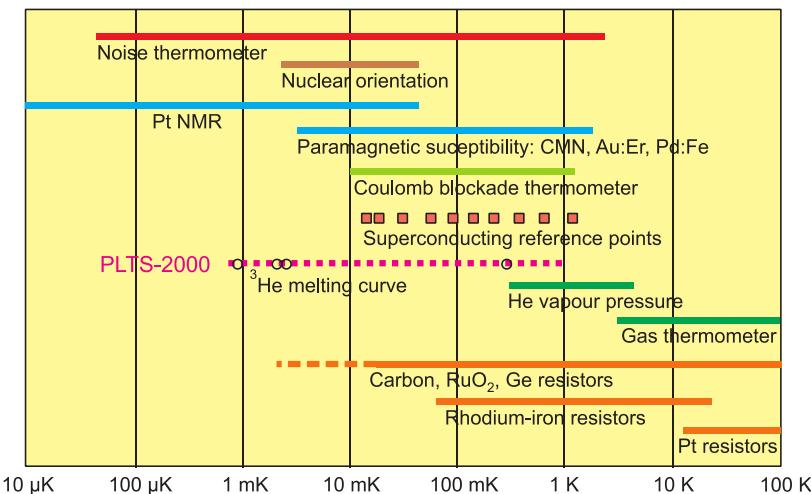
It must be possible to **measure** pressure (ambient, gas), temperature (everywhere) and flow (of gas) at cryogenic temperature. Specific sensors are therefore installed for this purpose in the cryostat enclosure, attached to different places in the "candlestick".

---

<sup>853</sup> See [Raytheon, IBM partner for quantum in defense, aerospace](#) by Nicole Hemsoth, in TheNextPlatform, October 2021.

Temperatures are measured with cryogenic thermometers<sup>854</sup>! These are found in particular at **Lake Shore Cryotronics** with its Cernox thermometers which go down to 100 mK and resist well to the ambient magnetic field and its ruthenium oxide thermometers which go down to 10 mK. At less than 20 mK, noise thermometers using Josephson junctions are used (and the loop is closed...). Some thermometers are placed on the plates opposite the heat exchange tubes and the mixing box.

## Low Temperature Thermometers



Still, progresses need to be done even in this area, noticeably to measure precise temperatures in the 10 mK range and with no delay<sup>855</sup>.

## Vacuum

Besides photon qubits, most other qubit types require some form of vacuum to isolate the qubits from their environment. We usually make a distinction between different levels of vacuum. The most stringent ones are used with trapped ions and cold atoms which require ultra-high vacuum (UHV) conditions whereas solid-state qubits like superconducting and electron spins are less demanding. UHV starts at  $10^{-9}$  mbar.

One problem to avoid when creating vacuum is outgassing. It manifests with particles being ejected from the internal enclosure surfaces and materials, including residual water coming from the air. The phenomenon is avoided with carefully selecting the materials.

Cold atoms qubits require a pressure of  $10^{-10}$  mbar while trapped-ions goes down to  $10^{-12}$  mbar. In both cases, low pressures and outgassing are obtained with heating the system enclosure above 200°C for several hours while the vacuum pumps are operating. This “bake-out” process removes water and other trace gases sitting on the chamber surface. Heating is implemented with heater stripes placed around the chamber. The chamber exterior can also be cooled with liquid nitrogen to contain any further gassing.

There are many vacuum and ultra-high-vacuum systems vendors. The most commonly seen in research labs is **Pfeiffer** (Germany).

<sup>854</sup> Source of the diagram: [Thermometry at low temperature](#) by Alexander Kirste, 2014 (31 slides). We can see that there are about ten types of thermometers that go down to less than 1K. The most commonly used one exploits the Coulomb block based on tunnel junction. The electrical voltage of the junction varies linearly with the cryogenic temperature.

<sup>855</sup> That's what researchers from Chalmers in Sweden achieved in 2020. See [Primary Thermometry of Propagating Microwaves in the Quantum Regime](#) by Marco Scigliuzz, Andreas Wallraff et al, December 2020 (14 pages).

At last, measuring pressure in vacuum is also a challenge. Classical mechanical pressure are of no use in the UHV to XUV (extreme ultra-vacuum) ranges covering  $1 \times 10^{-6}$  to  $1 \times 10^{-10}$  Pa. The NIST in the USA is proposing a solution applicable to cold atoms to cover these ranges of pressures<sup>856</sup>.

## Lasers

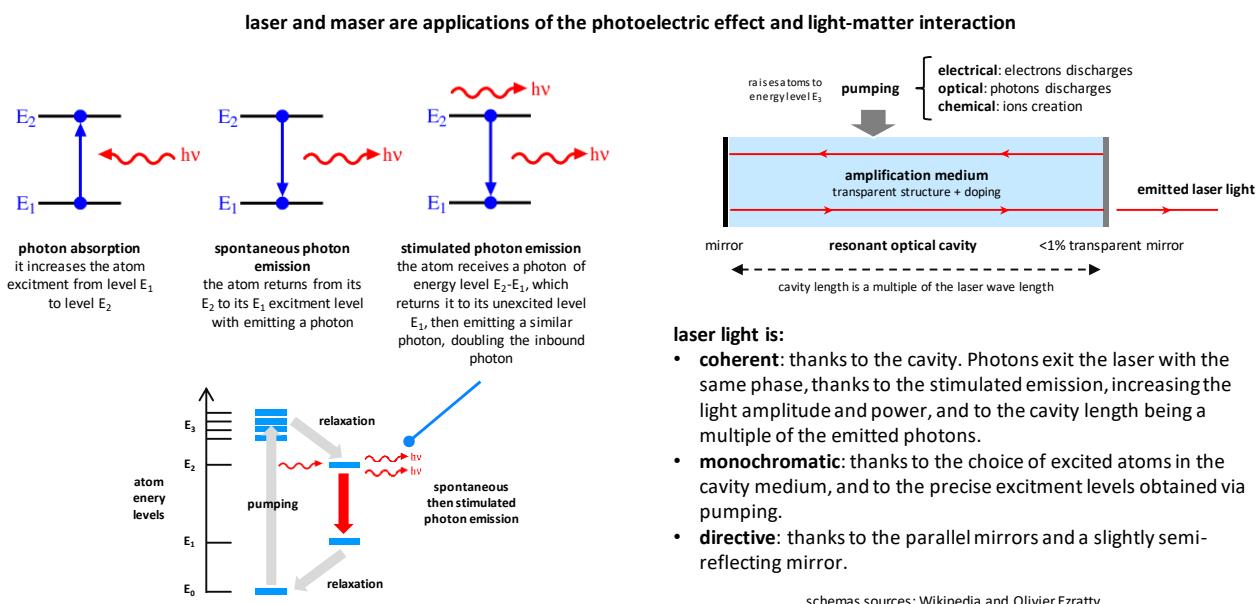
Masers and lasers are applications of three successive discoveries and inventions:

- **Fabry-Pérot resonant cavities**, named after Charles Fabry<sup>857</sup> (1867-1945) and Alfred Pérot (1963-1925). Their system invented in 1898 was originally used to create an interferometer.
- **Stimulated emission**, formalized by Albert Einstein in 1917. It occurs when an excited atom receives a photon of energy equivalent to a transition between two energy levels. It then re-emits two photons identical to the received one and the energy level of the atom is reduced to its ground state.
- **Optical pumping**, invented by Alfred Kastler in 1949 at ENS in France, which earned him the 1966 Nobel Prize in Physics.

It generates a population inversion, creating a high proportion of atoms excited at level  $E_2$  in the diagram below compared to level  $E_1$ . Optical pumping often excites atoms to energy levels higher than  $E_2$  in the diagrams *below*, with a non-radiative transition from these levels to the  $E_2$  level and then from the  $E_1$  level to the fundamental level of the  $E_0$  atom. If pumping was performed only between levels  $E_1$  and  $E_2$ , their proportion would balance and the laser effect could not be triggered. Three-level pumping is used with pulse lasers and four-level pumping with continuous lasers.

A laser is based on a resonant cavity filled with a gain or amplifier medium. The pumping of this gain medium is optical, electrical or chemical. Once at the high energy level ( $E_2$  in the diagram *below*), the atom drops to the  $E_1$  energy level either spontaneously or stimulated.

The mechanism can be self-sustained since the spontaneously emitting photons then generate the stimulated emission of identical twin photons in frequency, phase and amplitude.



<sup>856</sup> See [Development of a new UHV/XHV pressure standard](#) (Cold Atom Vacuum Standard) by Julia Scherschlig et al, 2018 (15 pages).

<sup>857</sup> We owe to Charles Fabry the creation of the Institut d'Optique, of which he was the first director in 1926 of the engineering school that was originally called SupOptique or Ecole Supérieure d'Optique.

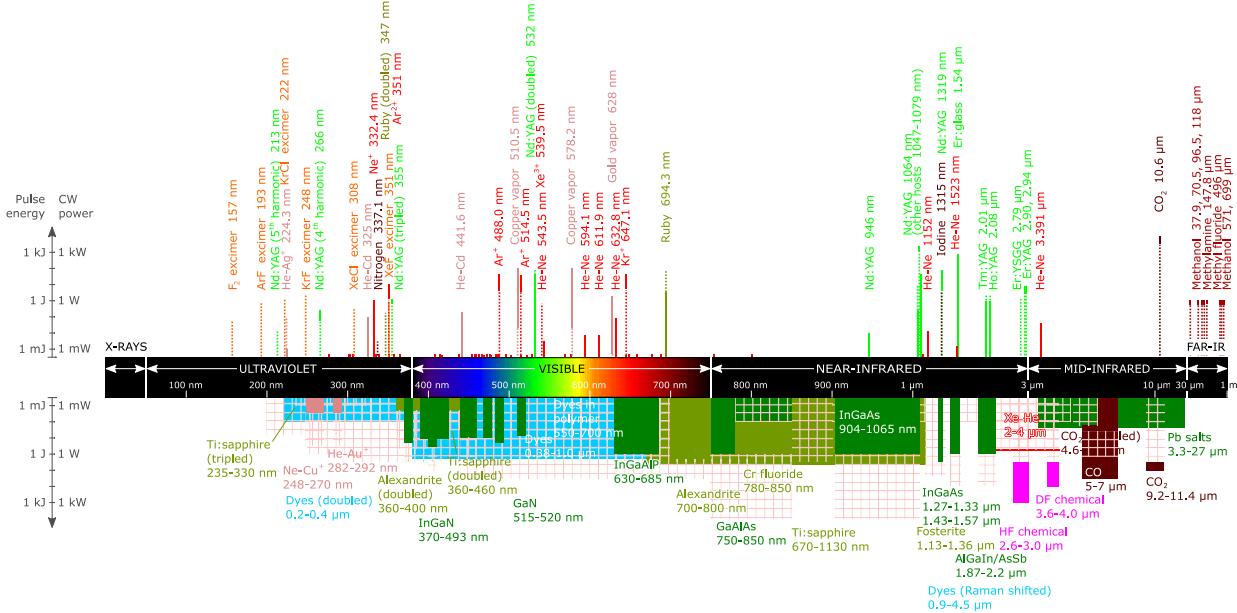
The stimulated emission is sustained by placing the atoms in a transparent cavity, filled with solid, liquid or gas, and parallel mirrors trapping the photons. One of the mirrors is slightly semi-reflective, allowing some of the amplified light to exit the laser.

This system of mirrors plays the role of a resonator. It reflects off-axis and thus undesirable photons out of the laser and the wanted on-axis photons back into the excited population where they can continue to be amplified thanks to the laser pumping.

The light resulting from this process is **directive** (thanks to the resonator and its parallel mirrors), **monochromatic** (thanks to the choice of excited atoms and the fineness of the cavity) and **coherent** (the photons are in phase and with the same wavelength/frequency thanks to the stimulated emission and the length of the cavity being a multiple of the laser wavelength). The laser photons frequency depends on the materials used in the cavity and the optical length of the cavity. As an order of magnitude, a 1mW red laser emits  $3 \times 10^{15}$  photons per second.

Lasers (light amplification by stimulated emission of radiation) appeared conceptually in 1958 in an article by Arthur Leonard Schawlow and Charles Hard Townes. The first **gas laser** was created in 1960 by Theodore Maiman, using helium-neon. **Excimer-based** gas lasers cover ultraviolet.

We then had successively **doped crystal lasers** (also named solid-state lasers, such as ruby which is  $\text{Al}_2\text{O}_3$  doped with  $\text{Cr}^{3+}$ , or YAG, Yttrium garnet and Aluminum  $\text{Y}^{3+}\text{Al}^{5+}\text{O}_{12}^{-2}$ ), **chemical lasers** (covering the infrared spectrum), **semiconductor diode lasers** (the most common today, usually based on gallium arsenide, or AsGa), **fiber lasers** (using rare earth elements like neodymium, erbium and thulium, mainly used in optical communications), and finally, **free electron lasers**, which we already briefly covered in relativistic quantum mechanics section (source: [Wikipedia](#)).



The lasers operate either in pulses or continuously. The first mode is used to create very high-power levels. To create very powerful lasers, laser amplifiers are created which consists of chains of lasers with a primer laser that is connected to a series of lasers that successively amplify the light generated by the previous laser.

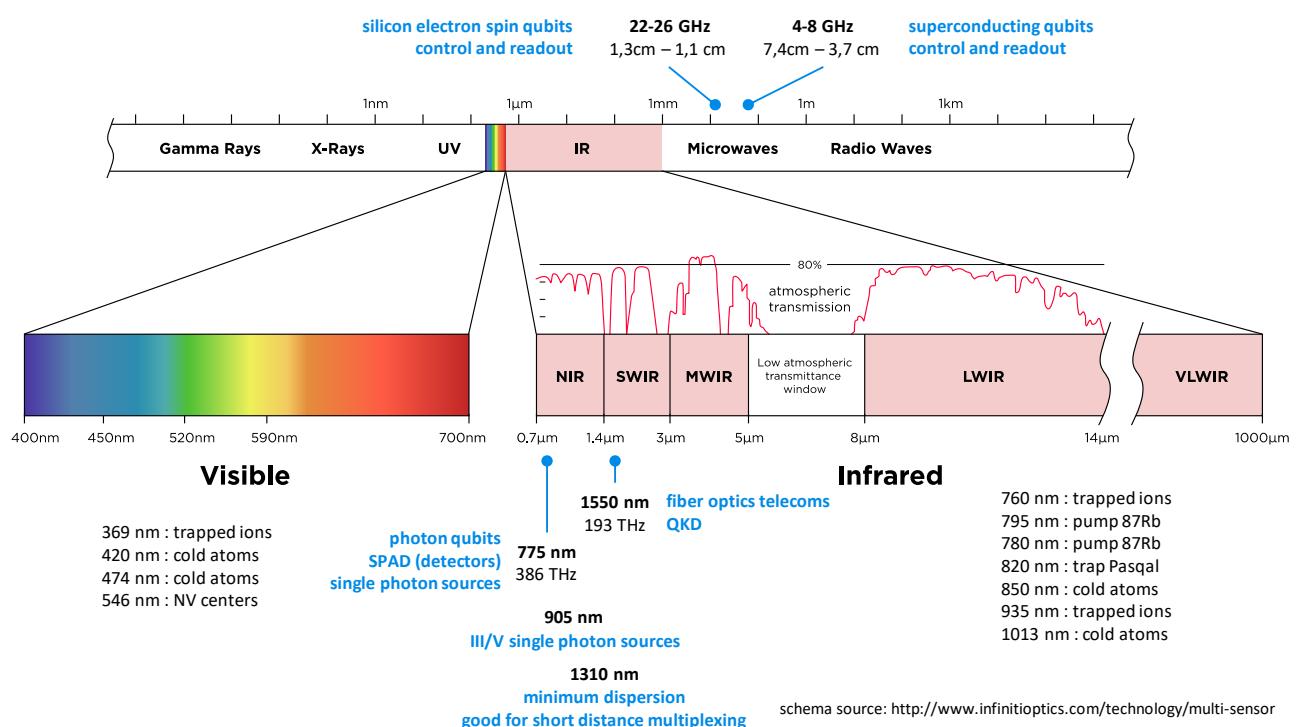
Lasers applications are quite various: industrial diamond drilling and cutting (1965), barcode readers (1974), laser printing (1981), office scanners, Laserdisc (1978), audio CDs (1982), DVDs (1995), surgery, particularly in ophthalmology (glaucoma, retinal detachment, refractive surgery), cosmetic surgery, in dermatology, for tattoo and hair removal, telecommunications, laser pointers, depth sensors, focus sensors for smartphones, iPhone FaceID sensor, measurement and alignment in construction, all sorts of LiDARs, stereolithography 3D printing, confocal microscopy (very shal-

low depth images), flow cytometry (cell counting), DNA chips analysis, video projector light sources, velocity measurement, the stripping of certain materials, various weapons, nuclear fusion, telescopes adaptive optics, atoms cooling, quantum telecommunications, quantum cryptography and finally, quantum computing, and on and on and on. In short, lasers are everywhere!

The frequency ranges covered by lasers range from infrared to ultraviolet. There are even types of lasers with adjustable frequency. Free electron lasers go as far as X-rays. Gamma-rays lasers - or grasers - do not yet exist.

In quantum technologies, the most commonly used laser wavelengths are 775 nm (beginning of the near infrared region next to red) and 1550 nm (middle of the near infrared region). The first one is used for quantum computing thanks to efficient photon generation and single photon detection (particularly with APD, avalanche photo diodes). The second is used in optical fiber for long distance communications, data transmission and QKD systems.

There are many solutions to up and down convert photons from/to these two wavelengths. For example, these conversions are mandatory when connecting several photon-based quantum computers through a fiber optic link. Solid-state qubits require another type of conversion, mostly from micro-waves to 1550 nm infrared photons, given the conversion must convert the quantum information in the solid-state qubit to some encoding in the resulting photons, like their polarization.



Another breed worth mentioning are femtoseconds lasers, which create short pulses of coherent light in the range from the femtosecond ( $10^{-15}$ s) to the picosecond ( $10^{-12}$ s). They are used in micro-machining and various other tasks, including quantum sensing in relation with frequency combs<sup>858</sup>.

The **Maser** (1953) or "Microwave Amplification by Stimulated Emission of Radiation" was invented before the laser, in 1953, by Nikolay Basov, Alexander Prokhorov and Charles Hard Townes, who were awarded the Nobel Prize in Physics in 1964.

<sup>858</sup> See [20 years of developments in optical frequency comb technology and applications](#) by Tara Fortier and Esther Baumann, NIST, 2019 (16 pages).

It is the equivalent of the laser, but emits microwaves instead of visible light. The first masers were made with ammonia and generated 24 GHz microwave photons. Hydrogen Masers followed in 1960.

gas	doped crystals	chemical	diodes	fibers	free electrons
ionized argon	rubis	hydrogen-fluoride	AsGa	ytterbium	
ionized krypton	Nd-YAG	deuterium-fluoride	DFB	erbium	
helium-neon	rare earths		VCSEL	$\text{Nd}^{3+}$	
copper-neon	titanium				
nitrogen	chromium				
$\text{CO}_2$	OPO				
excimers					

There are many laser vendors who play a role in second revolution quantum technologies, both with photon qubits, quantum telecommunications, quantum cryptography and quantum sensing. Lasers are also used to control cold atom and trapped ions qubits.

## Stable Laser Systems

**Stable Laser Systems** (2009, USA) offers Fabry-Perot lasers and cavities that can be used for cold atom confinement. The startup launched by Mark Notcutt is based in Boulder, Colorado, one of the nerve centers of quantum technologies in the USA, near NIST and the University of Colorado. His team also includes Jan Hall, winner of the 2005 Nobel Prize in Physics for the discovery of the effect that bears his name.



**Toptica Photonics** (1998, Germany) is a photonics equipment manufacturer developing laser sources covering a wide range of frequencies from 190nm (UV) to Terahertz waves, including laser diodes and frequency combs. Their lasers can be used to control trapped ions and cold atoms<sup>859</sup>. They employ over 320 people for a revenue of \$82M.

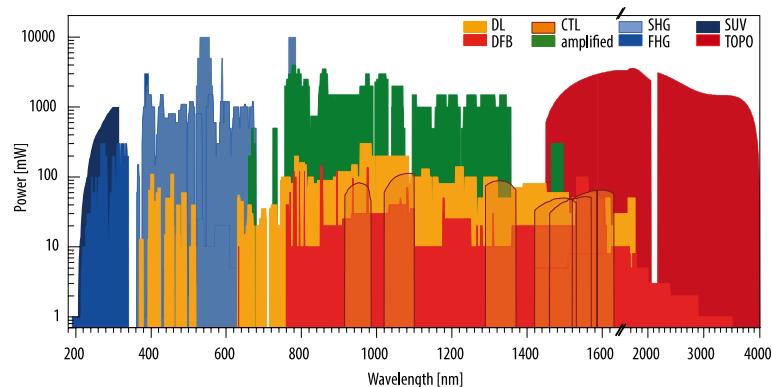


Fig 2 Each quantum system requires lasers with a specific combination of wavelengths and power levels. The broad wavelength coverage from 190 nm to 4  $\mu\text{m}$  provided by Toptica's tunable diode lasers combined with reliable and convenient operation therefore enables many spectacular applications of quantum technologies. (Source: Toptica)



**Lumibird** (1970, France) is a supplier of lasers. Formerly Quantel and Keopsys, it is a large SME with more than 800 employees and a turnover of 110 M€, 80% of which is exported.

<sup>859</sup> See [The Control of Quantum States with Lasers](#) in Photonics View, 2019 (3 pages).



**Chromacity** (2013, UK) is a manufacturer of lasers targeting various industry and research needs, including quantum communications.

Their flagship product, the Chromacity OPO, has a tunable optical parametric oscillator that covers near-IR and mid-IR wavelengths. Some of their lasers can create entangled photons.



**DenseLight Semiconductors** (2000, Singapore) manufactures various laser products.



**FemTum** (2016, Canada) creates mid-infrared lasers which can be used in quantum optics and silicon photonics applications and quantum sensing using optical frequency combs. It is a spin-off from the Center of optics, photonics and laser (COPL) in Quebec City.



**FocusLight Technologies** (2007, China) produces laser diodes and laser optics components.



**Freedom Photonics** (2005, USA) manufactures lasers and photodiodes.



**GLOphotronics** (2011, France) sells hollow-core photonic crystal fiber (HC-PCF) and their functionalized form Photonic Microcells (PMC). These lasers use a proprietary fiber technology and gas photonics. They are partnering with CNRS XLIM lab in Limoges.



**iPronics** (2019, Spain) develops general-purpose integrated programmable photonic systems, where optical hardware complements software to perform multiple functions.



**Q.ANT** (2018, Germany) develops a green laser optimized for NV centers quantum sensors. It is a subsidiary of the TRUMPF Group. It also manufactures powerful lasers used in ASML lithography machines and light channels on silicon for qubits transport. They are also working on photonic-based quantum computing.



**Silentsys** (2021, France) created a closed-loop voltage regulation electronic system that complements lasers and their servo controller to reduce the emitted laser noise and improve its frequency precision.



**UnikLasers** (2013, UK, £4.1M) sells ultra-narrow linewidth, high power lasers at the specific wavelengths related to the exact atomic transitions targeted for quantum sensing applications.

It can transform a MHz linewidth laser into an Hz linewidth laser. It is currently adapted to continuous lasers running in the 1550 nm and 1050 nm wavelengths and fits in a 2U rack system. Their OFD system (optical frequency discriminator) delivers a continuous voltage signal driving the laser diodes that is proportional to the frequency fluctuations of the input laser beam. The technology core is optical, using frequency combs. They also propose low power voltage power systems. One of their OFD can drive two lasers.



**Vexlum** (2017, Finland) produces high-power narrow-linewidth vertical external-cavity surface-emitting lasers (VECSELs) including blue and UV lasers, used among other things, to control trapped beryllium ions.

It is a spinoff from Tampere University of Technology Optoelectronics Research Centre (ORC).

And also: **Spectra Physics** (1961, USA), **Altitun** (1997, Sweden, \$10M), **Calmar Laser** (1996, USA) and **Ampliconyx** (2016, Finland who manufactures short-pulses lasers), **Active Fiber Systems** (2009, Germany) which creates femtoseconds fiber lasers and is a spin-off from Fraunhofer IOF, **InnoLume** (2002, Germany, \$26.8M, which sells laser diodes), **FISBA** (1957, USA) which develops multi-wavelengths lasers, **Intense Photonics** (1994, USA, \$51M, which develops single and multi-mode monolithic laser array products, and high power laser diodes and was acquired by Orix Group), **Lytid** (2015, France) which manufactures terahertz cascade lasers, **Spark Lasers** (2015, France) and their picosecond and femtosecond lasers, **Amplitude Laser Group** (2001, France) and their femtosecond lasers, **neoLASE** (2007, Germany) a supplier of various laser products including laser amplifiers, **Alpes Lasers** (1994, Switzerland) which sell infrared quantum cascade lasers, **Luna Innovations** (1990, USA, \$13.1M), **Vector Photonics** (2020, UK, £1.6M) is a spin-off from the University of Glasgow which develops semiconductor lasers based on PCSELs (Photonic Crystal Surface Emitting Lasers) and **OEwaves** (2000, USA, \$15M) provides lasers, oscillators and optical/RF tests and measurement systems.

## Photonics

Let's now look at other photonics equipment manufacturers. They sometimes also manufacture lasers but even more.



**Accelink** (1976, China) sells optoelectronic components, including fiber optics modulation and demodulation systems, lasers and SiO<sub>2</sub>/Si material plane optical waveguides. They probably play a role in the deployment of quantum telecommunication networks.



**Aurea Technology** (2010, France) is a photonics equipment manufacturer targeting various markets including quantum communications (QKD) and quantum sensing.

It sells twin photon sources (TPS), time correlated single photon detectors (Picoxea), photon counters (SPD\_A and SPD\_OEM\_NIR), time correlators (Chronoxea) and high-resolution fiber sensors (q-OTDR) and picosecond pulse lasers (Pixea). They also developed Fluoxea, a fluorescence lifetime imaging mapping system using time-correlated single photon counting that can be used to characterize semiconductors, qualify quantum dots or measure local magnetic fields (with the help of NV centers).



**Azur Light Systems** (2010, France) develops high-power laser amplification systems in the infrared and the visible using ytterbium-based fibers with low thermal dissipation.



**Qontrol Systems** (2016, UK) develops photonics components including photonics device status readout modules and backplanes (boards) on which several of these modules can be installed. These modules drive photonics devices via a 12V voltage and read signals with 18-bit accuracy. This is control electronics.



**CAILabs** (2013, France, €16.7M) is a company based in Rennes, France, which is a spin-off from the LKB of ENS Paris and markets photonics equipment and in particular spatial multimode multiplexing systems for optical fibers supporting up to 45 nodes.

This is what makes it possible to multiply the speed of the optical fibers of the telecom operators' networks. In particular, they have KDDI (Japan) as a customer. The startup is managed by Jean-François Morizur (CEO) and Guillaume Labroille (CTO) with Nicolas Treps from LKB being their scientific advisor.



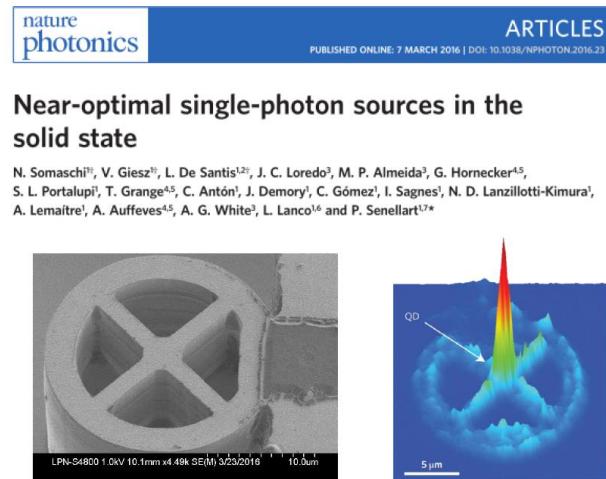
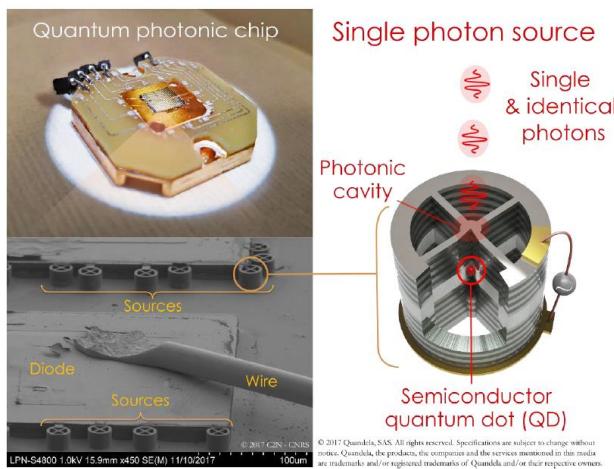
**Quandela** (2017, France, €35M) is a startup specialized in the generation of indistinguishable photons with quantum dot fed by a laser. They target research, telecommunications and quantum computing use cases.

Quandela's team is composed of Valérian Giesz (CEO), an engineer from the Institut d'Optique with a PhD in photonics, Niccolo Somaschi (CTO), PhD from the University of Southampton and Pascale Senellart (CSO), CNRS research director at C2N from CNRS and Université Paris-Saclay. They also have Alain Aspect, Andrew White and Eleni Diamanti in their advisory board. It had a staff of about 15 people in September 2021 and several international customers, mainly in Europe, Russia and Asia. Their team also includes Shane Mansfield, who works on algorithms and software.

With a single trapped atom forced to emit a photon in a given direction by laser-activated cavity quantum electrodynamics, they are able to generate photon streams that are well separated in time and with stable quantum characteristics, with wavelengths from 924 nm to 928 nm in the near infrared, this range being progressively extended<sup>860</sup>.

This creates a very bright photon source that can then be multiplied to create indistinguishable photons used in quantum photon processors and various other applications such as quantum cryptography<sup>861</sup>.

They are developing single photon sources running at telecom wavelength as part of the project ParisRegionQCI, a regional project, led by Orange, with an end goal to deploy a QDK-fibered link between Paris and the Paris-Saclay University.



The photon source must be cooled down to a temperature range of 5K-10K, which is achievable with compact cryostats costing only a few thousand Euros and using helium 4, such as the atoDRY800 from **Attocube** (Germany). These cryostats use a pulsed head, equivalent to the first cooling stage of the dry dilution cryostats. These single photons are particularly indicated to allow the creation of quality quantum qubit gates.

Quandela's photon generator was previously offered as a combination of two packaged products:

<sup>860</sup> See [Near optimal single-photon sources in the solid state](#), Niccolo Somachi, Valerian Giesz, Pascale Senellart et al, 2016 (23 pages). Pascale Senellart describes in detail how Quandela's photon generators are made in her talk [Quantum optics with artificial atoms](#) in a Rochester Lecture in June 2018 (1h10mn). The prestigious [Rochester Lectures](#) are held once a year in Durham, UK. The 2017 edition welcomed Peter Knight and the 2012 edition Alain Aspect.

<sup>861</sup> The process was improved in Pascale Senellart's laboratory in 2020 to generate even brighter and purer photon sources from a spectral and polarization point of view thanks to quantum dot excitation with phonons. See [Efficient Source of Indistinguishable Single-Photons based on Phonon-Assisted Excitation](#) by S. E. Thomas, Pascale Senellart et al, July 2020 (10 pages).

- The **Qubit Control Single Unit** which allows complete filtering of the single photons emitted by the sources in an attocube cryostat of the laser used for quantum dot excitation. It is mainly composed of filters tuned to the energy of the optical transition of the emitter.

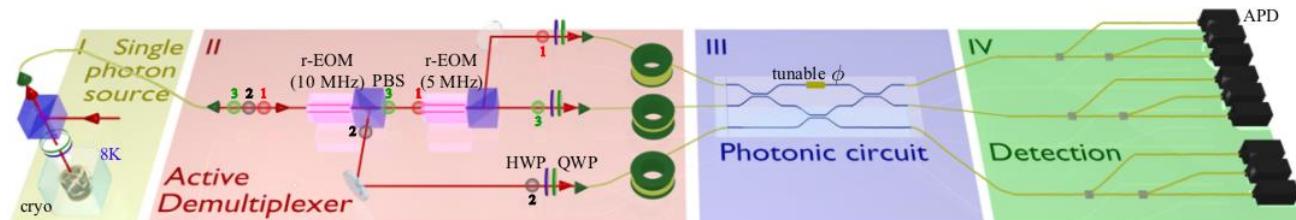
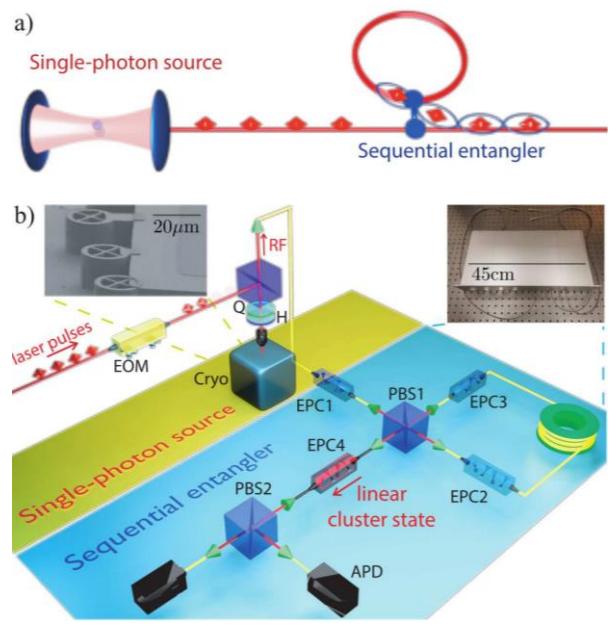


- The **QShaper** is a more compact device that generates femto/pico-second laser pulses on an optical fiber that will then feed the QCSU quantum dot above. It is powered at the input by the customer's laser. It is used to prepare the laser beam with the right spatial and temporal shape. It is a device made up of various filters. It is calibrated to supply the semiconductor sources.

Quandela launched in 2020 a compact and integrated version of this whole set, fitting into a data-center rack. The fiber is glued to the photon source, which will eliminate the mechanical part of the calibration. The pulsed head of the 4K cryostat is also integrated in this 3U rack, the compressor being outside and water-cooled at first. Eventually, it will be integrated in the rack and cooled by air.

The rack was designed by **Pentagram**, the same British designer that IBM used for the Q System One launched in January 2019. It is 1.75m high and 80cm wide. It stacks all the elements: the QShaper, the new QCF and a control computer with its keyboard. The whole thing consumes about 5 to 6 kW, the bulk of it coming from the cryostat.

Quandela and the C2N laboratory collaborate with research labs around the world to create advanced photonics platforms. In 2020, they published with a team from the **Hebrew University of Jerusalem** a paper on the creation of a photon cluster state for quantum computing (*below*). The idea is to use single photons and to entangle them with each other via a delay line, and inject them into a computing circuit based using cluster states and MBQC (measurement based quantum computing) method<sup>862</sup>. In Europe, they collaborate mainly with **Fabio Sciarrino**'s team in Italy, in the Netherlands with **Quix**, in Spain with **INL** and other teams in Austria, the United Kingdom, Slovakia and Israel. They are part of the European FET project PHOQUSING for boson sampling led by Fabio Sciarrino's team.



<sup>862</sup> See [Sequential generation of linear cluster states from a single photon emitter](#) by D. Istrati et al, 2020 (14 pages).

In 2019, they experimented with Quandela's photon source to demultiplex it into three photons which were then injected into a photonic integrated circuit integrating a programmable quantum gate. The photonic circuit was precisely etched with a femtosecond laser<sup>863</sup>.

A last, since 2020, Quandela has started working on creating a photon-based quantum computer using their own photon source.



**Quantum Opus** (2013, USA) develops single photon detectors based on superconducting nanowires, the Opus One. The compact version Opus Two is an 8U data center rack-mount package, including cryostat<sup>864</sup>. This company benefited from US federal funding, including \$100K in 2015 and \$1.5M in 2015 from DARPA and \$125K from NASA in 2018. They are a provider of the Chinese team who did run the gaussian boson sampling experiment announced in December 2020.



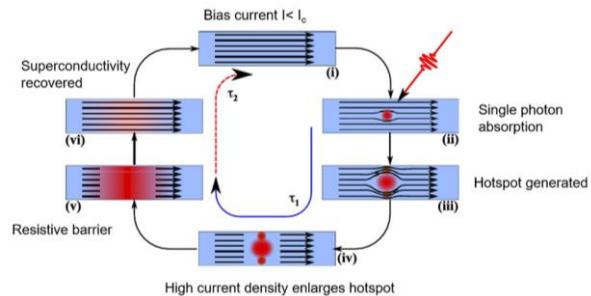
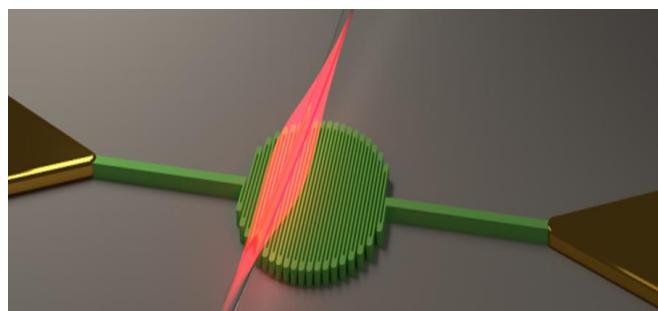
**Qubitekk** (2012, USA, \$5M) is a supplier of photon and entangled photon sources for use in the context of quantum cryptography (QKD). This technology can also be used to manage part of the communication between qubits in some types of quantum computers. It competes to some extent with Quandela.



**Scontel** (2004, Russia) offers single photon detectors in the visible and infrared (SSPD, for Superconducting Single Photon Detecting Systems). These detectors are cooled at 2.2K helium-4 using a Sumitomo SRDK 101 pulse head system with a water-cooled HC-4E compressor.



**Single Quantum** (2012, The Netherlands) offers Qos single photon detectors integrated in a 2.5K liquid helium cooled cryostat. Their sensor uses the SNSPD (superconducting nanowire single photon detector) technique, made of a thin film of superconducting nanowires shaped into a flattened serpentine coil. This device captures a single photon from an optical fiber and have a detection efficiency of 85% to 90%, covering wavelengths from 800 nm to 1550 nm.



**Sparrow Quantum** (2016, Denmark, \$2.2M) is a spin-off from the Niels Bohr photonics research laboratory. Like Quandela and Qubitekk, they offer single photon sources.

Their solution is based on InAs quantum dots. Their engineering differentiation lies with the quantum dot efficient coupling with a slow-light photonic-crystal waveguide.

<sup>863</sup> See [Interfacing scalable photonic platforms: solid-state based multi-photon interference in a reconfigurable glass chip](#) by Pascale Senellart et al, 2019 (7 pages).

<sup>864</sup> See [Introduction to Quantum Opus and revolutionary superconducting detection systems](#) (14 slides).

A laser is illuminating the quantum dots with using a confocal microscope. Their photon coherence indistinguishability is between 95% and 98% with their Sparrow Chip 2021 Resonant. They are generated in the 920-980 nm wave range. The photon generation system is cooled at 6K.



**VLC Photonics** (2011, Spain) produces photonics equipment and fabless design of photonic integrated circuits. The company is involved in European Flagship projects.

It is a spin-off of the University of Valencia. The company was founded by Iñigo Artundo, Pascual Muñoz, José Capmany and José David Domenech. They also market technical reports at prices ranging from 4K€ to 5.4K€ per piece.



**Photonic** (2019, Canada) is a spin-off from the Silicon Development Lab at Simon Fraser University in Vancouver. They develop silicon-based photonic qubits. They are working in particular on methods of conversion between electron and photon spins for the transport of quantum information between silicon qubits.

**Excelitas** (2010, USA) sells various photonics devices including Single-Photon Counting Modules (SPCMs).

**Hamamatsu Photonics** (1953, Japan) provides silicon photodiodes, electron multipliers for detecting electrons, ions, and charged particles, photon counters, LCoS based spatial Light Modulators (SLM) used for cold atoms controls, laser cooling systems, quantum imaging and image sensors for the detection of neutral atoms, trapped ions and NV centers fluorescence.

**Miraex** (2019, Switzerland) has two main quantum technologies in its portfolio : photonic based quantum sensors for vibration, acceleration, acoustic, pressure, electrical field and temperature measurement and a quantum system converting matter qubits into photon qubits and vice versa. It's a spin-off from EPFL.

**Micron-Photons-Devices** (2004, Italy) aka MPD creates Single Photon Counting Avalanche Diodes, "SPAD", fabricated using custom silicon, standard CMOS and InGaAs/InP technologies. It also sells photon counting based QRNGs.

**Qubitrium** (2020, Turkey) develops entangled photon sources, laser current drivers and single photons detectors.

**Photon Force** (2015, UK) creates single-photons cameras of 32x32 pixels. It can be used in various photonic based quantum sensing applications. It enables time-tagging of incoming photons with a time resolution of 55 pico-seconds.

**Coversion** (2009, UK) develops laser frequency conversions devices that are used in many quantum optics applications. It's a spin-off from the University of Southampton.

We also have **Ibsen Photonics** (1991, Denmark) which provides spectrometers and various photonic equipment, **Ki3PHotonics** (2015, Canada) who develops multiplexing optical fiber solutions for QKD implementation, **Lumiphase** (2020, Switzerland) which develops optical modulators, **Pixel Photonics** (2020, Germany) which designs Single Photon Detectors, **Bay Photonics** (2007, UK) which provides photonic circuits assembly and packaging, **Qubig** (2008, Germany) which develops light modulators (amplitude and phase modulators, phase shifters, Pockels cells) that can be used in quantum computing or communications, etc.

## Other enabling technologies vendors

These companies are developing physical components and enabling technologies that can play a role in building quantum computers.

More often, as this market remains limited to research, these startups are more generalist and target broader markets than quantum computing, covering physics research in general and even various industrial applications.



It has labs in UK, France, Spain and Italy. They develop several quantum enabling technologies like frequency-stabilized lasers used to control cold-atoms, an ion-trap chip carrier, entangled sources of photons for space based QKD, a squeezed light quantum MEMS gravimeter.



**Aeponyx** (2011, Canada, \$11,4M) is a fabless micro-optical switch semiconductor chips designer and manufacturer, specialized in Micro-Electro-Mechanical-Systems (MEMS) and Silicon Photonics.

**Alter Technology** (2006, Spain/Germany) is a subsidiary of the German group TÜV NORD specialized in micro and optoelectronics engineering for space and harsh environment applications.

**Angstrom Engineering** (1992, Canada) is a manufacturing tool vendor. Their Quantum Series line of physical vapor deposition (PVD) systems is adapted to the creation of Josephson Junctions, from using an electron beam source to deposit aluminum, magnetron sputtering for niobium, to gas flow management.

**AuroraQ** (2017, Canada) creates communication systems based on superconducting qubits, including quantum communication repeaters. It is complemented by the QSPICE Design software which allows the design of superconducting quantum circuits. In other words, this is an ultra-niche market<sup>865</sup>.

**DiamFab** (2019, France) is a spin-off of Institut Néel in Grenoble specialized in the growth of doped diamond layers on a diamond wafer substrate. Among other markets, they also target NV center use cases in quantum technologies. Diamond is also used as a high-performance semiconductor for power applications for diodes and field-effect transistors.

**Elementsix** (1946, Luxembourg) is a subsidiary of De Beers Group, the world's leading diamond producer, which, among other things, manufactures synthetic diamonds for use in NV centers based systems, mostly used in quantum sensing. They hold a large number of patents in the related processes.

**Hummink** (2020, France) developed a patented technology combining a nanometric “pen” with an oscillating macroresonator to perform a capillary deposition of various liquids.

It can print conducting materials with an existing choice of 10 different materials. It can be used to add precision items on devices in 3D. They happen to already work with Alice&Bob and C12, two quantum computing startups developing qubits running at <1K.

<sup>865</sup> See [The Geometry of a Quantum Circuit and its Impact on Electromagnetic Noise](#), 2018 (15 pages).



**Kelvin Nanotechnology** (2020, UK) is an electron beam lithography and nanofabrication company. It manufactures various miniaturized MEMS and photonic components used in quantum technologies.

These include 3D ion traps, various photonic devices, MEMS gravimeters and lasers built on 200 mm wafers in features going as low as 20 nm. They are based at the James Watt Nanofabrication Centre (JWNC) in Glasgow, Scotland.



**Labber Quantum** (2016, USA) develops software solutions for controlling the qubits of experimental quantum computers. They are used to calibrate qubits. The startup was acquired by **Keysight Technologies** in March 2020.



**LakeDiamond** (2015, Switzerland, €2M) produced synthetic diamonds used to create NV centers qubits in diamonds or with quantum sensing.

They use vacuum deposition with the CVD method (Chemical Vapor Deposition). The company closed in February 2020 after getting funding from an ICO in 2018 (Initial Coin Offering, using some crypto-currency).



**Lucigem** (2016, Australia) manufactures fluorescent nanodiamonds that can be used in various quantum applications, particularly for medical imaging. The company is the result of work carried out at Macquarie University in Sydney.

**Qzabre** (2018, Switzerland) creates NV center-based tips and probes to be used in scanning microscopes. They also sell a NV center microscope, the QSM. The startup was created by Christian Degen from ETH Zurich.



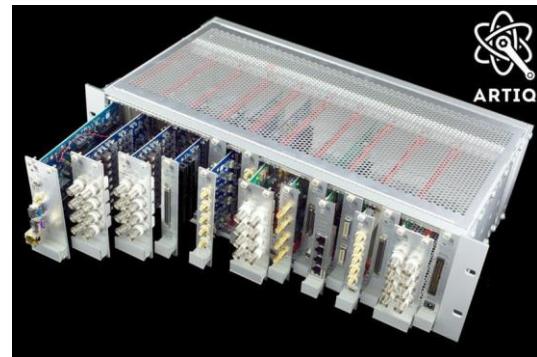
**Adamas Nano** (2010, USA) sells nanodiamond particles for various use cases including NV centers-based sensors. **Bikanta** (2013, USA, \$1.7M), **Cymaris Labs** (2004, USA) and **FND Biotech** (2016, Taiwan) sell fluorescent nanodiamond targeting medical imaging applications. **Diamond Materials** (Germany) is a manufacturer of various variations of diamonds including NV centers. **Photonanometa** (2011, Russia) is another producer of diamond with NV-center defects.



**M-Labs** (2007, Hong Kong), formerly known as Milkymist, is working on the ARTIQ (Advanced Real-Time Infrastructure for Quantum physics) project.

This system combines hardware and a real-time operating system to control quantum computer hardware based on trapped ions. It's a bit like the trapped counterpart of startups such as the Israeli Quantum Machines. They have developed their own FPGA circuit for ARTIQ, all programmed in Python. The solution has been developed with the Ion Storage Group team at NIST in the USA, working on ion trapped qubits.

The company was founded by a French engineer, Sébastien Bourdeauducq.





**Nano-Meta Technologies** (2010, USA) is a spin-off from the University of Perdue that aims to create a quantum information storage system. It is in fact a private contract research laboratory.

It commercializes intellectual property on technologies associating photonics and nanomaterials that could be used in quantum cryptography systems.



**Photon Spot** (2010, USA) develops nanowires based single photon detectors. They have received a DARPA funding of \$100K in 2014 and \$1.5M in 2015.

**Plassys Bestek** (1987, France) develops and manufactures vacuum and ultra-high-vacuum thin film deposition systems with a turnover of about 7M€. Most of their tools are based on physical vapor deposition processes (vaporization of metal or compounds for deposition on a substrate, all under vacuum).

Positioned at the end of the 1990s as a key supplier of equipment for the fabrication of superconducting qubits, they have developed a wide range of electron beam deposition systems under the name "MEB" which makes Plassys the leader for this technology (Yale, Rigetti Computing, QCI, NTT, Oxford, CEA Saclay, Qilimanjaro, TU Delft... rely on their tools). They also supply the "SSDR150" chemical vapor deposition reactor for the growth of ultra-pure diamond which is the raw material for the development of the NV center technologies.

Their R&D and production machines dedicated to quantum technologies are now grouped under the Qutek Series brand. In addition to the "MEB" systems, Qutek series includes "MP" systems (sputtering deposition for superconducting or photonic devices) and thermal evaporation system for indium bumps (interconnection of superconducting qubits).



**QBee.eu** (2020, Belgium) is a sort of quantum accelerator or incubator created by Koen Bertels, who also leads the Quantum Computer Architectures Lab in TU Delft and also works at Qutech.

They run various research projects like defining a quantum micro-architecture for quantum accelerators using the OpenQL language from TU Delft, a quantum computing emulator, quantum genomics and quantum finance plus some services in education and consulting.



**Q-LION** (2019, Spain) develops an error correction code solution for trapped ion qubits. The startup is a spin-off from the Bank of Santander's Explorer incubation program. It was created by Andrea Rodriguez Blanco, who was still working on a thesis in 2020.



QuTech

**QuTech** (2014, The Netherlands) is the quantum hardware spin off from TU Delft University. It collaborates with Intel in the development of superconducting qubits and with Microsoft in topological quantum.

The company is an applied contract research laboratory. It also develops software, such as the **Quantum Inspire** development platform, which enables quantum algorithms to be run on conventional computers in emulation mode. It provides a graphical programming interface in the QASM language. The code can then be executed in emulation mode in the cloud on a classic machine, the Dutch national supercomputer Cartesius, with 5, 26 and 32 qubits, depending on the chosen package.

Cartesius is equipped with thousands of Intel Xeon and Xeon Phi CPUs and a few dozen Nvidia Tesla K40m GPUs with 130 TB of memory delivering 1.84 PFLOPS. The equipment comes from Atos. Quantum Inspire also provides cloud access to QuTech qubits since April 2020.



**Raith** (1980, Germany) provides nanofabrication and electron beam lithography instruments. These tools are involved in the manufacturing of all sorts of qubits, trapped ions, superconducting, electron spin, topological qubits, NV centers and nanophotonics.



**S-Fifteen Instruments** (2017, Singapore) is a spin-off from the renowned CQT laboratory and develops qubit control systems, entangled photon sources, single photons detectors and quantum cryptography solutions covering QKD and QRNGs.



**StarCryo Electronics** (1999, USA) creates SQUIDs sensors used mostly in quantum sensing and other cryo-electronics products (cables, connectors, ...).



**Vapor Cell Technologies** (2020, USA) provides alkaline atom capsules, mainly rubidium, for use in various miniaturized solutions using cold atoms<sup>866</sup>. The company was founded by Doug Bopp, a former NIST researcher from Boulder.



**Zyvex Labs** (1997, USA) develops atomic precise manufacturing (APM) solutions that can be used to produce components for use in quantum computing (such as the deposition of dopants for superconducting qubits and silicon) and quantum metrology.

They were funded by NIST, DARPA and the Department of Energy SBIR research programs. The company was founded by Jim Von Ehr.

## Raw materials

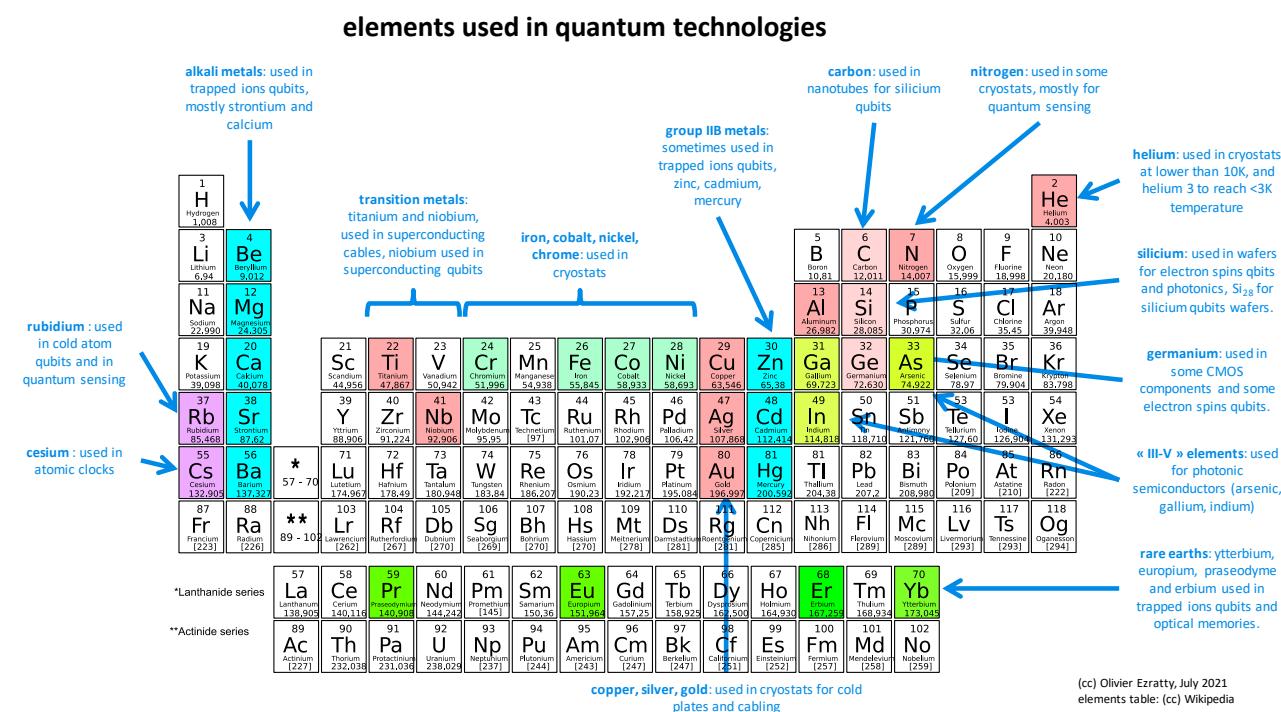
For any new hardware technology, it is now a common practice to wonder about its environmental friendliness. We've already been dealing with the energetic dimension of quantum computing. Another key aspect to investigate is the raw materials that are used. What are their sources of supply, their global reserves, their economic and environmental cost of extraction, consumable raw materials if any, and finally, the recycling processes of these materials?

<sup>866</sup> See [Chip-scale atomic devices](#) by John Kitching, 2018 (39 pages) which makes a very interesting inventory of measurement components using this technology: magnetometers, gyroscopes, atomic clocks. You will say that this should go in the metrology section and you will be right.

In this exclusive content, we make a broad inventory of the different raw materials used in and around quantum technologies of all types, particularly in quantum computers. All these elements are positioned in an in-house Mendeleev periodic table of elements, *below*<sup>867</sup>.

We mainly have two types of materials to study: those used in qubits and the supplemental materials, particularly for cables and other supporting structures as well as the gases used in cryostats, mostly helium 3 and 4.

The materials used in qubits are sometimes quite rare (strontium, ytterbium, beryllium). Their selection is based on their energy transitions which correspond to laser or microwave wavelengths that can be used practically with market sources. Other constraints explain their choice such as the stability of some of these energy levels. Some materials are very rare but their needs in quantum technologies remain marginal in proportion to their production and world consumption.



This is at least the case as long as millions of quantum computers using them are not manufactured. We are not yet at the stage where the consumption of certain elements would come mostly from quantum technologies, as may be the case for smartphones concerning certain rare earths and minerals such as the famous coltan<sup>868</sup>.

One differentiating aspect of quantum technologies relates to the isotopes used which are sometimes the rarest of their elements. This is the case for helium (3) used in cryogenics below 4K or for cesium (133) for atomic clocks or rubidium (87) in cold atoms. Silicon (28) is used in silicon qubits and, although it is the most abundant isotope, requires costly refining. Carbon (12) is also used in nanotubes like with the startup C12 Quantum Electronics, while Carbon 13 is used in some NV center structures.

I do not mention in this inventory the materials used in the production of semiconductors, such as fluorine and other various solvents. And there are many of these!

<sup>867</sup> See also this very nice illustrated poster: [The Periodic Table of the Elements](#), in Pictures.

<sup>868</sup> The coltan is the contraction of columbite-tantalite. It is used to recover tantalum and niobium. If it is an important source for tantalum, it is in fact secondary for niobium compared to other minerals. See USGS [Mineral Commodity Summaries 2020](#), the equivalent of the French BRGM (204 pages) that helped me create this part.

We will also not deal with the recycling of quantum computers, an issue that has not yet arisen due to their current very limited number. However, it can be reduced to the more generic issue of recycling various electronic devices.

## Helium

Helium is a great paradox in the table of elements. It is the second most abundant element in the Universe after hydrogen. Nuclear fusion does the rest to create all the other elements in first- and second-generation stars. Yet, this element is quite rare on Earth and its reserves are dwindling. It is a noble, inert gas that does not interact chemically with any other element because its electron layer is complete with two electrons. Lighter than air, it tends to leave the atmosphere. As we have seen in detail in the cryostats section, page 361, helium is used for cooling superconductors and electron spins qubits systems.

As soon as one needs to go below 1K, one must use a mixture of two helium isotopes,  $^4\text{He}$  which is the most common and stable (with two neutrons) and  $^3\text{He}$  which is much rarer (with only one neutron). For cryogenics above 1K,  $^4\text{He}$  is sufficient.

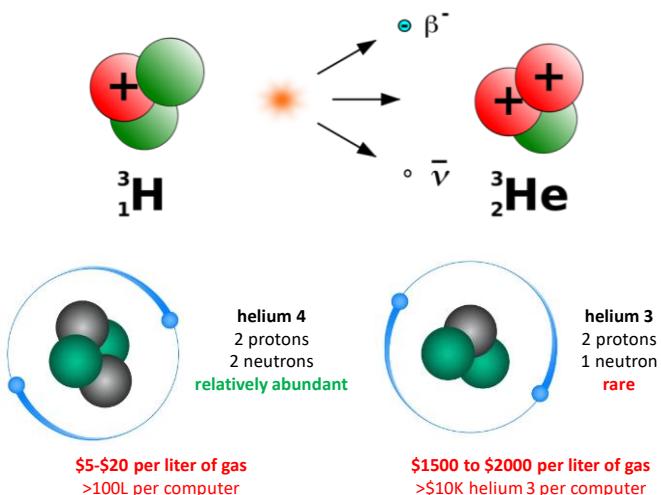
For at least a decade, many specialists have been concerned about a shortage of  $^4\text{He}$  supply. It is commonly used for cooling superconducting magnets in particle accelerators such as the CERN LHC and in MRI scanners or to inflate balloons. It is also used as a neutral gas for the production of semiconductors. Fortunately, new sources of natural gas from which  $^4\text{He}$  can be extracted have emerged, notably in Tanzania and Qatar<sup>869</sup>. But a low annual growth in demand of just 1.6% is too high compared to production forecasts. Air Liquide is one of the major players in this global market, operating a large  $^4\text{He}$  extraction and production unit in Qatar, linked to their gas operations. It seems however that the shortage is temporarily gone<sup>870</sup>.

The  $^3\text{He}$  isotope is rather rare, therefore quite expensive! It was historically a by-product of the storage of tritium-based H-bombs. Tritium gradually disintegrated to produce  $^3\text{He}$ . It was therefore recovered from H-bomb stockpiles! With the reductions in nuclear weapons stockpiles, the production of  $^3\text{He}$  is now coming from specialized nuclear power plants.

Tritium can be produced with irradiating lithium or with tritium-controlled decay in specialized nuclear facilities, such as those controlled by the US Department of Energy. Tritium is an isotope of hydrogen with one proton and two neutrons.

$^3\text{He}$  is produced at the U.S. Department of Energy's Savannah site in South Carolina and at the Canadian CANDU power plant<sup>871</sup>.

The price of  $^4\text{He}$  gas is around €20 per liter while the price of  $^3\text{He}$  gas is between €2K and €3K per gas liter.



<sup>869</sup> See [Helium - Macro View Update](#), Edison Investment Research, February 2019 (21 pages).

<sup>870</sup> See [Helium shortage has ended, at least for now](#), June 2020.

<sup>871</sup> See [Savannah River Tritium Enterprise](#) (4 pages). Helium-3 is also exploited in various specialized applications: in neutron detectors used in security systems, in oil exploration, in medical imaging and in nuclear fusion research. Also see [CANDU Reactor](#), Wikipedia.

A typical dilution-based cryostat requires 15 to 18 liters of  $^3\text{He}$  gas for a little over 100 liters of  $^4\text{He}$  gas! The gases are purchased separately and mixed at the right dosage by the manufacturer of the dry cryostat. At the end, it is therefore necessary to pay at least 30 to 40K€ of  $^3\text{He}$  and  $^4\text{He}$  per dry cryostat.



DoE Savannah River Site in South Carolina



The Tritium Extraction Facility began operating in 2007.

The  $^4\text{He}$  which feeds the pulsed head and passes through the large compressor must be very purified.

France has some  $^3\text{He}$  production capacities located in a CEA nuclear reactor in Grenoble. But it does not necessarily use them for quantum computers because this production is too expensive<sup>872</sup>.

We can also find  $^3\text{He}$  on the surface of the Moon but it is not very practical to extract it and ship it back to Earth even if it is technologically possible<sup>873</sup>! This isotope could be interesting to feed nuclear fusion reactions, pending its complicated technological development.

$^3\text{He}$  is therefore a real bottleneck in the production of superconducting and electron spin quantum computers! It cannot even be avoided for the latter, which requires a temperature of about 1K<sup>874</sup>.

## Silicon

Silicon is the key element in many semiconductor components used in or around quantum processors. While being the second most abundant element in the Earth's crust after oxygen, the silicon used in semiconductors comes from a few quartz mines. This is because quartz is composed of at least 97% silicon, which is easier to refine. After chemical-based refinement, silicon is turned into large cylindrical ingots which are then sliced into thin wafers. Wafers are then processed in semiconductor fabs with transistors that combine silicon oxide and different doping materials such as hafnium.

Silicon qubits require using  $^{28}\text{Si}$ , because the null spin of its nucleus does not interfere with the spin of the trapped electrons used as the qubit observable. The silicon wafers on which the qubits are etched are covered with a thin layer of  $^{28}\text{Si}$ .  $^{28}\text{Si}$  is the most abundant variant of the element while  $^{29}\text{Si}$  represents less than 4%.

$^{28}\text{Si}$  made headlines in 2010 when some German researchers created a perfect crystal ball made of  $^{28}\text{Si}$  to accurately determine the Avogadro number, which determines the number of elements, here atoms, in a mole<sup>875</sup>.

<sup>872</sup> See [Isotope Development & Production for Research and Applications \(IDPRA\), Supply and Demand of Helium-3, 2016, Responding to The U.S. Research Community's Liquid Helium Crisis, 2016 \(29 pages\)](#) and [How helium shortages will impact quantum computer research](#) by James Sanders, April 2019.

<sup>873</sup> See [There's Helium in Them Thar Craters!](#). China is planning to harvest Helium 3 on the Moon.

<sup>874</sup> Helium-4 is used to cool superconducting magnets in MRI systems. It is also used to cool the magnets of the LHC at CERN. The constraints are different: it is just a matter of obtaining superconductivity for the magnets that focus the particle beams. The required temperature is between 1.8K and 4.5K, much "hotter" than the 15 mK of electron-based quantum processors (superconductors, silicon, NV Centers, Majorana fermions). On the other hand, the volumes to be cryogenized are much larger. In some cases, however, the required temperature can fall below 1K, particularly for the search for dark matter. In CERN's LHC, 9 Tesla magnets are cooled to 1.8K with 18 kW cryostats that handle 120 tons of helium 4.

<sup>875</sup> See [An accurate determination of the Avogadro constant by counting the atoms in a  \$^{28}\text{Si}\$  crystal](#) by B. Andreas, 2010 (4 pages). Silicon 28 was obtained by centrifuging silicon fluoride ( $\text{SiF}_4$ ) gas, then transformed into  $\text{SiH}_4$  which was then used to create the crystal by vacuum deposition of purified silicon. All this was carried out in different laboratories in Russia, in Nizhny-Novgorod and Saint Petersburg. The researchers involved also came from Italy, Australia, Japan, Switzerland and BIPM in France, from their respective weights and measures offices.

The tests were carried out on a 5 kg sample at a cost of 1M€. In 2014, an American team improved the purity of  $^{28}\text{Si}$  to 99.9998% with pumping silicon ions in a magnetic field, allowing it to be separated by mass<sup>876</sup>.

This continued in 2017 with 99.999%<sup>877</sup>  $^{28}\text{Si}$  produced by a team of Russian and German researchers. The interest of  $^{28}\text{Si}$  was to allow a precise counting of the number of silicon atoms in the mass considered, because of its perfect crystal structure, dimensioned by X-ray interferometry. The Avogadro number determined by the 2010 experiment was  $N_A = 6.022\ 140\ 84(18) \times 10^{23}$ . The ambition of these two projects was to create a new material standard of the kilogram, the 1889 material standard preserved in France that degrades by oxidation.

Finally, in 2018, the Avogadro number was redefined in the international measurement system as a slightly different constant of  $6.022\ 140\ 76 \times 10^{23} \text{ mol}^{-1}$ . Indirectly, however, these two experiments did advance the know-how of  $^{28}\text{Si}$  purification, at a time when its interest in creating silicon qubits was barely in the radar. What a good illustration of serendipity in science!

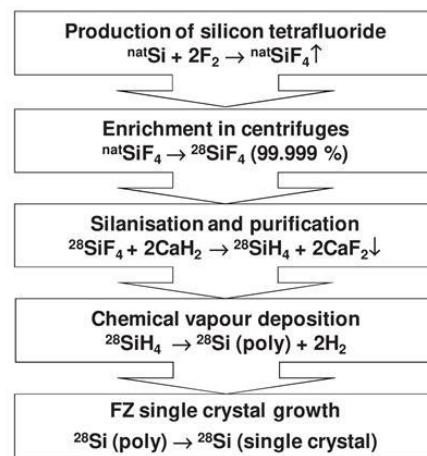
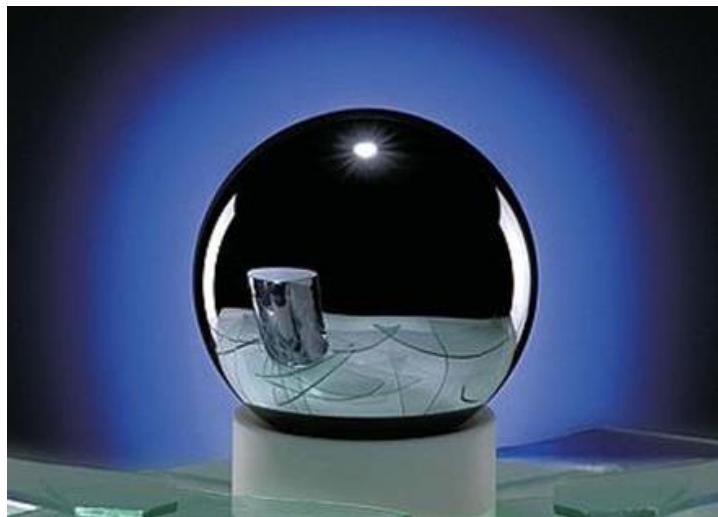


Figure 4. Main technological steps of the  $^{28}\text{Si}$  crystal production (natSi: silicon of natural isotopic composition).

The silicon purification process is complex. It involves the production of silicon tetrafluoride ( $\text{SiF}_4$ ) of all isotopes. Enrichment in  $^{28}\text{Si}$  is carried out in a centrifuge, originally at the Central Design Bureau of Machine Building in St. Petersburg, in fact, a former plutonium enrichment plant reassigned for this use in 2004.

The gas is transformed into silane ( $^{28}\text{Si H}_4$ ) at the **Institute of Chemistry of High-Purity Substances** of the Russian Academy of Sciences in Nizhny-Novgorod. It can then be deposited by vapor deposition (CVD) on silicon, releasing hydrogen. The resulting ingot can then be stretched to create a perfectly crystalline silicon ready to be sliced into wafers. CEA-Leti researchers are also working with Russian teams at Nizhny-Novgorod on the process for vacuum deposition of  $^{28}\text{Si}$  on 300 mm wafers<sup>878</sup>. In October 2021, **Orano** announced its ambition to produce  $^{28}\text{Si}$  in France.

<sup>876</sup> See [Purer-than-pure silicon solves problem for quantum tech](#) by Jonathan Webb, 2014 which refers to [Enriching  \$^{28}\text{Si}\$  beyond 99.9998% for semiconductor quantum computing](#) by K J Dwyer et al, 2014 (7 pages).

<sup>877</sup> See [A new generation of 99.999% enriched  \$^{28}\text{Si}\$  single crystals for the determination of Avogadro's constant](#) by N V Abrosimov et al, 2017 (12 pages) which describes very well the process of purification of  $^{28}\text{Si}$ , the source of the illustration on this page.

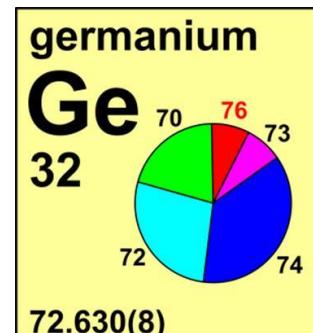
<sup>878</sup> See [99.992% 28Si CVD-grown epilayer on 300 mm substrates for large scale integration of silicon spin qubits](#) by V. Mazzocchi of CEA-Leti and colleagues from France and Russia, 2018 (7 pages).

**Air Liquide** is also partnering with the Nizhny-Novgorod laboratory for this process of CVD (chemical vapor deposition) of  $^{28}\text{Si}$  on a 30 to 60 nm thin film that is 99.992% pure<sup>879</sup> above a conventional silicon wafer. Knowing that Air Liquide also masters the conversion of SiF<sub>4</sub> into silane.

## Germanium

Germanium is a semiconductor metalloid that is part of the III-V family. It is used in many fields: in photonics, in SiGe heterojunction bipolar transistors which are used for the amplification of weak microwave signals as well as in electron spin qubits chipsets.

With spin qubits, it must be isotopically purified to generate  $^{73}\text{Ge}$  which corresponds to 7.36% of its proportion (in purple in the chart *opposite*). It is a stable, natural and non-radioactive isotope. Germanium is generally extracted from zinc ores and also from zinc-copper ores. In 2019, 130 tons of germanium were produced, with China being the main supplier with 85 tons ([source](#)). Data on known reserves are variable and are estimated at approximately 9,000 tons, mainly located in China, Canada and the USA. Along with gallium and indium, which are also III-V materials, germanium is considered a critical resource.



Isotopic purification of germanium is carried out by the same Russian teams at Nizhnii Novgorod as those producing  $^{28}\text{Si}$ . It uses a germanium tetrafluoride centrifugation process similar to the one used to produce germanium tetrafluoride and explained *above*<sup>880</sup>.

## Rubidium

Rubidium is an alkali metal used to create cold atom qubits that are excited into highly energetic Rydberg states. It is also used in quantum sensing, notably to create atomic clocks and micro-gravimeters.

It is an alkaline, soft, silvery metal with a melting temperature of only 39.3°C (*on the right*, in molten state, source [Wikipedia](#)). In a cold atom calculator, the metal is used very sparingly. It is supplied in ampoules of a few solid grams. It is heated in a small box to be sublimated into gas which then feeds the vacuum chamber where the lasers will trap individual atoms. The metal costs about \$85 per gram and about \$1600 per 100g. It is readily available from chemical companies. Only 5 tons are produced annually worldwide, including China, Canada, Namibia and Zimbabwe<sup>881</sup>. It is a by-product of the extraction of cesium and lithium.

The isotope  $^{87}\text{Ru}$  is the most used and represents 27.8% of available rubidium. It is radioactive but with a half-life longer than the age of the Universe, so it is very stable. World reserves are estimated at 100,000 tons, which is enough to keep up with the current rate of production and consumption.

<sup>879</sup> See [Quantum computing: progress toward silicon-28](#), April 2018.

<sup>880</sup> See [Production of germanium stable isotopes single crystals](#) by Mihail Fedorovich Churbanov et al, April 2017 (6 pages).

<sup>881</sup> Each human weighing 70 kg contains about 0.36g of it. However, we are not going to create a variant of Soylent Green to exploit it. Rubidium mining in Canada is carried out by Tantalum Mining Corporation, which belongs to the Chinese group Sinomine Resources since June 2019.



## Niobium

Niobium is a transition metal used in superconducting qubits as well as in microwave cables driving superconducting and electron spin qubits. **Coax Co** (Japan) has a monopoly in the manufacturing of these cable, which are very expensive, about \$3K per half a meter segment. And three are needed per superconducting qubits, positioned between the 4K and 15mK cryostat cold plates.

In industry, it is used in the production of high-strength special steels, in superconducting magnets, in particle accelerators, in arc welding, in bone prostheses associated with titanium, in optics, as a catalyst for rubber synthesis, in aircraft engines and in gas turbines. World production was estimated at 68,000 tons per year in 2018, with Brazil accounting for 88%, followed by Canada for just over 9%, generated by a single mine.

It comes from the exploitation of pyrochlore, an ore combining calcium, sodium, oxygen and niobium.

It is not very expensive and is priced at \$45 per kilogram, but in its ferro-niobium form. The reserves are of 9 million tons, enough to last 130 years at the current rate. But in practice, niobium is considered a "risky" resource because its demand is growing rapidly.

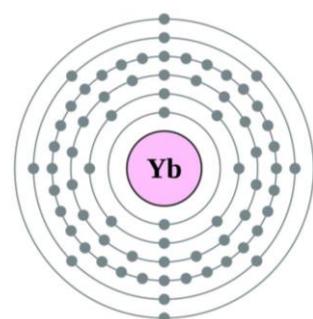


## Ytterbium

Ytterbium is a rare earth of the lanthanide series which is used in trapped ions qubits, quantum memories, atomic clocks, doping of certain lasers and, more rarely, in cold atom qubits.

Otherwise it is used to reinforce certain specialized steels.

The metal is extracted from monazite, a tetrahedral crystalline rock structure of phosphorus oxide associated with various rare earths, which contains only 0.03% of it. Production follows a complex cycle using sulfuric acid and ions exchange. Quantum applications use isotope 171, one of the 7 non-radioactive isotopes of the element. It represents 14% of its proportion in the rocks from which it is extracted. This isotope is probably more expensive than the regular multi-isotope version which is sold between \$500 and \$1K per kilogram.



Approximately 50 tons are produced annually, mainly in China, the USA, Brazil, India and Australia, with reserves estimated at one million tons. Creating trapped ions computers require about one gram per quantum processor.

## **Erbium**

This rare earth of the lanthanide family is used in quantum memories, in some fancy cold atom qubits and in certain lasers (Er:YLF type for yttrium lithium fluoride or Er:YAG type for yttrium aluminum oxide). It is found in some optical fibers used in optical amplifiers.

Finally, it can be used to create vanadium alloys found in cryostats thanks to its high thermal mass heat absorption capacity.

China is the main producer, followed by the USA. It comes from extracting xenotime (phosphate ore) and euxenite (an ore also containing niobium, titanium and yttrium). The ore is processed with hydrochloric or sulfuric acid and then neutralized with soda ash. After a bunch of chemical treatments, erbium ions are extracted by ion exchange on polymer resins.



Erbium is then obtained by heating its oxide with calcium at 1450°C in a neutral argon atmosphere. All this is a long and expensive chemical process, probably polluting of lot but carried out on small volumes. Erbium is produced at a rate of about 500 tons per year. Its price per gram is about \$20, which is quite affordable to integrate it in memories or cold atoms qubits.

## **Strontium**

Strontium is the most common alkali metal used to create trapped ions qubits, with its isotope 87, representing 7% of its five isotopes. It is used as a red dye in fireworks.

Mexico and Germany are the main producers, with an estimated world production of 220,000 tons per year and reserves of over one billion tons. It is notably used in bones anti-cancer radioactive chemotherapies.

Strontium is considered to be toxic. This is the case of all these rare metals which, being pure, oxidize quickly whatever happens. In particular, it explodes when being in contact with water.

## **Gold**

In quantum technologies, gold is mainly used as a thin layer covering the copper plates of the cold plates in cryostats. It prevents copper oxidation and adds good thermal conductivity. The volume used is quite small in relation to gold production and global reserves.

## **Titanium**

Titanium is mainly used in association with niobium in superconducting microwave cables.

In industry, it is used for its resistance to corrosion, particularly in the aerospace industry. Some submarines have an all-titanium hull. Titanium oxide is used as a painting white pigment. It is found in great quantities on Earth since it is the fifth most abundant metal. But only a few ores contain a high enough concentration of it to make its production profitable. The main producing countries are Australia, South Africa, Canada and Norway at a rate of 4.2 million tons per year. Reserves are in excess of 600 million tons.

## **Nitrogen**

Liquid nitrogen is used in cryostats to clean the gaseous helium that feeds them. It is also found in small quantities in NV Centers crystals. It is not a rare commodity. But its production in liquid form is quite energy consuming.

## **Other materials**

Many other relatively common materials are used in quantum technologies.

**Copper** is found in the cryostats cold plates and with some of the various electrical connectors. It is purified at 99.99% to become free of impurities and oxygen (OFHC for oxygen-free high conductivity), in order to improve its thermal conductivity and electrical conductance. It is also widely used in trapped ions chambers. As far as its depletion is concerned, its consumption in quantum technologies is minor.

**Carbon** is exploited in a variety of places, including with carbon nanotubes from C12 Quantum Electronics. This carbon must be purified to keep only its isotope 12.  $^{12}\text{C}$  is acquired in the form of methane in bottles acquired in the USA for \$10K. It is 99.997% purified. The isotopic separation of  $^{12}\text{C}$  uses a chemical process applied to  $\text{CO}_2$ . Carbon is also used in NV centers.

**Aluminum** is used in some superconducting qubits as well as for part of the connector technology in cryostats. It is abundant.

**Manganese** is used in very small quantities as a dopant in some superconducting qubits and can be used with trapped ions qubits.

**Silver** is mainly used in powder form in some heat exchangers in dilution refrigeration systems.

**Iron** is a commodity used in the form of steel in the structure of quantum computers.

**Cesium** is mainly used in atomic clocks, in its isotope 133. Reserves are sufficiently abundant in relation to identified needs. They are mainly located in Canada.

In addition to germanium, **gallium** and **indium** play a key role in III-V components used mainly in photonics. This is one of the few areas of quantum technologies where there is a strong dependence on China as a source of supply.

Finally, **beryllium**, **calcium**, **zinc**, **cadmium** and **mercury** can be used in trapped ion qubits. But the most common are ytterbium and calcium.

Element	Calculation	Sensing and others	Rarity	Cleanliness
Helium 3	Cryostats			
Helium 4	Cryostats	Cryostats		
Silicon 28	Silicon Qubits			
Rubidium	Cold Atoms	Cold Atoms		
Niobium	Cables, supra qubits			
Ytterbium	Trapped ions, memory			
Erbium	Cold atoms, memory			
Strontium	Trapped ions			
Gold	Cold plates			
Titanium	Cables			
Gallium		Photonics		
Germanium		Photonics		
Indium		Photonics		
Nitrogen	Cryostats	NV Centers		
Aluminum	Cryostats, supra qubits			
Silver	Cryostats			
Cesium		Clocks		
Carbon	NV Centers, nanotubes	NV Centers		

# Alternatives to quantum computing

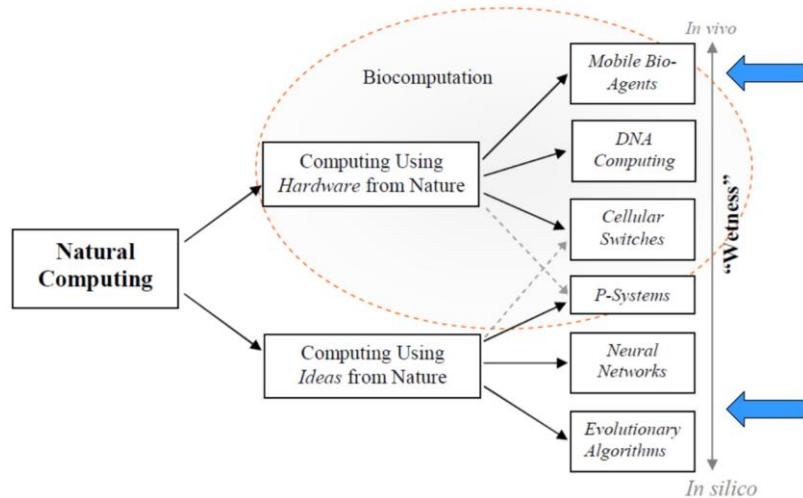
This part consolidates a set of technologies and companies that propose to significantly increase the computing power of computing machines while not relying on the quantum technologies.

We will discuss supercomputers in general, digital annealing which is an alternative to D-Wave quantum annealing, reversible and adiabatic computing, superconducting processors, probabilistic computers and optical coprocessors<sup>882</sup>. Many of these avenues have been explored by major players such as IBM for superconducting components or by startups and with ups and downs.

Some, such as MemComputing and InfinityQ, go so far as to tout exponential computing accelerations on more or less traditional architectures based on classic CMOS components. To the point of proving implicitly that P=NP in complexity theory, i.e. that the class of problems that can be solved in polynomial time with respect to their size is equal to the class of problems that can be verified in polynomial time. The consensus being that P<>NP, this is obviously questionable!

Some of these technologies are part of what is known as **unconventional computing**, i.e. these that differ in one way or another from Turing's machine-based technologies and Von Neumann's architecture based on control units, computing, registers and memory that are the basis of today's classic computers.

These do not all necessarily bring significant computing acceleration competing with quantum computing. This is particularly the case for the different domains that are part of **natural computing** that use physical elements from nature or are inspired by nature<sup>883</sup>. This includes computers based on biological components like DNA, p-systems or membrane computers, spintronics and neuromorphic processors that are adapted to artificial intelligence processing<sup>884</sup>.



Others, such as superconducting classical computing, could be useful to allow quantum computers to "scale". We can therefore also evaluate these different technologies from the point of view of their complementarity, rather than competition, with quantum computing. It explains why this broad topic is incorporated in the [enabling technologies](#) part.

## Supercomputers

The so-called "quantum supremacy" announced by Google in October 2019 systematically referred to power comparisons with supercomputers, in particular with the **IBM Summit** installed at the Oak Ridge laboratory of the US Department of Energy since 2018<sup>885</sup>.

<sup>882</sup> I don't cover analog computing which seems entirely out of fashion. See [Analog Computers](#) by Francis Massen (80 slides).

<sup>883</sup> Schema source: [Unconventional Computing: computation with networks biosimulation, and biological algorithms](#) by Dan Nicolau, McGill University, 2019 (52 slides).

<sup>884</sup> See [Unconventional Computation](#) by Bruce MacLennan, University of Tennessee, who is a reference in the field, October 2019 (306 pages) and [Unconventional Computing](#) by Andrew Adamatzky et al, Springer, 2018 (698 pages).

<sup>885</sup> We'll see in a later part that this comparison was non-sense and was mixing apples and oranges in an unfair way towards the IBM Summit and HPC overall. With factoring-in the noise generated by Sycamore, emulating it requires only the power of a simple PC.

This kind of supercomputer falls within the field of “High Performance Computing”, which we will study briefly here to put it into perspective in relation to quantum computing.

The notion of HPC has not always been well defined, particularly since it is a moving target. The power of a supercomputer from the 1980s is now available in a simple recent server if not in your smartphone. However, it is possible to describe the category with its application requirements. HPC and supercomputers are essentially used for digital simulation and the analysis of complex data. These tools are provided to both researchers, public services and industry for their most advanced computational needs.

HPC are used for weather forecasting<sup>886</sup>, organic and inorganic chemistry simulations, aerospace and automotive simulation, nuclear weapon simulation<sup>887</sup>, in finance, more recently in machine and deep learning and, we tend to forget, also to create computer graphics in movie and TV series productions. The mathematical models used in supercomputers are used in particular to solve partial differential equations and to carry out N-body simulations.

These systems are demanding in several ways: in computing capacity, often evaluated in floating-point operations per second, if possible, in double precision (FLOPS), in data storage capacity, and above all, in the ability to transfer data rapidly between storage, memory and processing units. It is in these areas that supercomputers are most distinct from commodity servers used in data centers.

This table describes the power consumption gap between computing and memory access, which are becoming increasingly expensive the further away memory is from computing.

The ratio goes up to more than 1 to 1000! It explains the attempts to bring memory closer to computing units.

Function	Energy in Picojoules
8-bit add	0.03
32-bit add	0.1
FP Multiply 16-bit	1.1
FP Multiply 32-bit	3.7
Register file access*	6
Control (per instruction, superscalar)	20-40
L1 cache access	10
L2 cache access	20
L3 cache access	100
Off-chip DRAM access	1,300-2,600

source: The End of Moores Law & Future General Purpose Computing and a Road Forward, by John Hennessy 2019 (49 slides)

Historically, supercomputers such as **Cray's** relied on home-grown vector processors and various proprietary massively parallel systems<sup>888</sup>.

These systems have been swept away over the last decade by cluster-based architectures using standard market processors of the CPU type, complemented in recent years by GPGPUs and A100 (in 2020).

<sup>886</sup> As for IBM Weather Channel and its GRAPH (Global Hi-Resolution Forecasting System) forecasting model which is accurate to within 3 km. It is based on an HPC, the Dyeus with 76 nodes of 4 V100 GPUs and 2 Power 9 CPUs. See [High Performance Computing for Numerical Weather Prediction at The Weather Company, an IBM Business](#) by Todd Hutchinson and John Wong, 2019 (18 slides).

<sup>887</sup> This is the role of the supercomputer at CEA-DAM in Bruyères-le-Châtel in the Ile-de-France region, which is fed with data from the Megajoule laser located in Aquitaine.

<sup>888</sup> Cray was acquired by HPE in 2019.

A cluster contains several nodes, each containing several CPUs and/or GPGPUs, themselves multicore, and fast interconnection between these nodes, between clusters, and fast access to data storage, increasingly based on SSDs, which are much faster than hard disks, and at last fast networking access.

Clusters based on standard microprocessors now account for 85% of the 500 largest supercomputers in the world<sup>889</sup>. The CPUs most often come from Intel (Xeon), AMD (Opteron then EPYC), IBM (Power9) while Nvidia dominates the market with its GPGPUs (general purpose GPUs), including the famous V100 generation Volta launched in 2017 and its successor A100 Ampere announced in May 2020. Two thirds of the top HPC now include such Nvidia GPGPUs. This trend accelerated as the OpenMP and OpenACC frameworks were ported to Nvidia GPUs, making these easier to use for a host of existing scientific applications.

This is a form of commoditization of supercomputing, even if these are heavyweight architectures to deploy in large clean rooms. The added value has shifted to the architecture of interconnection, memory and storage, and of course, software.

Interconnection in clusters uses technologies such as Nvidia's NVLink, which connects GPUs and CPUs at high speed. Clusters are interconnected by multiple 200 Gbits/s fiber optic links, often from **Mellanox**, Nvidia's subsidiary since 2019. On a larger scale, HPE is promoting the **Gen-Z** architecture optimized for data access in distributed "data-centric" systems.

Operations on supercomputers are programmed with different development tools. One example is **OpenFOAM**, an open-source SDK used to simulate fluid mechanics, chemical reactions, heat transfer, solid mechanics, electromagnetism and also in finance. And besides **LS-DYNA** for structural simulation. Finally, the parallel application development library for Fortran, C and C++ **OpenMP** is very commonly used for scientific computing, as is **OpenACC**. Let's not forget also that there are many optimization algorithms based on practically acceptable approximations, such as for traveling salesman type problems.

Chinese and Japanese vendors are developing their own custom supercomputers microprocessors, in order to limit their dependence on USA companies. In Japan, the **Fujitsu** Fugaku supercomputer uses Fujitsu A64FX chipsets comprising 52 Arm cores and 32GB of HBM2 memory delivering a nominal power rating of 2.7 TFLOPS (processor layout *below*). The Fugaku, which is not a poisonous fish, has a total of 415 double precision PFLOPS with 396 racks and 152,064 processors. Its installation was completed in June 2020 and enabled Fujitsu to win first place on the podium of the world's most powerful supercomputers ahead of the USA with the IBM Summit<sup>890</sup>.

China's largest supercomputer is the **Sunway TaihuLight** at the National Supercomputing Center in Wuxi. With a capacity of 93 PFLOPS, it uses 40,960 SW26010 256-core 64-bit RISC architecture home-built processors (with simplified instruction set).

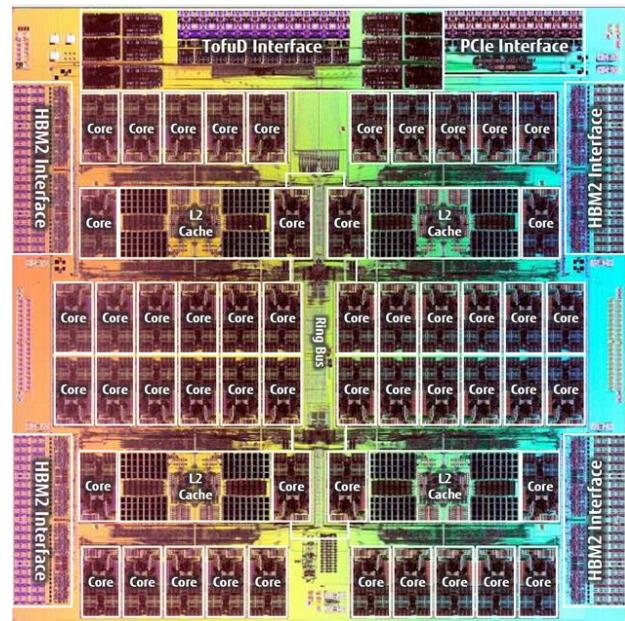
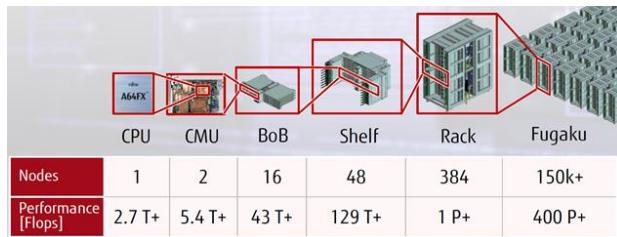
As of mid-2021, China had deployed 37.6% of the world's Top 500 supercomputers, ahead of the USA with 24.4%, but only 4% of the TOP50 for 38% in the USA and 6% for France, which was ahead of China but behind Japan, South Korea, Italy and Germany.

The European Union launched the **EPI** (European Processor Initiative), a project aiming to bring technology independence with supercomputers multicore microprocessors as well as in car embedded systems. It mainly involves German and French players, notably **Atos**.

---

<sup>889</sup> The Top 500 is based on a standardized benchmark, the HPL for High Performance Linpack. It is used to solve a set of linear equations using Gaussian elimination using dense matrices and floating number calculus. See the last published version as of the writing of this ebook: <https://www.top500.org/lists/top500/2021/06/>.

<sup>890</sup> See [Fujitsu and RIKEN Take First Place Worldwide in TOP500, HPCG, and HPL-AI with Supercomputer Fugaku](#), June 2020 and [Japanese Supercomputer Development and Hybrid Accelerated Supercomputing](#) by Taisuke Boku, 2019 (59 slides), [Supercomputer Fugaku](#), 2019 (13 slides) and [The first "exascale" supercomputer Fugaku & beyond](#) by Satoshi Matsuoka, August 2019 (80 slides).



The effort is carried by the startup **SiPearl**, led by Philippe Notton. It is part of the **EuroHPC** project to create pre-exaflops and exaflops supercomputers, including one in Germany and one in France. The planned budget is 1B€, half of which will be allocated evenly between the European Union and its Member States.

In France, the **Jean Zay** supercomputer deployed at GENCI on behalf of the CEA, CNRS and Inria is equipped with 2696 Nvidia V100 GPUs and over 3462 Intel Xeon Cascade Lake CPUs. It is cooled by "hot water", from 30°C to 42°C. It was deployed as part of the French AI plan announced in 2018. Use cases are scientific simulation and machine learning.



Hewlett Packard Enterprise



**HPE SGI machine**  
 >3642 CPU Intel Cascade Lake with 12 and 20 cores  
 2696 GPU Nvidia V100, 1,3 PB SSD storage  
 28 PFLOPS in 2020  
 < 2 MW  
 hot water cooling (32°C-42°C)

The GENCI computing center is due to house a quantum accelerator, probably from **Pasqal**, within a few years. It will be integrated into a hybrid computing architecture. Many other European HPC centers have similar plans, in Germany, Italy and the Netherlands, among others.

Since the advent of the cloud, HPC and supercomputing resources are now available on demand. Cloud data center do not necessarily provide HPC resources. This depends on the servers and clusters deployed architectures and on the packaging of the cloud vendor's offering.

This notion can be associated with the notion of hyperscale, which covers the capacity of a cloud infrastructure to adapt to the increasing customer computing needs.

Machine learning and deep learning applications are the most recent applications implemented on supercomputers, particularly since they are using GPGPUs that run tensors enabling efficient matrix operations, which are very common in neural networks. In practice, however, most supercomputers continue to run scientific simulation applications.

The market for microprocessors dedicated to machine learning and deep learning acceleration has been booming for several years. A wide variety of approaches have been adopted by its vendors.

It can be represented as below on two axis: in the Y axis, the level of cores specialization, and on the X axis, the number of cores.

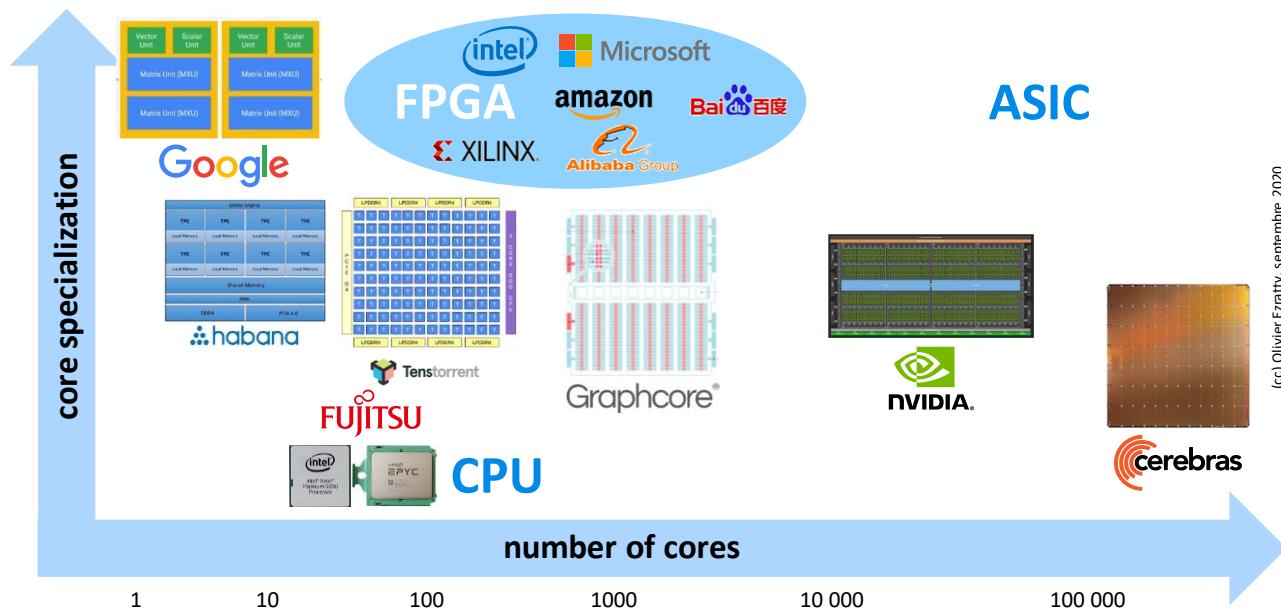
**Google's TPUs** (Tensor Processing Units) are highly specialized for training neural networks, especially convolutional image recognition networks. Nvidia's GPUs contain thousands of classical arithmetic calculation cores as well as hundreds of tensors for matrix computing, which optimizes their versatility.

The most extreme processor is the **Cerebras V2** launched in 2021 with its 850,000 cores. It's a 21 cm square chipset containing a hefty 2.6 trillion 7 nm transistors and 40 GB of integrated SRAM ultra-fast cache memory. Their first version launched in 2019 is already deployed in two test servers at the DoE in the USA with one and two of these chipsets. The first benchmarks published late 2019 did show excellent performance in neural networks training.

Finally, **FPGAs** are dynamically programmable circuits that allow the creation of custom circuits at rather low cost and high flexibility<sup>891</sup>. These are used by some cloud vendors such as Microsoft (with its Brainwave chipsets) and Chinese cloud companies like **Alibaba** and **Baidu**.

Some of these cloud players are developing their own supercomputers. **Google** has created its TPU pods over several generations for its data centers. A TPU v3 board contains four TPU chips, each with two cores, with 16 GB of HBM memory for each TPU core. A TPU v3 Pod has up to 2048 TPU cores and 32 TB of memory.

**Nvidia** integrates its A100 GPUs in SuperPods totaling 140 DGX A100 and 1120 A100 servers and 4 Po of storage, for 700 PFLOPS. These FLOPS are however not necessarily the same as those used to evaluate the TOP 500 supercomputers. Vendor communication is sometimes misleading.

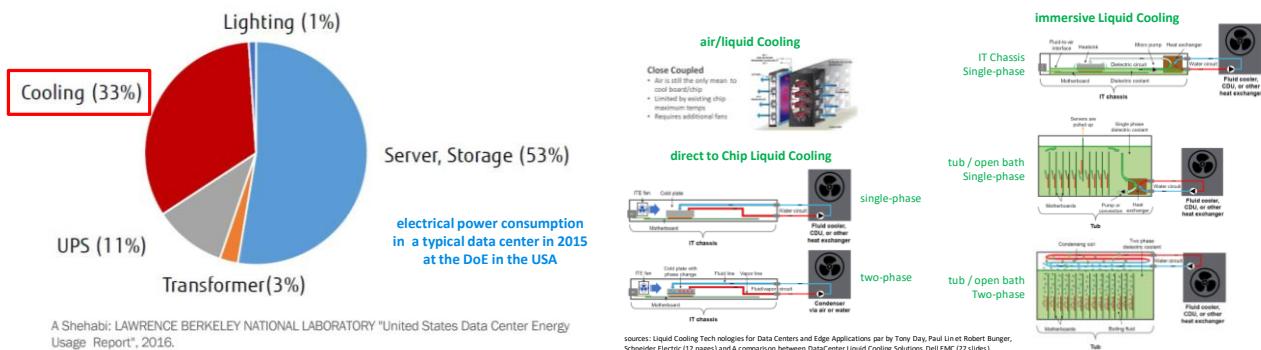


(cc) Olivier Ezratty, septembre 2020

<sup>891</sup> The FPGA market is currently dominated by two vendors: Intel, after its acquisition of Altera in 2015, and AMD, after its acquisition of Xilinx in 2020. In 2019, Xilinx had a 52% revenue market share and Intel about 35%.

Both to improve performance and to reduce energy consumption, there are a number of ways to make these calculations more efficient: **Approximate Computing**, which reduces precision in neural network training and/or inferences without affecting the results, **Quantization**, which switches from floating-point calculations to integer computing during or after training, **Binary Neuron Networks**, which is even simpler with 1 bit output neurons taking us back to the Perceptrons era of 1957 and **Sparse Computing**, which allows computations to occur on compressed representation of matrices, this being useful only for sparse matrices, without prior decompression.

Last but not least, there is the close integration between memory and computing capabilities. For example, the French startup **UpMem** offers DRAM memory modules integrating dozens of RISC-V cores to perform in-memory computing and speed-up certain processes by a factor of 10, particularly for big data applications. It is also possible to tune the cores clock frequency when they are waiting for data from memory.

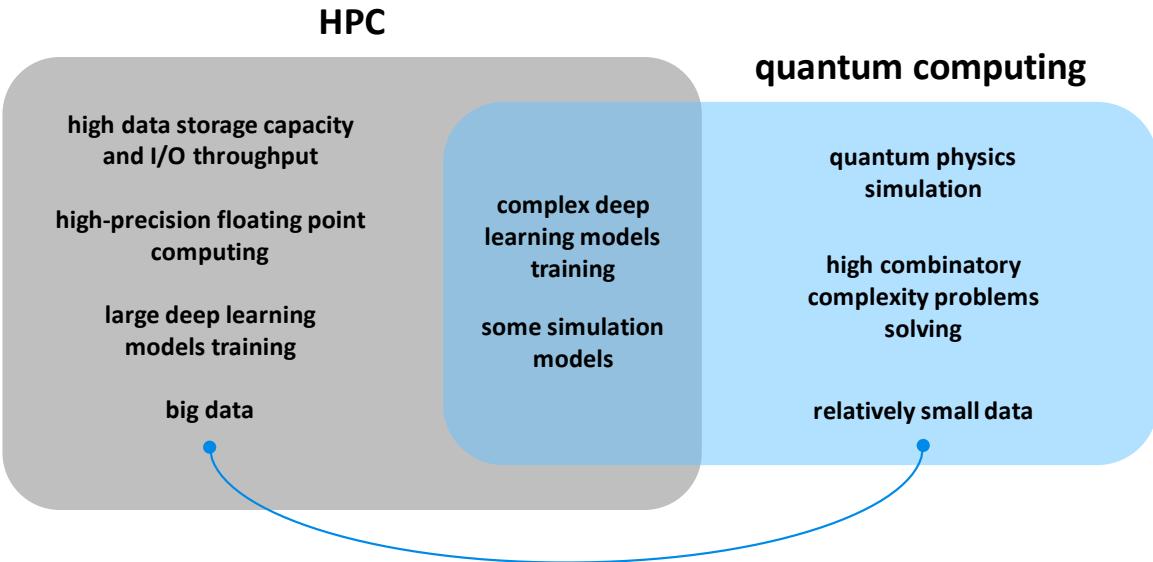


Supercomputers are quite energy hungry. Their increasingly powerful microprocessors consume several hundred of Watts. A third of the electrical energy consumed by a data center is spent on cooling. Specialized server racks now easily consume more up to 30kW. It has now reached the point where liquid cooling is preferred for removing heat from components, usually with water. This provides greater efficiency.

Whatever happens with quantum computers, supercomputers will always be relevant. Applications using large amounts of data are not suitable for quantum computing, even with zillions of qubits. Indeed, data loading time in qubits is a huge bottleneck because it relies on very long series of quantum gates that are not as fast as classical data processing. Applications adapted to quantum computing should not rely on high-volume data feeds. This is the case with weather forecast which requires heavy data sets. It will rely on classical supercomputing for a long time despite some exaggerated claims<sup>892</sup>.

It is used to solve complex problems of combinatorial or minimum energy research. It is likely that for a long time to come we will have hybrid architectures combining classical computers or supercomputers and quantum accelerators. This is the approach adopted by supercomputer suppliers like **Atos**.

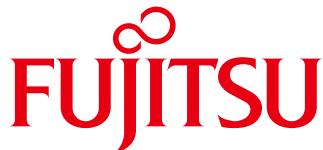
<sup>892</sup> See [Forecasting the Weather Using Quantum Computers](#) by 1Qbit, 2017. The paper references [CES 2019: IBM unveils weather forecasting system, commercial quantum computer](#) by Abrar Al-Heeti, January 2019, which covers two entirely unrelated announcements from IBM, one on weather forecasting using classical computing and another, related to their Q System One, both introduced at CES 2019.



(cc) Olivier Ezratty, 2021

## Digital annealing

Digital annealing is a non-quantum variant of quantum annealing used in D-Wave computers. It has the advantage of exploiting standard component production technologies in CMOS. The level of acceleration provided at the calculation level is not a priori exponential. We have several industry vendors here with **Fujitsu** and **Hitachi**. I have also included here some related solutions coming from **MemComputing** and **InfinityQ**. Let's also mention the support of annealing simulation by the **Atos QLM** with a capacity to handle 50000 variables and an optimized implementation of the SQA algorithm (simulated quantum annealing).



**Fujitsu** announced in early June 2018 a digital annealing computer operating at room temperature. Fujitsu is one of the world leaders in the supercomputer market with IBM, HPE and Atos. It was therefore logical that they explored ways to upscale their HPC offering.

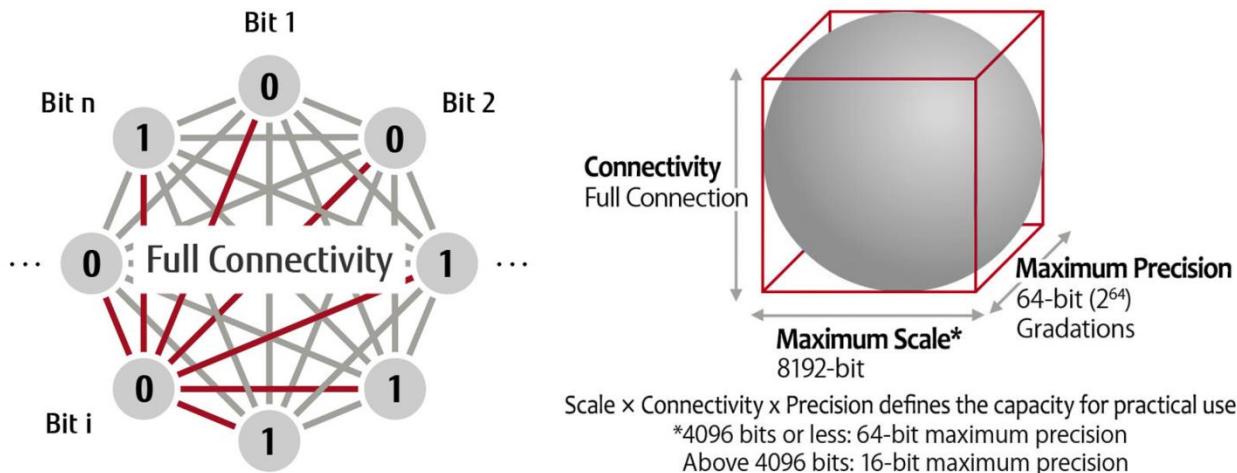
It is supposed to scale much better than D-Wave quantum annealers<sup>893</sup>. The technology is developed on CMOS classical components in partnership with the University of Toronto. It is already proposed as a cloud offering.

It is used to solve optimization problems and to carry out molecule screening in biotechs. The dedicated chipset contains 1,024 bit update blocks incorporating memory to store their weights with a precision of 16 bits, logic blocks to perform value inversions and the associated control circuits. This is reminiscent of memristor-based neural networks. As with D-Wave, problems are loaded into the system in the form of matrices with biases in the links between elements and the system looks for a minimum energy state to solve the problem. It has some familiarity with the Ising model used in D-Wave.



Its designer, **Hidetoshi Nishimori** of the Tokyo Institute of Technology, believes that Fujitsu will be able to create solutions that outperform D-Wave. In 2019, Fujitsu announced its second generation of chips with 8,192 blocks. They expect to reach one million blocks thereafter.

<sup>893</sup> See [Fujitsu's CMOS Digital Annealer Produces Quantum Computer Speeds](#), 2018.



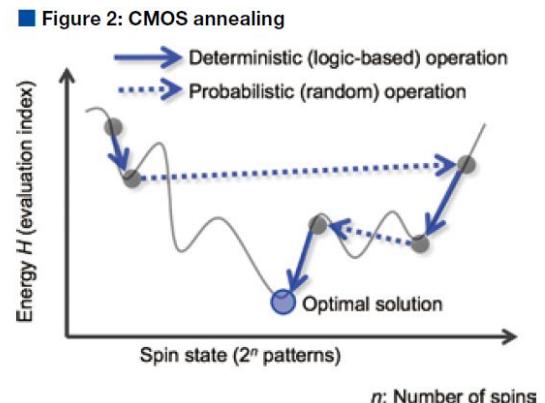
Development tools are provided by **1QBit**, in which Fujitsu has made an investment. Fujitsu has been collaborating since April 2020 with **Quantum Benchmarks** (Canada) on quantum algorithms and error suppression codes, based on an IA Fujitsu algorithm and their experience with their digital annealing<sup>894</sup>. Fujitsu is also partnering with **Entanglement** (USA) which developed a Covid vaccine logistics optimization solution with its annealer.

## HITACHI

Fujitsu is not the only Japanese company exploring digital annealing. Hitachi also launched a related initiative although, contrarily to Fujitsu, it seems it did stay in research lab and didn't reach commercialization.

Their system is implementing a hardware solution to solve Ising models.

It's mixing probabilistic and deterministic approaches running in a CMOS component to find some energy minimum of a combinatorial problem expressed as an Ising model<sup>895</sup>. It doesn't find the absolute minimum to the problem but an acceptable solution. The CMOS uses SRAM to store the virtual "spin states" of the Ising model problem. Hitachi stated that it could help solve combinatorial optimization problems such as the travelling salesman problem efficiently. The architecture was first relying on FPGAs which makes sense given it didn't reach volume production.



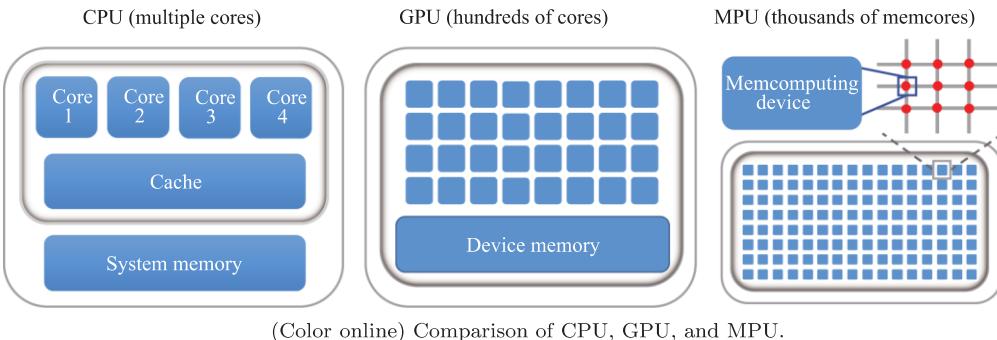
The mysterious startup **MemComputing** (2016, USA) can be positioned in a category close to Fujitsu's offer. It is a solution inspired by quantum annealing computation. They use the principle of invertible computing units, able to circulate data both ways, from input to output and output to input. It also uses oscillating Boolean gates implementing a non-Von-Neumann computing model and some tunnel effect<sup>896</sup>.

<sup>894</sup> See [Fujitsu Laboratories and Quantum Benchmark Begin Joint Research on Algorithms with Error Suppression for Quantum Computing](#), April 2020 and [Fujitsu Laboratories and Quantum Benchmark Begin Joint Research on Algorithms with Error Suppression for Quantum Computing](#) by Fujitsu, March 2020.

<sup>895</sup> See [CMOS Annealing Machine – developed through multi-disciplinary cooperation](#) by Hitachi, Ltd., November 2018, [Overview of CMOS Annealing Machines](#) by Masanao Yamaoka, January 2019 (4 pages) and [CMOS Annealing Machine: an In-memory Computing Accelerator to Process Combinatorial Optimization Problems](#), April 2019.

<sup>896</sup> See [Global minimization via classical tunneling assisted by collective force field formation](#) by F. Caravelli, F. C. Sheldon and L. Traversa, Arxiv preprint, February 2021 (15 pages).

Their hardware solution MemCPU Coprocessor is to place memory next to computing units in processing unit<sup>897</sup>. These memristor-like computing cells have symmetrical inputs and outputs interconnected to neighboring cells.



It computes exclusively with integer numbers. There is no floating-point calculations at all. They would automatically find a complex balance of a parameterized system. This is the principle of SOLGs (Self Organizing Logic Gates) in this diagram<sup>898</sup>.

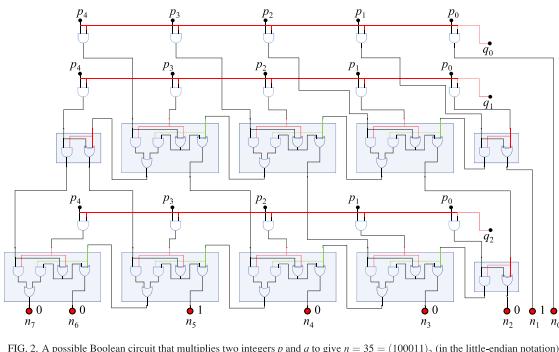


FIG. 2. A possible Boolean circuit that multiplies two integers  $p$  and  $q$  to give  $n = 35 = (100011)_2$  (in the little-endian notation).

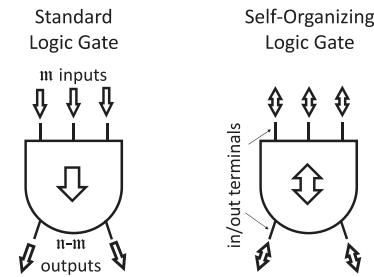


FIG. 3. Left panel: sketch and symbol of a standard  $\mathcal{M}$ -terminal logic gate with  $\mathcal{M}$  inputs and  $\mathcal{N} - \mathcal{M}$  outputs. Right panel: sketch and symbol of the corresponding self-organizing logic gate.

The company was founded by **John Beane**, a serial entrepreneur, with two physics researchers, **Massimiliano Di Ventra** and **Fabio Traversa**, who have done extensive work on memory computing<sup>899</sup>.

Their architecture is supposed to solve various classes of NP-complete and NP-difficult problems in polynomial time such as the 3-SAT problem<sup>900</sup>. They tout significant performance gains such as four orders of magnitude for machine learning applications, i.e. performance multiplied by 10,000!

<sup>897</sup> It is described in [Memcomputing: fusion of memory and computing](#) by Yi Li et al, 2017 (3 pages) where this schema comes from.

<sup>898</sup> SOLGs are described in the patent [Self-Organizing Logic Gates and Circuits and Complex Problem Solving With Self-Organizing Circuits](#), March 2018 (37 pages). It is further detailed in [Coupled oscillator networks for von Neumann and non von Neumann computing](#) by Michele Bonnin, Fabio Lorenzo Traversa and Fabrizio Bonani, Arxiv preprint, December 2020 (29 pages).

<sup>899</sup> See [Universal Memcomputing Machines](#) by Fabio Traversa and Max Di Ventra, 2014 (14 pages) and [Perspective: Memcomputing: Leveraging memory and physics to compute efficiently](#) by Fabio Traversa and Massimiliano Di Ventra, 2018 (16 pages).

<sup>900</sup> See [Memcomputing NP-complete problems in polynomial time using polynomial resources and collective states](#) by Fabio Traversa, Massimiliano Di Ventra et al, 2014 (10 pages) and [Evidence of an exponential speed-up in the solution of hard optimization problems](#) by Fabio Traversa et al, 2018. Then, See this [Conference](#) from Massimiliano Di Ventra at Berkeley in 2016 (26 minutes).

The application domains include the resolution of planning and optimization problems such as the traveling salesman problem, combinatorial<sup>901</sup>, bioinformatics, neural network training<sup>902</sup> and even integer factoring<sup>903</sup>, each time with an exponential gain in computing time compared to traditional computing.

For the moment, their solution is only emulated in conventional computers like with the AMD EPYC microprocessor and provided as an SDK operated in the cloud they have designed in partnership with **Canvass Labs** (2017, USA). Their electronic component is not yet manufactured, even at the prototype stage, and it is not clear whether it is possible to manufacture it.

In particular, they have managed to handle problems such as MIPLIB (Mixed Integer Programming Library), which are considered intractable with a 60-second response time on a server running Linux, and have even beaten a D-Wave. This is used to find a combination of given integers that can generate zero when added together (the "Subset Sum problem"). The startup manages to obtain a quantum scale advantage by emulating its process on traditional processors. This amounts to challenging all current theories of complexity. In short, it makes you dizzy.

In April 2020, MemComputing announced that it would make its XPC (Xtreme Performance Computing) software stack available in the cloud for researchers working on Covid-19<sup>904</sup>.

So, is this technology simply revolutionary and could it nullify many efforts in quantum computing, or are there one or more shortcomings? There are plenty of them. How do you initialize the system so that it is close to a global minimum? What is their real capacity to create these SOLGs in current CMOS components? How is noise managed in their system<sup>905</sup>? Is the system scaling well? Their approach would not be scalable according to several specialists including Scott Aaronson<sup>906</sup>.



**InfinityQ** (2019, Canada, \$1M) is a seemingly promising startup. They state that they have built the “*first quantum computing CMOS microchip technology to work at room temperature*”. Their qubit architecture is “*based on an artificial atom in a lambda configuration*” which “*exploits superposition and entanglement to achieve quantum computing without the burden of maintaining very fragile quantum objects*”.

It is a cloud native platform and quantum analog-computing technology that can run any coding language, any problem up to 100,000x faster than an average laptop, with the same energy consumption as a lightbulb. Their first-generation machines can solve complex optimization problems, linear system and FFTs (fast Fourier transforms). That's quite a heavy stack of promises.

They created a proof of concept with 10 qubits late 2020 and are announcing a 100 qubits MVP in 2021 and full commercialization after 2025. In April 2021, they mentioned that they had solved a traveling salesperson problem with 128 cities while other “*non-classical machines*” have solved a maximum of 22 cities. This system is currently programmed in C language.

---

<sup>901</sup> See [Stress-testing memcomputing on hard combinatorial optimization problems](#) by Fabio Traversa, Massimiliano Di Ventra et al, 2018 (6 pages).

<sup>902</sup> See [Accelerating Deep Learning with Memcomputing](#) by Haik Manukian, Fabio Traversa and Massimiliano Di Ventra, 2018 (8 pages).

<sup>903</sup> See [Polynomial-time solution of prime factorization and NP-hard problems with digital memcomputing machines](#) by Fabio Traversa and Massimiliano Di Ventra, 2017 (22 pages).

<sup>904</sup> See [MemCPUXPC SaaS Platform available free for COVID-19 Research](#), 2020.

<sup>905</sup> They provide an answer in [Directed percolation and numerical stability of simulations of digital memcomputing machines](#) by Yuan-Hang Zhang and Massimiliano Di Ventra, April 2021 preprint on Arxiv (12 pages).

<sup>906</sup> See [A Note on 'Memcomputing NP-complete problems' and \(Strong\) Church's Thesis](#) by Ken Steiglitz, 2015 (2 pages) which quickly demonstrates that this is not possible. The same goes for [Memrefuting](#) by Scott Aaronson in 2017 and for [A review of Memcomputing NP-complete problems in polynomial time using polynomial resources](#) by Igor Markov, 2015 (3 pages).

The company is run by Aurelie Hélouis (CEO) and Kristina Kapanova (CTO) and is backed by Philippe Dollfus, a CNRS Research Director in France who is specialized in computational nanoelectronics and John Mullen, former Assistant Director of the CIA. They also make business claims such as having projects starting with major unnamed UK and Canada banks, with a Swiss pharmaceutical and the Canadian government.

So, how can this feat be accomplished<sup>907</sup>? How is it different than what MemComputing is doing? They share some similarities: use CMOS components and solve complex problems in a polynomial way. The difference seems that MemComputing is using an invertible digital logic while InfinityQ is based on some analog processing. It also looks like an analog annealing system, which could also be compared with Fujitsu digital annealers. Their technology could be classified as some sort of reservoir computing running on CMOS doing rabi flops emulation<sup>908</sup>. All in all, their quantum, superposition and entanglement claims seem overexaggerated. At this point, we need more documented benchmarks and peer reviews to build any sound opinion on InfinityQ.

## Reversible and adiabatic calculation

Since the 1960s, researchers have been considering reducing computer power consumption by several orders of magnitude based on the principle of adiabatic reversible computing<sup>909</sup>.

The goal is primarily energy-based. It does not accelerate computing. In most cases, it is even contradictory with Moore's law, as the main techniques used result in a calculation speed decrease.

All this is due to our understanding, since the 1960s, of the link between computation and thermodynamic processes. **Rolf Landauer** created in 1961 the equation according to which the process of information processing that dissipates energy is related to memory erasure<sup>910</sup>. The erased information is turned into heat sent outside the computer, increasing the environment entropy. Rolf Landauer estimated that the dissipated energy was always greater than  $kT\ln(2)$  per erased bit, k being Boltzmann's constant ( $1.38 \times 10^{-23}$  J/K), T the temperature in Kelvin and  $\ln(2)$  the logarithm of 2 (about 0.69315). At room temperature, this gives 0.017 eV. This is the famous Landauer limit<sup>911</sup>.

More generally, Landauer's limit illustrates the link between the notions of logical and physical reversibility of computation. The first is linked to the ability to determine the input values of a calculation according to the output values.

The second is that the unfolding of a physical process in reverse may not violate the laws of physics, including the inescapable second law of thermodynamics according to which the entropy of a thermodynamic system always increases unless the process is reversible.

---

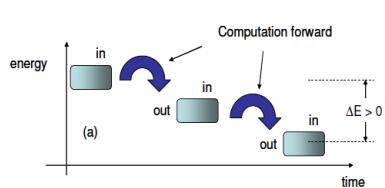
<sup>907</sup> See a [video of their presentation](#), December 2020 (17 mn).

<sup>908</sup> See [Quantum reservoir computing with a single nonlinear oscillator](#) by L. C. G. Govia et al, Raytheon, January 2021 (9 pages).

<sup>909</sup> To write this part, I used the many references from the excellent presentation [Reversible Adiabatic Classical Computation - an Overview](#) by David Frank, 2014, IBM (46 slides) from which the illustration on this page comes from, as well as from [The Future of Computing Depends on Making It Reversible](#) by Michael P. Frank, 2017 and [The Case for Reversible Computing](#) by Michael P. Frank, 2018 (19 pages). See also [Computers That Can Run Backwards](#) by Peter Denning and Ted Lewis, 2017 and [Theory of Reversible Computing](#) by Kenichi Morita, 2017 (463 pages). See also the review paper [Quantum Foundations of Classical Reversible Computing](#) by Michael P. Frank and Karpur Shukla, April 2021 (70 pages).

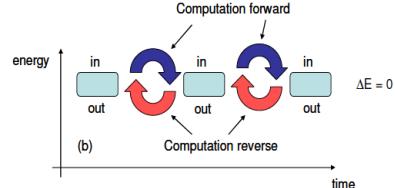
<sup>910</sup> See [Irreversibility and heat generation in the computing process](#) by Rolf Landauer, in IBM Journal of Research & Development, 1961 (9 pages).

<sup>911</sup> Landauer's limit was experimentally verified fifty years later, in 2011, by a team from ENS Lyon in Sergio Ciliberto's group. See [Experimental verification of Landauer's principle linking information and thermodynamics](#) by Antoine Bérut et Al, 2011 (4 pages) and [Information and thermodynamics: Experimental verification of Landauer's erasure principle](#) by Antoine Bérut, Artyom Petrosyan and Sergio Ciliberto, ENS Lyon, 2015 (26 pages). Other experiments followed to validate this, with magnetic memories, such as [Experimental test of Landauer's principle in single-bit operations on nanomagnetic memory bits](#) by Jeongmin Hong et al, 2016 (6 pages). The principle consists in lowering the energy barrier of the bit state transition when an operation is required and then to raise it again to preserve the bit state. See also Delft's 2018 experiment in [Quantum Landauer erasure with a molecular nanomagnet](#) by R. Gaudenzi et al, 2018 (7 pages).



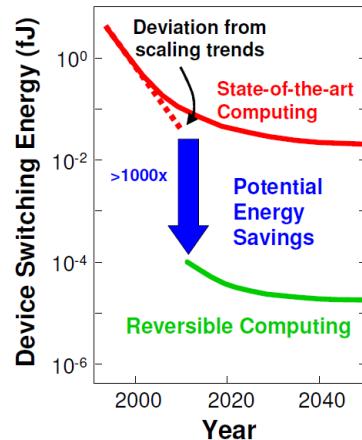
### Traditional CMOS

- Every computing operation uses unrecoverable energy
- Input information is lost at output, the process is non reversible



### Reversible Logic

- Output information is fed back to input
- Computational process is reversible
- Computation energy oscillates between input and output



Today, a CMOS component spends 5000 eV energy to erase one bit, almost 300,000 times more than the Landauer's limit. One could gain an order of magnitude and go down to 500 eV, but that would still be 30,000 times more than the Landauer limit. So, in order to reduce the computing energy consumption, why not avoid erasing information and, in the process, make all computing physically and logically reversible?

This would require a review of all current computational logic that relies at low-level on irreversible logic gates that destroy information, such as NAND or XOR gates that generate one bit from two bits.

In 1973, **Charles Bennett**, another IBM researcher and colleague of Rolf Landauer's, imagined a calculation method that would avoid this energy-dissipating erasure of information without requiring an infinite memory<sup>912</sup>.

He was followed by **Edward Fredkin** and **Tommaso Toffoli** who, in 1978 and 1982, imagined reversible logical gates inspired by a metaphorical physical model based on billiard balls, the BBM for billiard ball model<sup>913</sup>. These logic gates have as many outputs as inputs and it is easy to understand why they become reversible. Although their model was not practically feasible with contemporary electronics, it was then applied to the quantum equivalent of these gates that we already covered.

**Konstantin Likharev** proposed in 1976, then in 1982, to implement this reversible computational logic by manipulating the energy levels of superconducting Josephson junctions, under the name of "parametric quantrons"<sup>914</sup>. In 1991, this became the "quantron flux parametron" (QFP), capable of operating up to 10 GHz and developed by a Japanese team<sup>915</sup>.

This led then in 2003 to **Vasili Semenov**'s idea to use nSQUID circuits to realize these circuits, the n meaning "negative" because of a negative inductance that connects two SQUIDs of the device. As for any Josephson junction, it works under cryogenic temperature<sup>916</sup>.

<sup>912</sup> See [Logical reversibility of computation](#) by Charles Bennett, IBM Journal of Research and Development, 1973 (8 pages). Charles Bennett is also the creator of BB84 codes with Georges Brassard, which laid the foundations of quantum key distributions.

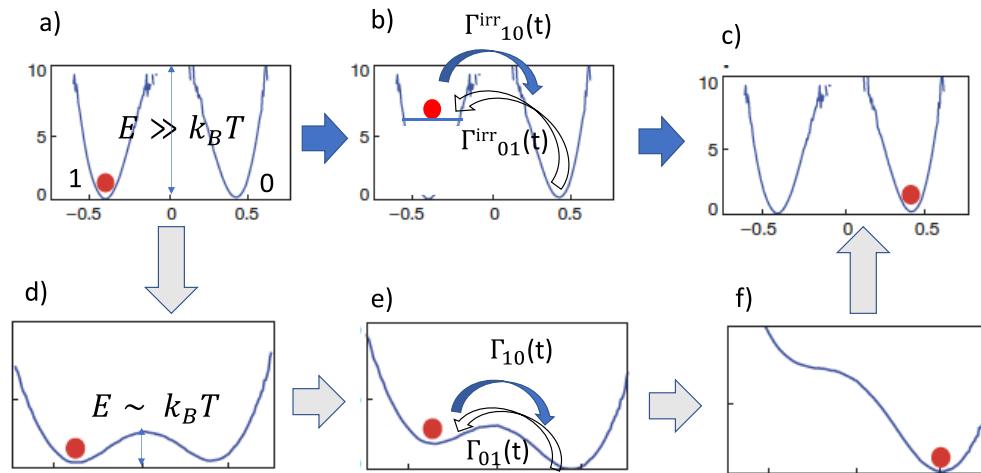
<sup>913</sup> See [Conservative Logic](#) by Edward Fredkin et Tommaso Toffoli, International Journal of Theoretical Physics, 1982 (35 pages).

<sup>914</sup> He tells this story in [Josephson Digital Electronics in the Soviet Union](#) by Konstantin Likharev, 2012 (18 slides).

<sup>915</sup> See [Quantum Flux Parametron: A Single Quantum Flux Device for Josephson Supercomputer](#) by Mitsumi Hosoya et al, June 1991.

<sup>916</sup> See an explanation of the process in [Engineering and Measurement of nSQUID Circuits](#) by Jie Ren, 2012 (26 slides). nSQUIDS are double SQUIDs connected by a negative inductance. SQUID = Superconducting Quantum Interference Device, a system used to accurately measure the magnetism of superconducting Josephson effect loops. These nSQUIDS were manufactured by Hypres.

Reversible computing is often associated with adiabatic computing but one could work without the other. The general principle of adiabatic computing is illustrated *below*: in a classical calculation, the energy barrier to switch the state of a system between a) and c) is high. In a quasi-adiabatic calculation, a physical system lowers the state energy transition barrier (in d) to trigger it (in e) and then in f, by raising the level of the barrier to its normal state<sup>917</sup>.



The processing energy cost is thus lowered by approaching Landauer's limit. The high level of the non-computation barrier guarantees the stability of the information managed outside of this operation. Lowering the barrier and raising it are often managed by trapezoidal voltage control of the transistors instead of looking like a square wave signal.

Between 1985 and 1993, reversible or partially reversible CMOS and CCD computing components were designed.

**Craig Lent** then proposed in 1997 an adiabatic computation system based on quantum dots and cellular automata (QCA for Quantum dots Cellular Automata) to operate up to 100 GHz<sup>918</sup>.

In the same manner, **Krishna Natarajan** suggested in 2004 to use MEMS (electro-mechanical components) to drive the trapezoidal voltage control necessary to create adiabatic CMOS components with a very low energy dissipation of 1 eV<sup>919</sup>.

The idea was pursued by a team from **CEA-Leti** and **Delft** in the Netherlands in 2017 and **Ralph Merkle** in 2019, with prototype circuits based on this kind of technology<sup>920</sup>.

In 2012, **Alexei Orlov** et al. experimentally validated Landauer's limit and, above all, the possibility of overcoming it (from below) with reversible calculation, all with a few discrete classical electronic components, resistors and capacitors<sup>921</sup>. Their experiment showed that a bit copy or erasing with copy could be done with an energy lower than Landauer's limit, at the price of slowing down the operation.

---

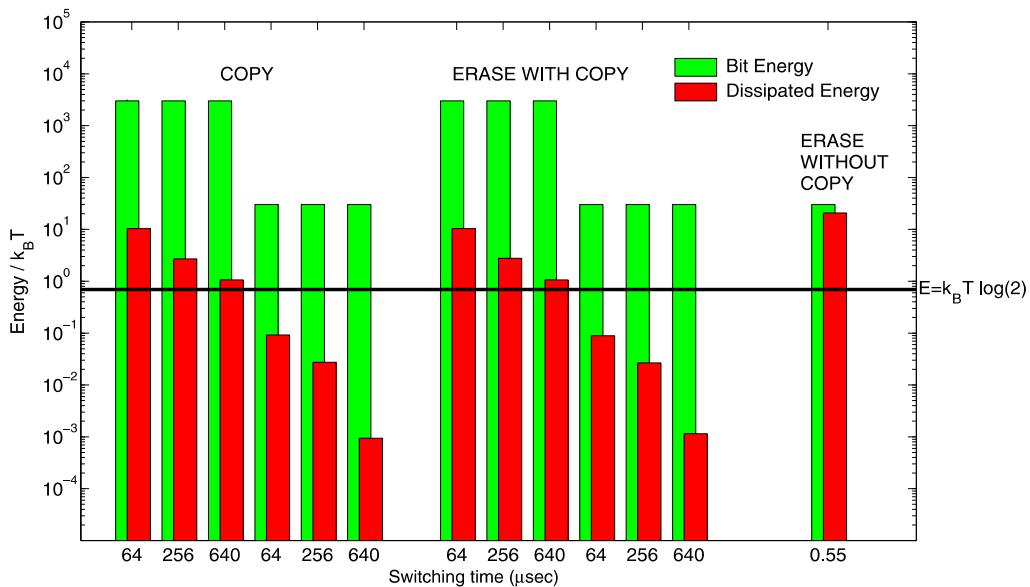
<sup>917</sup> Source: "Thermodynamics of computing, from classical to quantum" by Alexia Auffèves, May 2020 (11 pages), adapted from [Experimental verification of Landauer's principle linking information and thermodynamics](#) by Antoine Bérut et Al, 2011 (4 pages).

<sup>918</sup> See [A Device Architecture for Computing with Quantum Dots](#) by Craig Lent and Douglas Tougaw, 1997 (17 pages).

<sup>919</sup> See [Driving Fully-Adiabatic Logic Circuits Using Custom High-Q MEMS Resonators](#) by Krishna Natarajan et al, 2004 (7 pages).

<sup>920</sup> See [Adiabatic capacitive logic: A paradigm for low-power logic](#) by Gaël Pillonnet et al, CEA-Leti, 2017 (5 pages) and [Mechanical Computing Systems Using Only Links and Rotary Joints](#) by Ralph Merkle et al, 2019 (34 pages).

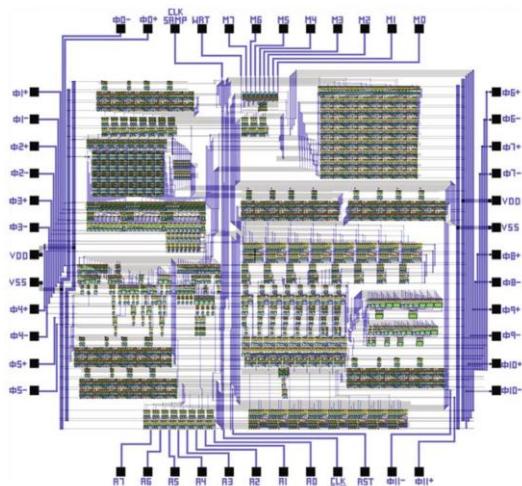
<sup>921</sup> See [Experimental Test of Landauer's Principle at the Sub-kBT Level](#) by Alexei Orlov, Craig Lent et al, 2012 (5 pages).



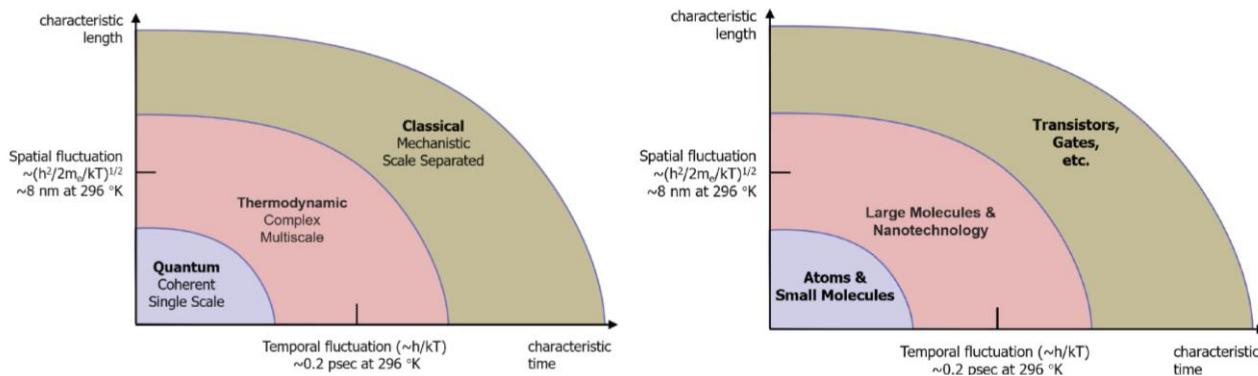
Pure and simple erasing did consume more energy than Landauer's limit. The model was safe! And it all worked at room temperature. In 2019, Alexei Orlov's team from Notre Dame University in Indiana produced the equivalent of an 8-bit microcontroller using a subset of a RISC-type MIPS instruction set with 5766 transistors, 40% of which are adiabatic (*opposite*)<sup>922</sup>. This seems to be, to date, the most successful realization of a reversible adiabatic processor. It remains however experimental and far from industry requirements. Its industrialization could be of interest to create microcontrollers for low-power connected objects.

However, this adiabatic CMOS technique requires a larger number of transistors. Therefore, emerges a new trade-off between a larger and more expensive to design and manufacture power saving component vs cheaper but more energy hungry conventional counterparts.

Still, the environmental cause has recently revived interest in reversible and adiabatic computing. It is promoted by the Computer Community Consortium group of the American **Computing Research Association** with the lead from Michael P. Frank's team at **Sandia National Labs**<sup>923</sup>.



They position it in an intermediate architecture between classical and quantum computing, but on quantities that are not necessarily relevant (dimension of components and duration of state fluctuation, see the diagram *below*)<sup>924</sup>. The purpose of the manifesto is to obtain US federal credits to finance this research. So, the story is not over!



## Superconducting processors

The idea of creating superconducting computers capable of taking advantage of the lack of resistance of low temperature electronic components dates back to the early 1960s. Its history evolves in parallel with reversible and adiabatic computing. It started with the discovery of the Josephson effect in 1962. This effect was later used to create two-states superconducting qubits with research starting in the early 1980s.

The expected benefits of superconducting transistors are an increase in clock frequency and a decrease in power consumption<sup>925</sup>! The gain is more significant with the clock frequency than with energy consumption. For example, in a Japanese SFQ component realized in 2019, the clock was 32 GHz while the power drain was 2.5 TOPS per Watt, in the average of most deep learning CMOS chipsets<sup>926</sup>.

Several generations of superconducting components have been developed over time<sup>927</sup>:

- **SFQ** (Single Flux Quantum) was a first-generation circuit, limited to a 1 GHz and 300 MHz clock frequency. Work started at IBM in the 1960s. They had invested the equivalent of \$100M today in a program that was partly funded by the NSA and which was abandoned in 1983 which are also based on the Josephson effect<sup>928929</sup>. D-Wave's superconducting qubit use SFQ-type components for generating and reading qubit control signals (DAC and ADC)<sup>930</sup>.

<sup>924</sup> See [Quantum Foundations of Classical Reversible Computing](#) by Michael P. Frank and Karpur Shukla, April 2021 (70 pages).

<sup>925</sup> See this very interesting presentation on [superconducting](#) components: [Superconducting Microelectronics for Next-Generation Computing](#) by Leonard Johnson, November 2018 (27 slides). The gain in power consumption would be between 10 and 1000. The integration level is currently low, of the order of 200 nm compared to 7 nm for the densest CMOS processors. But it is steadily increasing. There are even investigations to combine superconducting transistors, optoelectronics and neural networks. See [Superconducting Optoelectronic Loop Neurons](#) by Amir Jafari-Salim, 2018 (48 pages).

<sup>926</sup> See [29.3 A 48GHz 5.6mW Gate-Level-Pipelined Multiplier Using Single-Flux Quantum Logic](#) by Ikki Nagaoka et al, 2019.

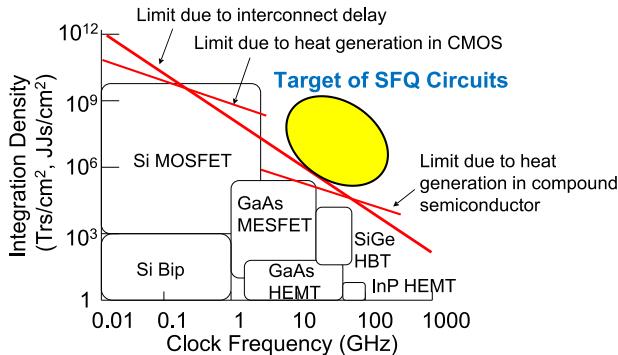
<sup>927</sup> See [Single Flux Quantum \(SFQ\) Circuit Fabrication and Design: Status and Outlook](#) by V. Bolkhovsky et al, Lincoln Laboratory at MIT, 2016 (34 slides) and [Cryogenic Electronic and Quantum Information Processing](#), IEEE, 2018 (67 pages) which provides a good overview of the various SFQ technologies around.

<sup>928</sup> See [The Long Arm of Moore's Law: Microelectronics and American Science](#) by Cyrus Mody, 2017 (299 pages), page 58.

<sup>929</sup> Source of the schematic that positions SFQs in terms of clock speed and integration compared to traditional components: [Impact of Recent Advancement in Cryogenic Circuit Technology](#) by Akira Fujimaki and Masamitsu Tanaka, 2017 (37 slides).

<sup>930</sup> See [Architectural considerations in the design of a superconducting quantum annealing processor](#) by P. I. Bunyk et al from D-Wave, 2014 (9 pages).

## Appealing Feature of SFQ Circuits



### RSFQ - Rapid Single Flux Quantum

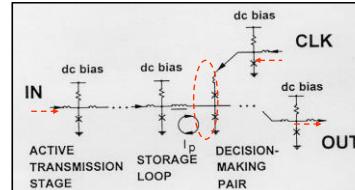
#### Timeline:

invented in 85-86, generally accepted in 90, adopted in the US in 91, became the main digital superconducting electronics by mid-end of 90s, first product by mid-00s

$$\int V dt = \Phi_0 = h/2e = 2.07 \text{ mV}\cdot\text{ps}$$

$$E_{SFQ} = 10^{-19} \text{ J}$$

Both Data and Clock are SFQ voltage pulses  $V(t)$  with quantized areas



- 750 GHz digital frequency divider demonstrated
- internal memory
- gate-level pipelining
- high-throughput
- low switching power
- dc bias only
- local timing
- amenable for synchronous and asynchronous schemes

- **RSFQ** (Rapid Single Flux Quantum) was invented in Russia in the mid-1980s and made from niobium and aluminum. It was then adopted in the USA in 1991 and the first ones were produced in the mid-2000s<sup>931</sup>. They have the advantage of being able to operate up to 750 GHz. They can be used to create ALUs (Arithmetic Logic Units<sup>932</sup>) running at 20/30 GHz as well as ADCs (analog to digital converters) running up to 40 GHz<sup>933</sup>. In RSFQ logic, binary information is managed in the form of quantum states of the Josephson junction flux, which is transferred as voltage pulses<sup>934</sup>. However, the technology does not use state superposition and entanglement as in superconducting qubits.

**Hypres** develops radio frequency reception systems using two superconducting components: **SQUID** (Superconducting Quantum Interference Device) based antennas that allow to capture magnetism with precision (invented in 1964) and an RSFQ chipset running at 30 GHz with 11K JJ (Josephson junctions)<sup>935</sup>!

- **AQFP** (Adiabatic Quantum Flux Parametron) which comprises two superconducting Josephson loops connected together by an inductance, reminiscent of the nSQUID principle<sup>936</sup>. The process is very energy efficient due to its ability to be reversible. A recent work from Japanese researchers prototypes a AQFP processor using 20,000 Josephson gates operating at 4.2K<sup>937</sup>.
- **RQL** (Reciprocal Quantum Logic)<sup>938</sup>, **eRSFQ** (Energy Efficient RSFQ) and **eSFQ** (Energy Efficient SFQ) are variants of the RSFQ that are more energy efficient due to the absence of bias resistance, replaced by an inductance. This is the variant chosen by Hypres and its subsidiary SeeQC. Their SFQs combine eRSFQs, of which they are the originators, and eSFQs. RQLs are studied to create superconducting memories.

<sup>931</sup> Source: [Single Flux Quantum Logic for Digital Applications](#) by Oleg Mukhanov of SeeQC/Hypres, August 2019 (33 slides).

<sup>932</sup> See for instance [gBSA:Logic Design of a 32-bit Block-Skewed RSFQ Arithmetic Logic Unit](#), 2020 (3 pages).

<sup>933</sup> This would be very useful to generate the microwaves to drive superconducting and silicon qubits.

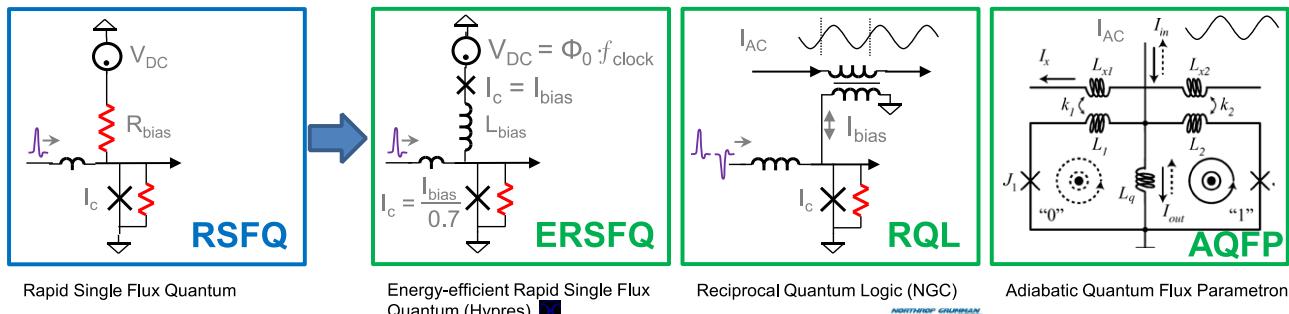
<sup>934</sup> Time management in logic programming must take this into account. On this topic, see [A Computational Temporal Logic for Superconducting Accelerators](#) by Georgios Tzimpragos et al, 2020 (14 pages).

<sup>935</sup> See [Superconducting Quantum Arrays for Wideband Antennas and Low Noise Amplifiers](#) by Oleg Mukhanov et al, 2014 (36 slides).

<sup>936</sup> See [Adiabatic Quantum-Flux Parametron: Towards Building Extremely Energy-Efficient Circuits and Systems](#), by Olivia Chen et al, 2018 (10 pages) and [Design and Implementation of a Bitonic Sorter-Based DNN Using Adiabatic Superconducting Logic](#) also from Olivia Chen et al, 2019 (24 slides).

<sup>937</sup> See [MANA: A Monolithic Adiabatic iNtegration Architecture Microprocessor Using 1.4-zJ/op Unshunted Superconductor Josephson Junction Devices](#) by Christopher L. Ayala et al, December 2020 (14 pages). They provide some impressive cryogenic needs for using this technology at a supercomputing scale.

<sup>938</sup> See [Ultra-Low-Power Superconductor Logic](#) by Quentin P. Herr et al, 2011 (7 pages).



- **SFETs** (Superconducting FETs, Field Effect Transistors) which implement a concept similar to adiabatic CMOS, but with a superconducting component. These components have been developed since the 1980s<sup>939</sup>.

There are a few other variants of superconducting components that I will just mention (SSV, SVJJ, STTJJ, S3JJ) because they do not seem to be common, on top of JMRAM that is investigated for implementing superconducting memory.

To date, the integration record for this type of component is only 144,000 Josephson junctions in a chipset, realized in a 248 nm integration<sup>940</sup>.

In the mid-2000s, the **NSA** invested \$400M in the RSFQ over the 2005-2010 period. Its goal was to create a processor with one million logic gates running at 50 GHz. The NSA document describing the project is surprisingly detailed and highly informative.

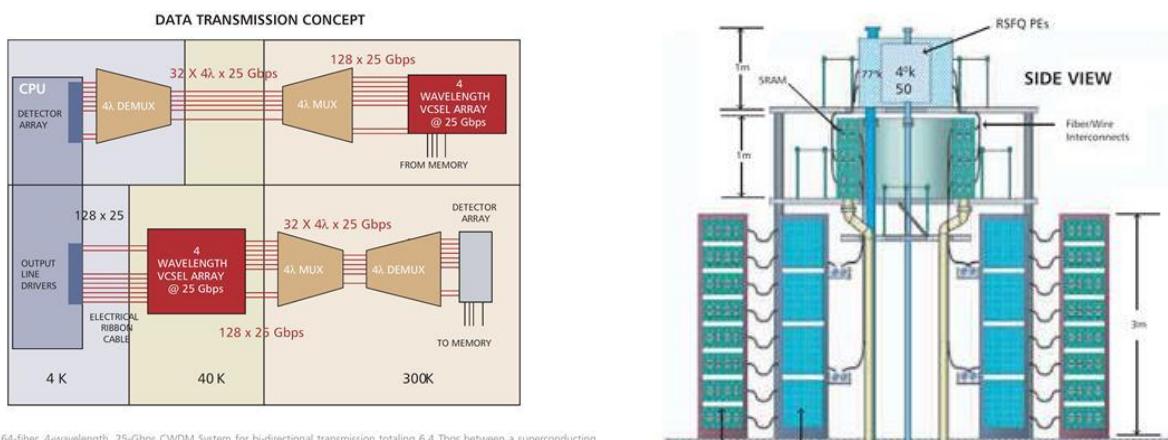


Figure 5-1. A 64-fiber, 4-wavelength, 25-Gbps CWDM System for bi-directional transmission totaling 6.4 Tbps between a superconducting processor at 4 K and high speed mass memory at 300 K. Optical connections are shown in red, electrical in black. This technology should be commercially available for 300 K operation by 2010.

It reveals the scope of the related technological challenges<sup>941</sup>. In particular, for creating cryogenic memories, superconducting or not: CMOS-Josephson junction hybrid, SFQ or monolithic RSFQ-MRAM. Then the communication between the cryogenic electronics and room temperature components, with a 25 Gbits/s optical fiber that we would probably now reach 100 or 200 Gbits/s, leaving aside the question of the optical signal modulation and demodulation. Cryogenics must be sized to support a large number of components.

<sup>939</sup> See [Josephson Junction Field-effect Transistors for Boolean Logic Cryogenic Applications](#) by Feng Wen, 2019 (7 pages) and [Superconducting silicon on insulator and silicide-based superconducting MOSFET for quantum technologies](#) by Anaïs Francheteau, 2017 (153 pages).

<sup>940</sup> See [Advanced Fabrication Processes for Superconducting Very Large Scale Integrated Circuits](#) by Sergey K. Tolpygo, 2015 (43 slides).

<sup>941</sup> See [NSA Superconducting Technology Assessment](#), 2005 (257 pages). The document is quite old but still very well crafted and interesting.

For testing purpose, a simple pulsed head is sufficient but more imposing installations are planned as power would grow, as in the illustration *below on the right*.

The project relied mainly on **Hypres**, the only American company entirely dedicated to the creation of superconducting components, who runs its own foundry since 1983. They were supplying radio frequency components for military use cases. In particular, they developed an 8-bit RSFQ processor and 28,000 Josephson junctions.

There is also **Northrop Grumman** with its foundry located in Linthicum, Maryland. Finally, **Chalmers University** in Sweden and various research laboratories in the USA (JPL, Berkeley, Stony Brook) as well as the **NIST** Boulder laboratory were also involved.

TABLE 2-2. SUPERCONDUCTOR RSFQ MICROPROCESSOR DESIGN PROJECTS					
Time Frame	Project	Target Clock	Target CPU Performance (peak)	Architecture	Design Status
1997-1999	SPELL processors for the HTMT petaflops system (US)	50-60 GHz	~250 GFLOPS/CPU (est.)	64-bit RISC with dual-level multithreading (~120 instructions)	Feasibility study with no practical design
2000-2002	8-bit FLUX-1 microprocessor prototype (US)	20 GHz	40 billion 8-bit integer operations per second	Ultrapipelined, multi-ALU, dual-operation synchronous long instruction word with bit-streaming (~ 25 instructions)	Designed, fabricated; operation not demonstrated
2002-2005	8-bit serial CORE1 microprocessor prototypes (Japan)	16-21 GHz local, 1 GHz system	250 million 8-bit integer operations per second	Non-pipelined, one serial 1-bit ALU, two 8-bit registers, very small memory (7 instructions)	Designed, fabricated, and demonstrated
2005-2015 (est.)	Vector processors for a petaflops system (Japan)	100 GHz	100 GFLOPS/CPU (target)	Traditional vector processor architecture	Proposal

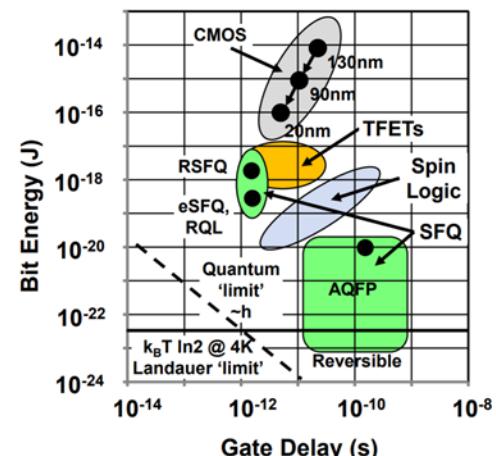
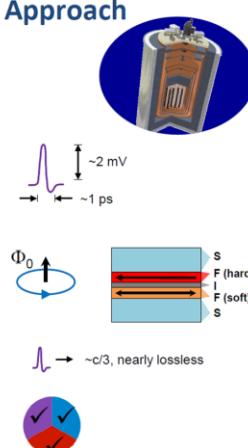
TABLE 3-2-2. STATUS OF LOW-LATENCY CRYO-RAM CANDIDATES					
Type/Lab	Access Time	Cycle Time	Power Dissipation	Density	Status
Hybrid JI-CMOS (UC Berkeley)	500 ps for 64 kb	0.1 - 0.5 ns depending on architecture	12.4 mW read 10.7 mW write (Single cell writing)	64 kB in < 3x3 mm <sup>2</sup>	All parts simulated and tested at low speed
RSFQ decoder w/ latching drivers (STEC/SRL)	?	0.1 ns design goal	107 mW for 16 kB (Estimate)	16 kB in 2.5 cm <sup>2</sup> (Estimate)	256b project completed (Small margins)
RSFQ decoder w/ latching drivers (NG)	?	2 ns	?	16 kB/cm <sup>2</sup> *	Partial testing of 1 kb block
SFQ RAM (HYPRIS)	400 ps for 16 kb (Estimate)	100 ps for 16 kb (Estimate)	2 mW for 16 kB (Estimate)	16 kB/cm <sup>2</sup> *	Components of 4 kB block tested at low speed
SFQ ballistic RAM (Stony Brook University)	?	?	?	Potentially dense Requires refresh	Memory cell and decoder for 1 kB RAM designed
SFQ ballistic RAM (NG)	?	?	?	Potentially dense Requires refresh	SFQ pulse readout simulated
MRAM (40K)	Comparable to hybrid CMOS	Comparable to hybrid CMOS (Estimate)	< 5mW at 20GHz (Estimate)	Comparable to DRAM (Estimate)	Room temperature MRAM in preproduction; Low temperature data sparse

\*Densities of JI memories are given for the technologies in use at the time of the cited work. Greater densities can be expected when a 20 kA/cm<sup>2</sup> process is used. The symbol ? signifies insufficient data.

The **IARPA** agency has taken over with the **Cryogenic Computing Complexity (C3)** project launched in 2014. It involved IBM, Northrop Grumman, Raytheon and Hypres and was due to end in 2018<sup>942</sup>.

### Superconducting Computing Approach

- Low temperature operation (~4 K)
  - Allows different physics
  - Commercially available refrigeration
- Logic
  - SFQ (Single Flux Quantum)
  - Switching energy  $\sim 2 \times 10^{-20}$  J
- Memory
  - compatible with SFQ logic
- Interconnects
  - Superconducting in the cold space
  - Input/Output: electrical or optical
- Major energy reductions in all 3 areas!

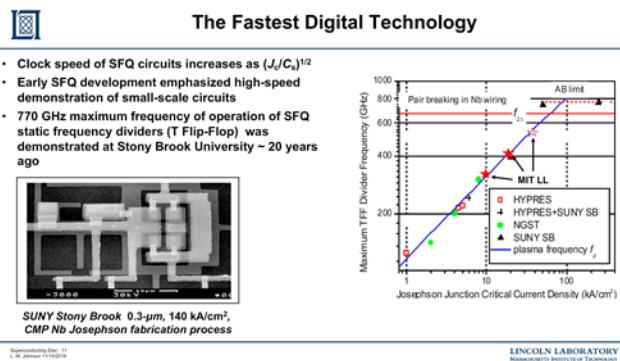


This project was part of the **National Strategic Computing Initiative (NSCI)** launched in 2015 by the White House, which focused on the development of supercomputers<sup>943</sup>. It's difficult to find out what this project has achieved as of 2021.

<sup>942</sup> See [Superconducting Computing and the IARPA C3 Program](#) by Scott Holmes, 2016 (57 slides) where the “Supercomputing Computing Approach” slide and the RSFQ/ERSFQ/RQL/AQFP schema from a previous page come from. All the presentations of the C3 conference are [here](#).

Outside the USA, the **Japanese Superconducting Computing Program**'s ambition in 2004 was to create a processor running at 100 GHz generating 100 GLOPS in SFQ, supplemented by 200 TB of DRAM running at 77K to generate a 1.6 PFLOPS system comprising 16,384 processors.

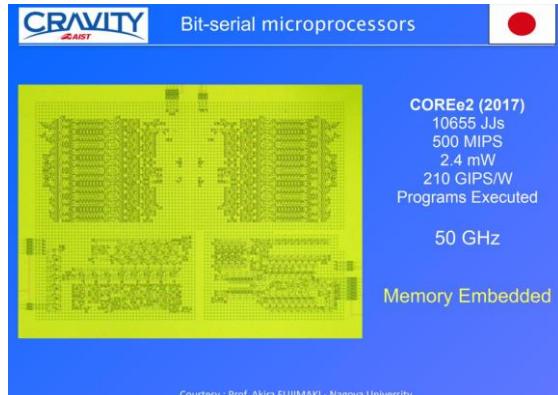
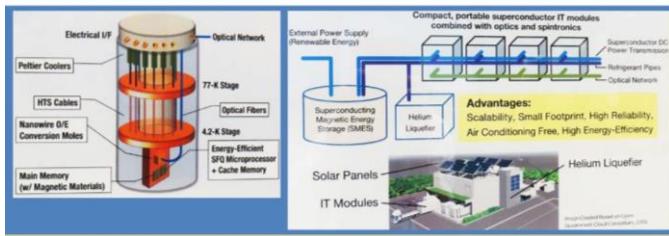
PROCESS	Current density [kA/cm <sup>2</sup> ]	minimum area [μm <sup>2</sup> ]	Maximum integration	Maximum frequency [GHz]
Hypres #03-10-45	0.03 1.0 4.5	~ 3.14	15,000	80 GHz RnIc=1.3mV @ 4.5 kA/cm <sup>2</sup>
Hypres #S45/100/200	0.1 1 4.5 10 20 30	~ 0.4	10,000	200 GHz @ 30 kA/cm <sup>2</sup>
MIT Lincoln Lab SFQx	10 20 50	~ 0.06	~ 800,000	240 GHz RnIc=2.17 mV @ 50 kA/cm <sup>2</sup>
ADP2	10	1.0	1100 JJ/mm <sup>2</sup>	80 GHz
STP2	2.5 - 20	0.25 - 4.0	100 JJ/mm <sup>2</sup> - > 2,000 JJ/mm <sup>2</sup>	30 GHz - 150 GHz
HSTP	10	1.0	70,000	80 GHz
Fluxonics standard	1	12.5	100 JJ/mm <sup>2</sup>	40 GHz RnIc = 0.256 mV
INRIM SNIS	up to 100	25	1,000 JJ/mm <sup>2</sup>	300 GHz RnIc = 0.1mV - 0.7mV
NIST Nb/Nbx Si1-x/Nb	up to 110	?	70,000	300 GHz
INRIM SNIS 3D FIB	up to 100	0.1	10,000 JJ/mm <sup>2</sup>	300 GHz RnIc=0.1mV - 0.7mV



All this with a cryostat consuming 12 MW and generating a thermal power of 18 kW at 4.2K. It has not yet seen the light of day about 17 years later<sup>944</sup>. Meanwhile, the IBM Summit supercomputer using traditional processors and GPUs generates 200 petaFLOPS consuming 13 MW, so why bother?

### Japanese 3-year program started

- “Superconductor Electronics System Combined with Optics and Spintronics”  
JST-ALCA Project: <http://www.super.nuge.nagoya-u.ac.jp/alca/> (Japanese)
- Processor goals: AQFP majority logic, 8-bit simplified RISC architecture,  
~25,000 JJs, ~10 instructions



**China** announced in 2018 a \$145M plan to build a superconducting computer by 2022. They had then created a chip with 10,000 Josephson junctions. Not sure they are ready for this milestone. **Russia** also has ambitions in this field<sup>945</sup>.

In **France**, the laboratory CMNE (Micro Nano Electronic Components) of the IMEP-LaHC (Microelectronics, Electromagnetism, Photonics, Microwave) of the UGA (Grenoble) was working in this area, under the responsibility of Pascal Febvre who is based in Chambéry.

In Korea, researchers from **Seoul National University** have proposed another path, creating computers with CryoMOSFET chipsets operating at a relatively hot temperature of 77K, reducing cooling costs.

<sup>943</sup> The following table comparing different types of achievements comes from [Superconducting Computing](#) by Pascal Febvre, CNRS, 2018 (56 slides). It is also the source of the slide on “Gravity Bit-Serial Microprocessors”.

<sup>944</sup> They managed to create the CORE1α in 2003 at 4999 JJ (Josephson junctions) running at 15 GHz, the CORE1β in 2006 at 10.955 JJ running at 25 GHz, the CORE1γ with 22,302 JJ also at 25 GHz, the CORE100 in 2015 at 3073 JJ and 100 GHz, the COREe2 in 2017 at 10,655 JJ and 50 GHz with an integrated memory. See [Impact of Recent Advancement in Cryogenic Circuit Technology](#) by Akira Fujimaki and Masamitsu Tanaka, 2017 (37 slides). This continued in 2019 with an 8-bit multiplier containing 20,251 JJ running at 48 GHz and consuming 5.6 mW. Source: [29.3 A 48GHz 5.6mW Gate-Level-Pipelined Multiplier Using Single-Flux Quantum Logic](#) by Ikki Nagaoka et al, 2019.

<sup>945</sup> See [The Outlook for Superconducting Computers](#) by R Colin Johnson, 2018.

Its benefits are less impressive than superconducting computing with an improvement of only 41% in single thread performance for the same power budget or a power reduction of 38% for the same performance, all of this including of course the cooling power budget<sup>946</sup>.

In the end, this branch of the superconducting computer industry is for the moment still immature. It has suffered from the uninterrupted advance of Moore's Law until the last few years and the difficulties of its practical implementation. It is not impossible that synergies will develop between quantum computing and this somewhat neglected branch. They can help each other, as can be seen with superconducting circuits for driving superconducting qubits or silicon. As we know, quantum computing will perhaps indirectly revive this sector<sup>947</sup>!

## Probabilistic computing

Probabilistic processors are another variation of exotic processors. They use probabilistic p-bits that can fluctuate rapidly between 0 and 1 with a low transition energy level. They are supposed to allow the resolution of so-called "quantum" problems without relying on quantum mechanisms. p-bits can be realized with nanomagnets and also with regular transistors<sup>948</sup>.

Various applications are promoted such as the creation of neural networks called BSN (Binary Stochastic Neuron) and the resolution of optimization problems similar to those treated by quantum annealing and gate-based quantum computing. The accelerations obtained are not qualified as exponential. It may be just polynomial, which is still interesting.

Work in this direction is quite recent and comes from **Purdue University** in Indiana<sup>949</sup> and from **Tohoku University** in Japan<sup>950</sup>. **HawAI.tech** (France), a Grenoble-based startup, is positioned on the same niche and targets applications in the field of AI in embedded systems using data from various sensors<sup>951</sup>. Their roadmap should lead to the creation of a complete probabilistic computer by 2024.



## Optical processors

Many research laboratories and startups are working on the creation of optical processors that are not based on photon qubits. Some are creating classical optical neural networks, others are adapted to convolutional neural networks or spiking neurons, the latter being closest to the way the human brain works.

---

<sup>946</sup> See [CryoCore: A Fast and Dense Processor Architecture for Cryogenic Computing](#) by Ilkwon Byun et al, 2020 (14 pages).

<sup>947</sup> At last, see this good review paper [Beyond Moore's technologies: operation principles of a superconductor alternative](#) by Igor I. Solov'ev et al, Russia, 2017 (22 pages). It mentions the potential of a two orders of magnitude gain in energy efficiency with superconducting based supercomputers, cryogenics included. On top of the various variations of SFQ, RQL and SQUID superconducting circuits, the review also covers cryogenic memory. One of the limitations of superconducting circuits is their low potential miniaturization. Josephson junctions density seems limited to 2.5 million junctions per cm<sup>2</sup>. To be compared with billions of CMOS transistors with 5nm/7nm nodes!

<sup>948</sup> See an explanation of p-bits in [Waiting for Quantum Computing? Try Probabilistic Computing](#) by Kerem Camsari and Supriyo Datta, IEEE Spectrum, March 2021, then [Integer factorization using stochastic magnetic tunnel junctions](#) by William A. Borders et al, 2019, [p-Bits for Probabilistic Spin Logic](#) by Kerem Y. Camsari, 2019 (11 pages) and [Stochastic for Invertible Logic](#) by Brian Sutton et al, 2017 (19 pages).

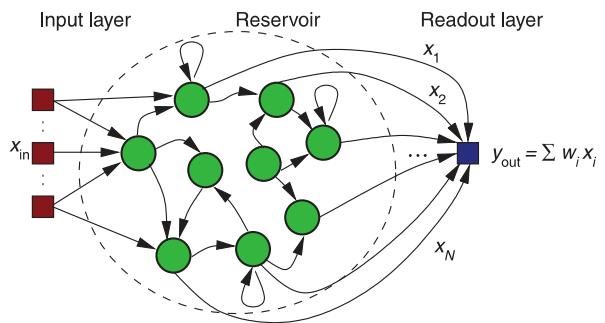
<sup>949</sup> See [From Charge to Spin and Spin to Charge: Stochastic Magnets for Probabilistic Switching](#) by Kerem Y. Camsari et al, February 2020 and [Hardware Design for Autonomous Bayesian Networks](#) by Rafatul Faria et al, 2020 (10 pages).

<sup>950</sup> See [Demonstrating the world's fastest spintronics p-bit](#) by Tohoku University, March 2021 and [Waiting for Quantum Computing? Try Probabilistic Computing](#) by Kerem Camsari and Supriyo Datta, 2021.

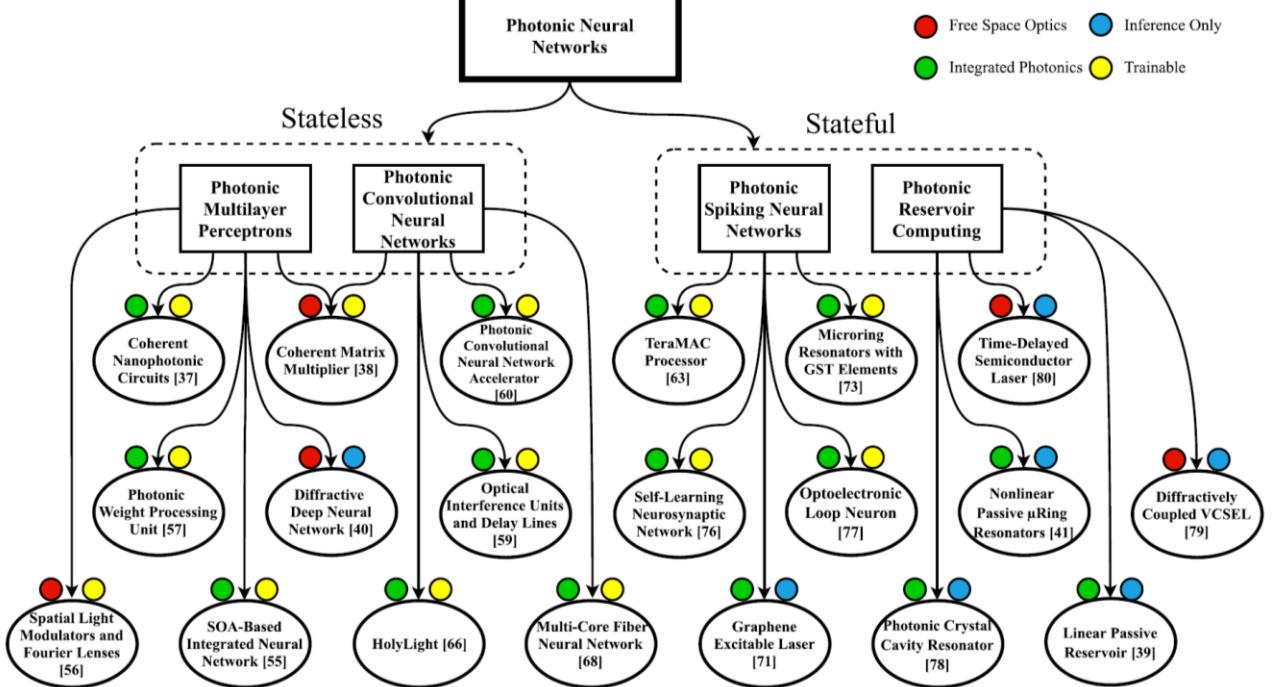
<sup>951</sup> See [Bayes from Cell to Chip](#) by Pierre Bessière, 2018 (33 slides).

Let's mention **reservoir computing** which is a specific category of recurrent neural networks used to process time series (in language processing, finance, energy, robotics)<sup>952</sup>. Their particularity is to use neuron weights and links between neurons randomly fixed in the reservoirs, all with non-linear activation functions for these links. The hundreds of neurons in a reservoir are fed by input data stored in the reservoirs. The activation functions non-linearity makes this memory evanescent. The training parameters of these networks are located in the weights of the neurons that connect the reservoirs to the output data<sup>953</sup>.

There are classic reservoir computing projects, rather based on memristors<sup>954</sup>, five types of optical reservoir computing and even quantum versions<sup>955</sup>! The different types of optical neural networks are mapped *below*<sup>956</sup>.



**Figure 1:** Standard layout of a reservoir computer, comprising an input layer (red), the reservoir (green) with randomized but fixed connections, and the linear readout layer (blue). Here, for simplicity a one-dimensional readout layer is drawn ( $l=1$ ).



<sup>952</sup> The concept of reservoir computing dates back to 2007. See [Toward optical signal processing using Photonic Reservoir Computing](#) by Kristof Vandoorne et al, 2008 (11 pages). It is also described in [Novel frontier of photonics for data processing - Photonic accelerator](#) by Ken-ichi Kitayama, 2019 (25 pages) as well as in this beautiful presentation [Introduction to Reservoir Computing](#) by Helmut Hauser (282 slides). The notion is different from the one of [reservoir engineering](#).

<sup>953</sup> The source of the schematic on reservoir computing is [Advances in photonic reservoir computing](#) by Guy Van der Sande et al, 2017 (16 pages) which provides an excellent focus on optronics based reservoir computing.

<sup>954</sup> See [Memristors and Beyond: Recent Advances in Analog Computing](#) by Nick Skuda, 2019 (12 slides).

<sup>955</sup> See [Universal quantum reservoir computing](#) by Sanjib Ghosh et al, from Singapore, 2020 (23 pages) as well as [Integrated Nano-photonics Structures for Optical Computing](#) by Laurent Larger et al, 2019 (50 slides).

<sup>956</sup> Diagram source: [Photonic Neural Networks: A Survey](#) by Lorenzo de Marinis et al, 2019 (16 pages).

We will now focus on solutions based on optical processes using image diffraction from DMD or DLP chips illuminated by a laser and sent on various structures such as random matrices or various metamaterials.

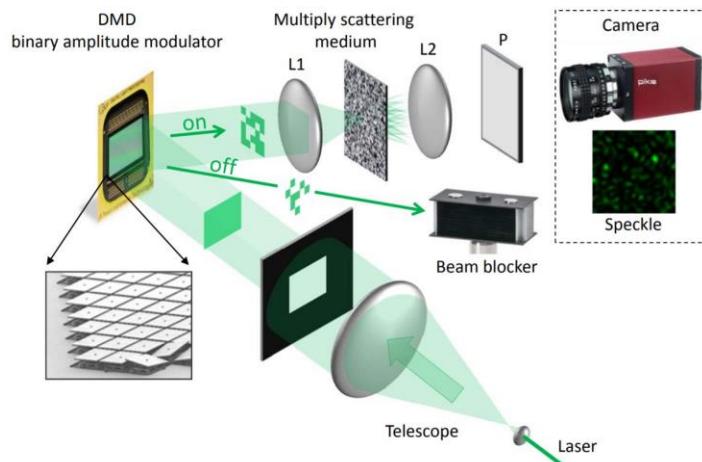
They are often based on the principle of the Optical Fourier Transform which allows to decompose a 2D image into spatial frequencies, itself represented in 2D. This transform is an image that contains key points representing shapes and repetitions in the analyzed images.

This can be leveraged to build convolution layers in convolutional neural networks. These serve to detect the presence of shapes in an image, the shapes being represented by filters. The Fourier transform helps to automatically identify these key shapes in the image. These systems capture the result with a CMOS sensor, usually with a very high resolution, much higher than that of the DLP or DMD chip used upstream. The diffraction thus carries out a projection in a space of larger dimension than the original image. All this is supported by serious mathematics<sup>957</sup>.

These different solutions are in their infancy. They can accelerate certain calculations for training complex neural networks. These accelerations seem to be rather polynomial and not exponential as quantum computing is supposed to generate. Except that they do not seem to be handicapped by noise issues as qubits are.

Let's now have a look at various commercial vendors in this very specific market.

**Lighton.io** (2016, France, \$3.7M) sells an optical coprocessor that accelerates neural networks training on large volumes of training data, such as with convolutional networks. A laser emits a beam that is magnified with some lenses to illuminate a DLP micromirror chip. The generated image then traverses a random matrix, the scattering medium in the illustration. A monochrome CMOS imaging sensor then analyzes it<sup>958</sup>.



The sensor captures the interferences generated by the set and some mathematical computing interprets the result. This process enables a reduction of a complex data set dimensionality.

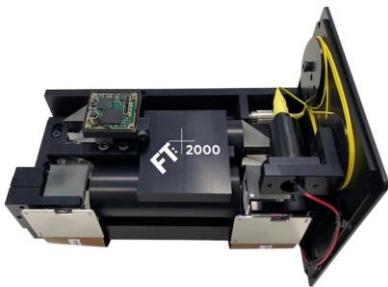
The miniaturized device fits in a 2U server. The system computing power comes in particular from the DLP and the CMOS sensor resolutions, which is about several million pixels. Everything is driven by Python libraries developed with TensorFlow. The targeted applications are first and foremost genomics and Internet of Things solutions.

---

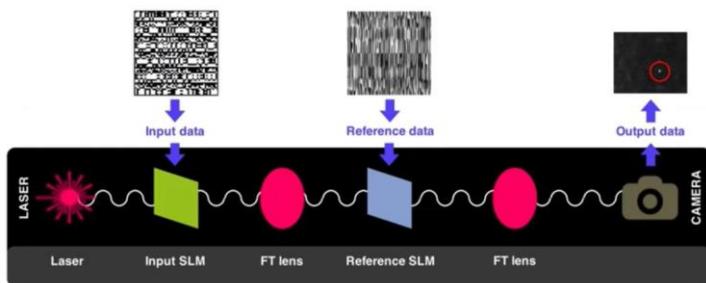
<sup>957</sup> See [An optical Fourier transform coprocessor with direct phase determination](#) by Alexander Macfaden et al, 2017 (8 pages) and [Performing optical logic operations by a diffractive neural network](#) by Chao Qian et al, 2020 (7 pages).

<sup>958</sup> The process is described in [Random Projections through multiple optical scattering: Approximating kernels at the speed of light](#), 2015 (6 pages).

**Optalysys** (2013, UK, \$5.2M) uses a process similar to that of LightOn<sup>959</sup>. Their FT:X 2000 system is structured around the realization of optical fast Fourier transforms based on diffraction. The project stems from research work at the University of Cambridge. They are involved in various projects, one in genetics to do genome sequence alignment, GENESYS, carried out with the **Earlham Institute**.



Once input and reference data is converted into symbol representations, the data is addressed into the optical system and matches are identified on a camera sensor:



The other project deals with weather forecasting for the European center **ECMWF** and a third one for plasma and fluid dynamics simulation, done for the DARPA. They also did run a convolutional network in 2018 on a MNIST base with 60,000 letters for training and 10,000 for testing. Its success rate was of only 70%. The startup was founded by Nick New, Robert Todd and Ananta Palani.



**Fathom Computing** (2014, USA) uses an "electro-optical" architecture capable of training memory and convolutional neural networks (LSTM). Their Light Processing Unit (LPU) would be able to read 90% of the tests from the MNIST handwriting database, using the same test as the one performed by Optalysys.

The system is adapted to linear algebra and matrix multiplication. They still have to miniaturize their device, which according to them should take at least two years, as of 2018. In 2021, it doesn't seem they achieved any result. The startup was launched by two brothers, William and Michael Andregg.

**Luminous Computing** (2018, USA, \$9M) aims to create a high-performance optical component that would replace 3000 Google TPUs! It would exploit multicolor lasers and light guides. According to the publications of their CTO, Mitchell Nahmias, it seems that they use optical spike neurons<sup>960</sup>. They can perform calculations very quickly, including in classical CMOS. So, in optical computation, it should be faster. Wait and see, given they are still in a rather stealth mode.

All these solutions from startups are still in the middle of the water. They have demonstrated interesting small-scale computing capabilities for ad-hoc needs. What remains to be done is to scale them up and integrate them into computing solutions that are generally hybrid. Efforts are therefore focused both on solutions packaging so that they can be integrated into standard server racks, and on development tools. Without developers, there is no application!

Let's add to this the **Copac** project funded by the European Union H2020. Its goal is to create an exotic quantum computing solution that does not exploit qubits. Its ambition is to enable the resolution of data analysis problems such as the simulation of complex systems or machine learning.

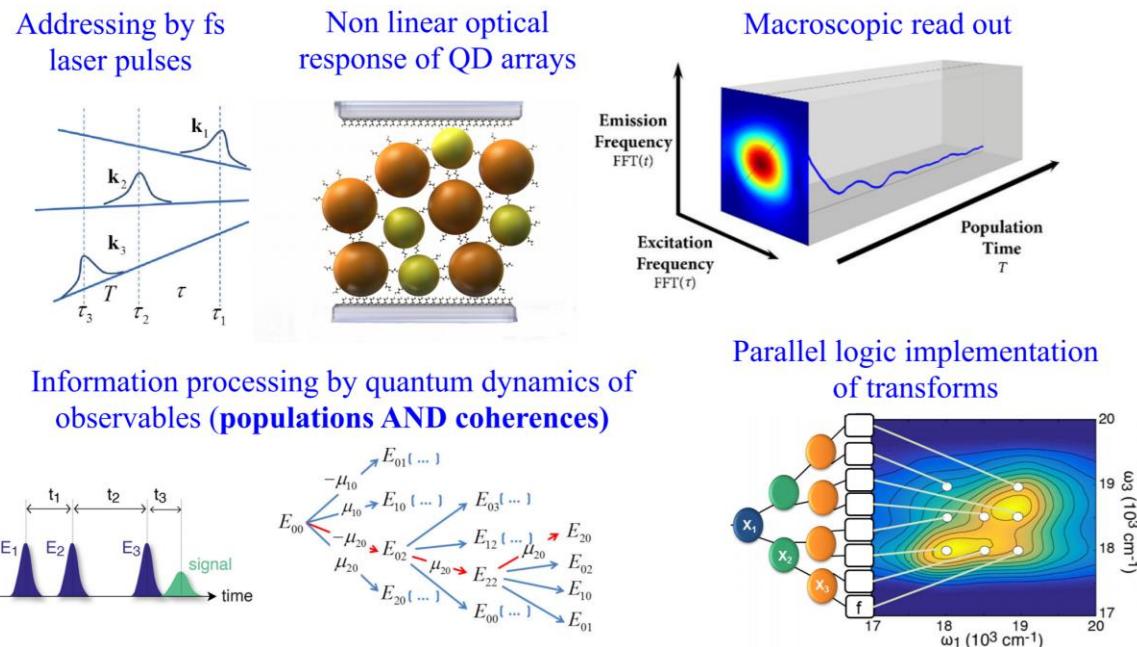
<sup>959</sup> See [Optalysys - Revolutionary Optical Processing for HPC](#), September 2017 (23 mn).

<sup>960</sup> See [Progress in neuromorphic photonics](#) by Thomas Ferreira de Lima, Mitchell Nahmias et al, 2017 (23 pages).

The processor would have the capacity to evaluate all the variables of a logical function in parallel. It is based on a quantum dots-based architecture that can be excited simultaneously on several frequencies by wideband lasers. The results are read by 2D spectroscopy of quantum dots. The machine would operate at room temperature. The process mixes classical computation (for the evaluation of functions) and quantum methods (to do it simultaneously on several sets of variables).

### Coherent Optical PArallel Computing

by ultrafast laser addressing, quantum engineered information processing and  
macro readout of semi-conducting quantum dot arrays.



The project is conducted with the Universities of Liège (Françoise Remacle), Hebrew University of Jerusalem (Raphael Levine), University of Padua, the CNR Institute for Physical and Chemical Processes of Bari, the company **KiloLambda** (2001, Israel) which manufactures the quantum dots and **ProBayes** (France), a subsidiary of La Poste which produces the compiler of the solution (Emmanuel Mazer and David Herrera-Marti, who now works at CEA-Leti)<sup>961</sup>.

The great uncertainty on this project, as is often the case, concerns its scalability. It depends in particular on the superposition of optical frequencies. The project documentation does not describe well the domain of the possible in terms of complexity classes of addressable problems.

<sup>961</sup> See [Coherent Optical Parallel Computing](#), 2017. The European project is funded until 2021. See more details in [Coherent Optical Parallel Computing Project Summary](#).

## Quantum enabling technologies key takeaways

- Cryogeny is a key quantum computing enabling technology particularly for solid-state qubits which work at temperatures between 15 mK and 1K. These systems rely on a mix of helium 3 and 4 in so-called dry-dilution refrigeration systems. Other simpler cooling technologies target the 3K to 10K temperature ranges that are used with photon sources and detectors, as used with photon qubits systems.
- Cabling and filters play another key role, particularly with solid-state qubits. Superconducting cables are expensive with 3K€ per unit and come from a single vendor source from Japan. Signals multiplexing is on the way!
- Microwave generation and readout systems used with superconducting and electron spin qubits are other key enabling technologies. The challenge is to miniaturize it and lower their power consumption to put them as close as possible to the qubits, operate them at cryogenic temperatures and simplify system cabling. It's a key to physical qubits scalability.
- Very low temperatures are measured within cryostats with specific thermometers.
- Many lasers and photonics equipment are used with cold atoms, trapped ions and photon qubits and also quantum telecommunications and cryptography. It includes single indistinguishable photon sources as well as single photon detectors. The lasers field is also diverse (wavelength, power, continuous vs pulse lasers, ...).
- Quantum technologies use a lot of various raw materials, some being rare but used in very small quantities. Whole some materials may have some incurred environmental costs, most of them do not seem to be scarce and they have multiple sources around the planet.
- We study various non-conventional computing technologies that may compete with quantum computing or even be of some help, like reversible and superconducting technologies that may be useful to create cryogenic electronics enabling the creation of scalable quantum computers.

# **Quantum algorithms**

It is now time to put aside quantum hardware and turn to quantum algorithms and software!

Gate-based quantum computers use so-called quantum algorithms that are theoretically much more efficient than their equivalents designed for classical computers. There are not that many algorithms and their relative performance compared to classical algorithms is not always obvious to prove. It is even sometimes contested. The assertion "*quantum computers are faster than classical computers*" is therefore debatable and must be discussed and analyzed on a case-by-case basis.

**Richard Feynman** described the idea of creating quantum simulators in 1982<sup>962</sup>. His idea was to create devices using the effects of quantum mechanics to simulate them, which would be almost impossible with traditional computers. This corresponds today to so-called quantum simulators, a specific breed of analog quantum computers. But we're dealing here mostly with gate-based quantum computing, based on **Yuri Manin**'s idea from 1980 and then refined by **David Deutsch** between 1985 and 1992.

Mathematicians have been working since the mid- and late 1980s on creating algorithms for quantum computers and simulators, long before any hardware was available.

The first quantum algorithms were published in the early 1990s, while the first two-qubit quantum systems appeared around 2000/2002. Researchers have been regularly creating new algorithms for the past 25 years, regardless of the relatively slow progress with hardware. The [Quantum Algorithm Zoo](#) launched in 2011 identifies 62 classes in the scientific literature and 430 algorithms (as of April 2021), organized in 4 algorithms groups (algebraic and number theory, Oracle problems, Hamiltonian simulations, optimization - numerics and machine learning). The list is maintained by Stephen Jordan, a researcher at Microsoft Quantum. This is still a modest number compared to the thousands of non-quantum algorithms<sup>963</sup>. Even though most classical computing developers don't know and use many algorithms in practice!

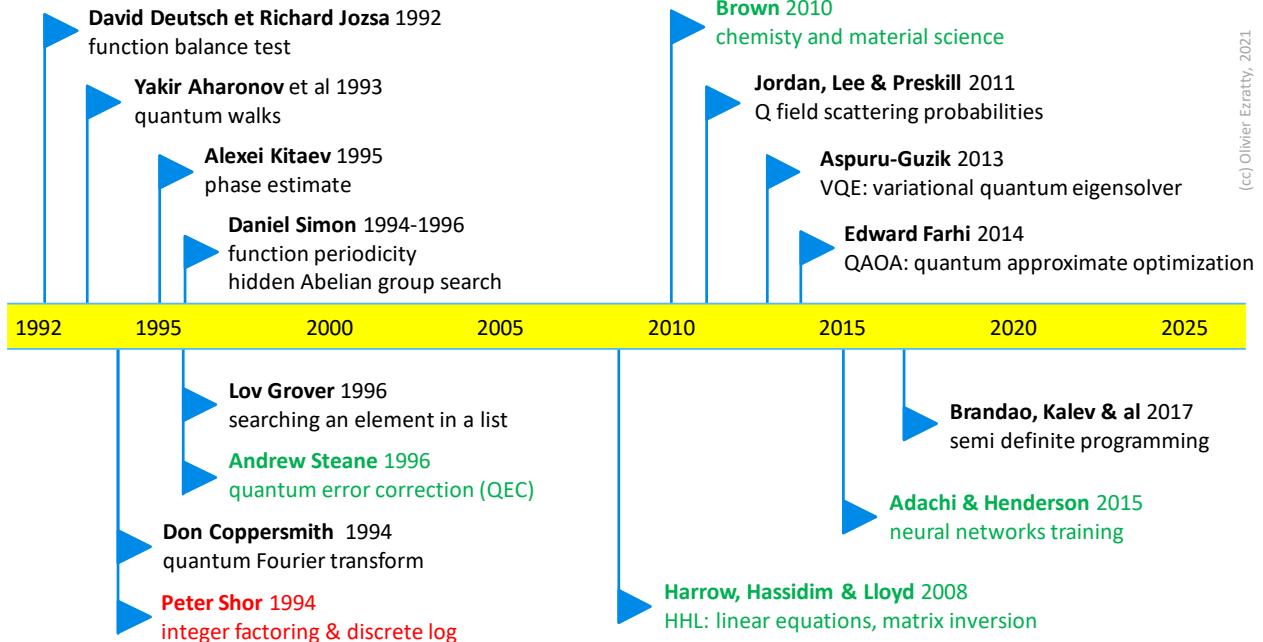
Quantum algorithms creation is thus a parallel research path with hardware progress, even though they might be sometimes closely related. This is not the first time in history. The emblematic **Ada Lovelace** did formalize the first algorithms and lines of code to run on **Charles Babbage**'s machine, which only saw the light of day in 2002 in London, 153 years after its conception ([video](#)) (see the sample program *below*). In 1842/1843, she had annotated a translation of her own of a paper by the Italian **Luigi Federico Menabrea** describing Babbage's machine. It took 102 years for the first electronic computers to see the light of day at the end of World War II! A beautiful game... of patience!

It is also reminiscent of **Leonardo da Vinci**'s helicopter designs dating from 1487-1490. A first human-powered helicopter created by the University of Toronto flew in 2013, AeroVelo ([video](#)) followed by another fairly close specimen from the University of Maryland flying in 2018 ([video](#))! So, more than five centuries apart! And even taking into account the flight of the first motorized helicopter in 1907, the time lag is still over four centuries. This same University of Maryland is one of the most advanced in the world in quantum computers based on trapped ions!

---

<sup>962</sup> See [Simulating Physics with Computers](#), Richard Feynman, 1982 (22 pages).

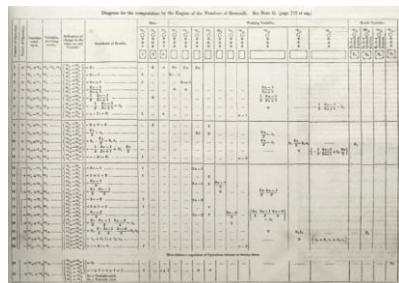
<sup>963</sup> For an extensive coverage of the key gate-based quantum algorithms, see [Lecture Notes on Quantum Algorithms](#) by Andrew M. Childs, April 2021 (181 pages) and [Quantum Computing Lecture Notes](#) by Ronald de Wolf, 2021 (184 pages).



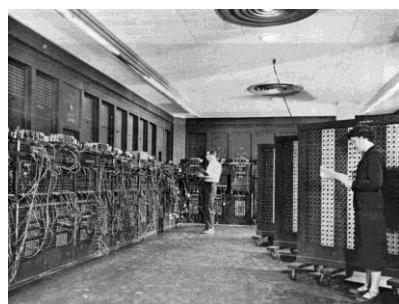
(cc) Olivier Ezratty, 2021

After the war, history repeated itself in part for much of the work in the vast field of artificial intelligence, where researchers were also working on algorithms, especially neural network-based algorithms, before any computers could execute them properly on a useful scale such as for objects recognition in images.

The first computers running perceptrons, the ancestors of today's artificial neural networks, were rudimentary. The rise of deep learning since 2012 is partly linked to the power of machines and GPUs able to train such neural networks. Hardware has once again joined algorithms that were ahead of their time.

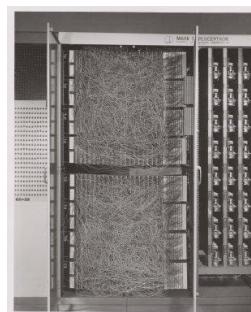


**Ada Lovelace**  
1842, first program for Babbage's analytical machine which didn't exist



**ENIAC**  
1945, first electronic computer

**McCulloch & Pitts**  
1943, artifical neurons concept



**Mark I Perceptron computer**  
1957, first synaptic processor



**Alexnet on Nvidia GTX 580**  
2012, first neural network with a recognition rate having less than 30% error rate.



**Léonard de Vinci**  
1487, aerial screw



**Paul Cornu, 1903**  
first motorized hélicopter  
1,5 m altitude



**AeroVelo, 2013**  
first human power helicopter flight

Even today, many of the quantum algorithms that are invented are not yet executable on a large problem scale on current quantum computers or on classical computing quantum emulators. There are not enough quality qubits available to be of any use and, more importantly, to be more powerful in any dimension than classical computers. Supercomputers can emulate about 50 qubits but no operational quantum computer can reach this number with error corrected qubits.

In another analogy with the History of Computer Science, we are still programming quantum computers with rather low layers of machine language, a bit like machine language or macro-assembler used 30 to 50 years ago, or more recently, for those who program low-level embedded systems or peripheral drivers. Today's quantum algorithms are mid- to low-level logical chunks of quantum code. Their assembly is even not yet done in practice.

The creation of quantum algorithms requires a capacity for abstraction that is beyond that of classical algorithms and programs, even taking into accounts object-based or events-based programming. We'll have to groom a new generation of mathematicians and developers capable of reasoning with the mathematical formalism of quantum programming as quantum computers mature. They will have to be able to conceptualize algorithms that are not easy to mentalize. Most of the times, though, quantum algorithms won't be simple language translation from classical programming language. They will solve problems that classical computers and classical programming languages can't solve.

One day, the abstraction level of quantum programming may rise to a point where it is no longer necessary to understand the low-level intricacies of quantum gates, Hilbert spaces, Hamiltonians and quantum interferences. But this is just a conjecture!

Today's classical quantum algorithms use quantum gates. But there are other variations:

- **Quantum annealing algorithms** such as those for D-Wave machines which are based on the initialization of relations between average quality qubits in matrices and on the search for a minimum energy based in particular on the tunnel effect. The basic algorithm there is about solving an Ising model. We've described it when discussing about [D-Wave](#).
- **Analog quantum simulators** are used to simulate quantum phenomena, for example to predict the organization of atoms in molecules. These include cold atom quantum simulators. An algorithm here is about preparing the state of the qubits in the system and their link weights. It's a process similar to D-Wave quantum annealing, with variations on the degrees of liberty handled in the system and qubits coherence.
- **Continuous variable quantum computers** that use quantum objects whose physical quantity can be measured as a continuous, not binary, quantity. This creates yet another programing model. They are mainly based on photons<sup>964</sup>.
- **Topological quantum computers**, which do not yet exist. This is the research path of Microsoft and some research laboratories, especially in China. We cover this on page 300. It should still be programmable with gate-based classical code.
- **Hybrid algorithms** combining traditional algorithms and quantum algorithms running on any of the above system<sup>965</sup>. This is notably the case of the Variational Quantum Eigensolver (VQE) which allows the resolution of chemical simulation problems as well as neural network training.

---

<sup>964</sup> See for example [Perspective: Toward large-scale fault-tolerant universal photonic quantum computing](#) by S. Takeda et al, April 2019 (13 pages) and [Continuous-variable quantum neural networks](#) by Nathan Killoran et al, June 2018 (21 pages) which deals with the use of continuous variable qubits to create neural networks.

<sup>965</sup> See [Hybrid Quantum Computation](#) by Arun, 2011 (155 pages).

We can also mention **Quantum inspired algorithms** which are algorithms running on classical computers that are inspired by quantum algorithms for solving complex problems. Their creation started long before the first experimental quantum computers were created.

In practice, the noisy intermediate scale quantum computers (NISQ) that are emerging now and will dominate the landscape for at least a good decade cannot run "deep" algorithms.

Namely, because of quantum gates and readout error rates is too high and limits the number of quantum gates that can be chained. We are thus limited to use algorithms that chain a rather small number of quantum gates.

This is the case for **VQE** (Variational Quantum Eigensolver), **QAOA** (Quantum Approximate Optimization Algorithm), **QAO-Ansatz** (Quantum Alternating Operator Ansatz, sometimes confusingly also named QAOA), Variational Quantum Factoring and some Quantum Machine Learning algorithms (Support Vector Machine, Principal Component Analysis and Quantum Variational Autoencoder). We will have the opportunity to study some of them later on.



<https://algassert.com/quirk>

online open source tool to learn  
programming up to 16 qubits

and **Atos**  myQLM  
free on desktop/laptop, emulate physical  
qubits characteristics

### key differences

- graphical circuit design (optional)
- analog computing
- playing with qubits interferences
- uncopyable but transferable data
- computing timing constraints (on NISQ)
- no debugging breaking points
- multiple runs and results averages

### variants

- classical/quantum hybrid algorithms
- quantum simulations (Hamiltonians)

(cc) Olivier Ezratty, June 2021

## Algorithms classes

Before getting into deep into quantum algorithms, let's take a detour with covering their practical usefulness known to date and for which category of quantum hardware they are designed. Then, how they are organized and what is the basic algorithms toolbox available to developers.

### Classes and use cases

Here's a simple classification of high-level algorithms by use cases<sup>966</sup>.

**Oracle function-based algorithms** can fasten the search of a needle in a haystack and find solution of some complex problems. Some are useful, some are not. The most famous oracle-based algorithms are Deutsch-Jozsa, Simon, Bernstein-Vazirani and Grover.

**Complex optimization problems**, particularly combinatorial problems like finding an optimal route for deliveries or automated drive, aka the traveling salesman problem. Such algorithms can also optimize the design of integrated circuits where one generally seeks to minimize the links between functional blocks, transistors and to minimize energy consumption, forms of sub-constrained

<sup>966</sup> There are many such classifications around. I've used the most common one.

optimization adapted to quantum processing. This category of algorithms can find solutions to combinatorial optimization problems (like discrete log, traveling salesperson problem and QUBO) and continuous optimization problems used in many other fields (linear programming, gradient descent, LPs, convex optimizations and semidefinite programming).

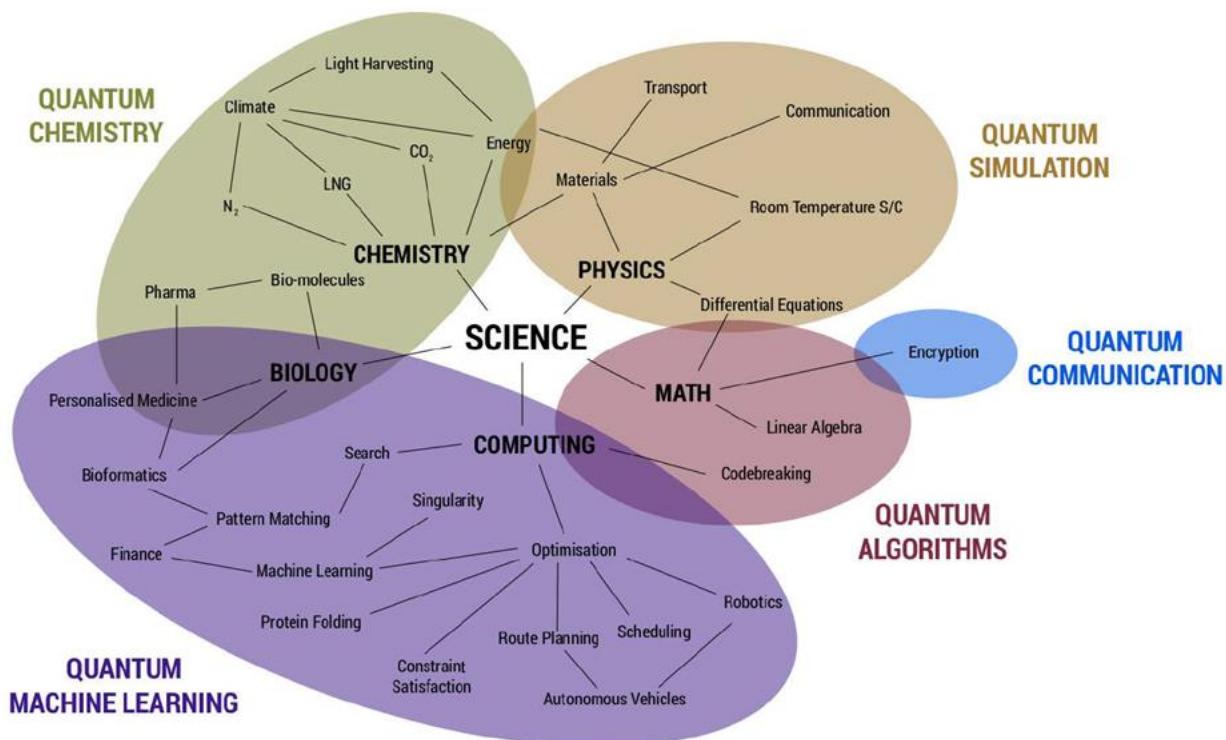
**Quantum machine learning** algorithms which under some circumstances could be more efficient than machine learning algorithms running on classical hardware, including GPGPUs and TPUs. This can impact both training machine and deep learning models and running inferences.

**Quantum physics simulations** is a broad field with applications in inorganic and organic chemical processes optimization and new material designs. This is based on simulating at the lowest level the interactions between atoms in molecules and crystal structures or magnetism, which themselves depend on the laws of quantum mechanics.

This may help invent new solutions such as more efficient batteries that can be charged more quickly and with greater energy density, craft chemical processes for carbon capture or nitrogen fixation or create of superconducting materials at room temperature.

**Biological molecule simulation** requires a much larger number of qubits, and therefore are positioned in the longer term. Quantum simulation may eventually help run simulations of biological molecules. This will start with the simulation of peptides, then polypeptides, and finally proteins folding and interactions. Biological molecules have the particularity of being overly complex, with structures that can reach tens of thousands of atoms. The top of the line would be the ability to simulate the assembly and then the operation of a ribosome, which is more than 100,000 atoms. It is the most magical molecular structure in living organisms, the one that assembles amino acids to build proteins from the messenger RNA code resulting from the transposition of gene DNA. This would be followed by the simulation of the functioning of a whole cell. But we are here bordering on with science fiction.

**Key factoring problems** relate to cryptography and breaking public encryption keys like RSA keys with Shor's integer factoring algorithm. These may be implemented over a very long-term, when highly scalable gate-based quantum computers are available.



**Hybrid algorithms**, as already mentioned, use a mix of quantum and classical algorithms. These are mostly used for chemical simulations but also quantum machine learning.

**Quantum inspired algorithms** are classical algorithms inspired by quantum algorithms, particularly those that rely on interferences which are key characteristics of quantum algorithms.

See also *above* this mapping of applications of quantum computing, which is however a bit fanciful, linking the learning machine to "singularity", which does not mean much<sup>967</sup>.

## Algorithms and quantum computing paradigms

There's a relation between these broad classes of algorithms and the class of quantum computers they can run on. Reusing the quantum algorithms paradigm classification used earlier in this ebook, this gives an idea of what works where and when, given these computer classes span from available systems (quantum annealing) to very long-term availability (large scale quantum computing).

	classical computers	quantum annealing computers	analog quantum simulators	universal gates quantum computers	
			NISQ	LSQ	
search algorithms				yellow	green
optimization algorithms		via QUBO	green	may require qRAM	may require qRAM
quantum machine learning		green		may require qRAM	may require qRAM
physics simulation		via Ising model	green	green	green
organic chemistry simulation		via Ising model	green	yellow	
integer factoring				Grover for symmetric keys	Shor requires a very large number of qubits
hybrid algorithms	green	green	green	green	green
quantum inspired algorithms	green	now	soon	later	much later

« quantumness » and arrow of time availability →

NISQ: noisy intermediate scale quantum computer, LSQ : large scale quantum computer  
 (cc) Olivier Ezratty, September 2021

## Algorithms process and compilation

As we have seen in a previous section describing the structure of [gate-based quantum computing](#), page 146, a quantum algorithm is built with three key parts: data initialization or preparation, computing and qubits readouts. This is always done on a data structure called a quantum register, made of N qubits. Data initialization, preparation and computing are all done with quantum gates.

**Results.** The algorithm result comes from the classical measurement of some qubits giving out a mix of 0s and 1s bits. In general, it is necessary to run several times the algorithm entirely and compute an average of the generated results. How many times must it be done? It depends on the nature of the algorithm and the speed at which we'll move from a probabilistic output (one run) to a deterministic result (average of several runs).

**Time constraints.** The algorithm run must be compatible with the quantum computer characteristics. The main ones are qubits numbers, gates and readout fidelities and coherence time. These parameters will condition the usable depth of computing, aka, the amount of series of gates that can be executed. This verification is generally performed by quantum code compilers.

<sup>967</sup> Source: [Silicon Photonic Quantum Computing](#) by Syrus Ziai, PsiQuantum, 2018 (72 slides).

It will also have to take into account the error correction codes that will be implemented in the hardware, either autonomously or through the control of the code compiler that will drive all logical qubits programming.

**Gates conversion.** Compilers play another key role: they translate the qubit gates used by the programmer into the set of physical qubit gates implemented at the hardware layer. Many quantum gates used by developers will be converted by the compiler into a set of universal quantum gates supported by the quantum computer. This will multiply the number of executed physical quantum gates compared to what shows up in the initial algorithm.

**Geometry.** They also take into account the physical geometry of qubits, i.e. how are they connected together. A simple two-qubit gate might require chaining a lot of SWAP gates because the two related qubits are far from each other in the quantum register physical layout.

**Efficiency.** An important consideration in creating quantum algorithms is to ensure that they are more efficient than their optimized counterparts for traditional computers or supercomputers. There are theories to verify this in order to evaluate the exponential, polynomial, logarithmic or linear rise in computing time as a function of the size of the problem to be solved, or a combination of all four. But nothing can replace experience!

**Everything is linear.** Quantum algorithms are practical applications of linear algebra, the branch of mathematics that handles vector spaces and matrix-based linear transformations. They are applied in large dimensional spaces, the vectors that define the states of qubit registers. Mathematically speaking, a qubit is a 2-dimensional vector space using complex number and a N qubits register manipulates a vector in a  $2^N$  dimensional space of complex numbers. Their manipulation is based on matrix-based calculations that allow the qubit state to be modified without reading the content of the qubits.

**Conditional programming.** Since quantum algorithms usually prohibits reading intermediate results, conditional programming is not obvious. Like running a given calculation depending on the value of some intermediate. However, multi qubits quantum gates (CNOT & co) are tools allowing conditional programming, but in another fashion than with classical computing. Conditional branching can be implemented in some situation and is implemented with hybrid algorithms using ancilla qubits for intermediate values measurements.

## Algorithms toolbox

All these algorithms are based on a small set of classical low-level algorithms that we'll describe in details:

- **Quantum Fourier Transforms** (QFT), which helps find periods in a signal. It's used in the famous Shor integer factoring, in many other algorithms (HHL, QML), discrete log search, solving the hidden subgroup problem (HSP) and even for simple reversible arithmetic<sup>968</sup>.
- **Quantum Phase Estimation** are relying on a QFT to find the eigenvalues or eigenvalues' phase of a unitary matrix or quantum subcircuit. It is used in HHL and many other quantum linear algebra algorithms.
- **Amplitude amplification** is used to amplify and select the desired state of a quantum superposition. It is used in the Grover algorithm and with combinatorial searches like the traveling salesperson problem search (TSP). It has a twin algorithm, amplitude estimation that estimates the value of the amplitude of the desired state.

---

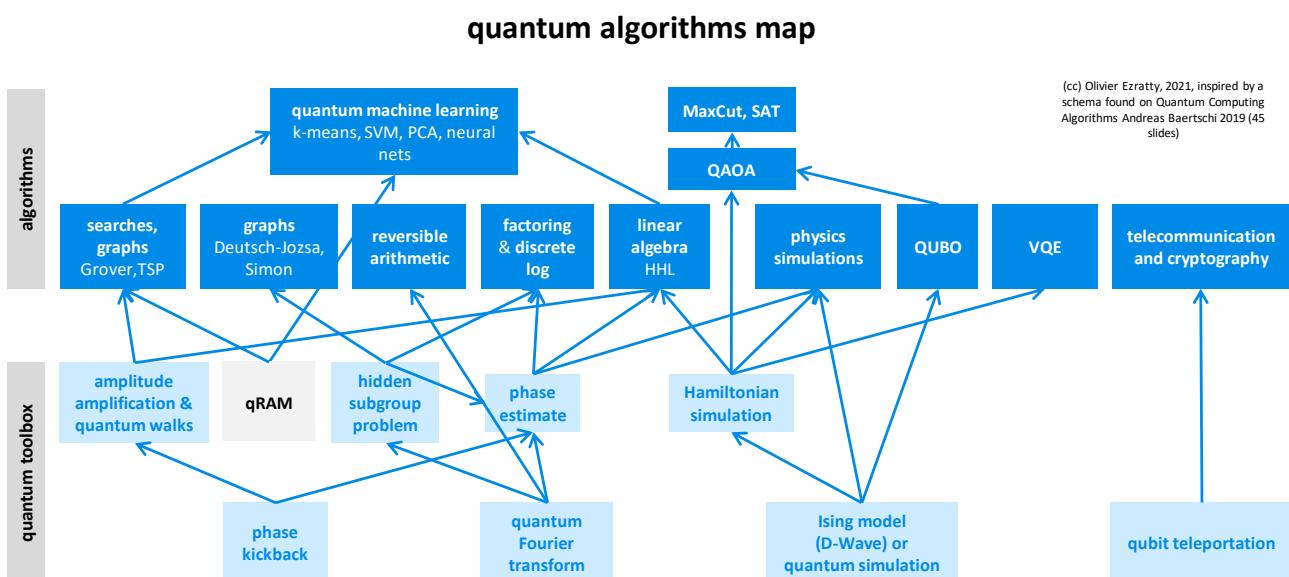
<sup>968</sup> See [A New Approach to Multiplication Opens the Door to Better Quantum Computers](#) by Kevin Harnett, 2019.

- **Quantum phase kickback** is an interference trick used in most oracle-based search algorithms and quantum walks, and then in quantum machine learning.
- **Hamiltonian Simulation** are used to find a point of equilibrium of a complex system such as in quantum physics simulation, neural networks training, the search for optimal paths in networks or process optimization. It can be implemented in all quantum paradigms: annealing, simulation and gate-based computing.
- **Ising model** is the mechanism used to drive quantum annealing and quantum simulators. Many physics simulation and combinatorial problems can be translated into some Ising model. This is the common practice used with D-Wave machines.
- **Quantum teleportation** is also an algorithm basic, used mostly in cryptography and telecommunication. It will also play a key role in distributed quantum computing and also in some non-telecom related algorithms.

We'll add here several other key basic algorithms components:

- **Data preparation**: how is data loaded in an algorithm? This is particularly important for quantum machine learning and optimization algorithms.
- **Uncompute trick**: which consists in reversing some parts of an algorithm after it is run. It allows to get rid of garbage states and cleaning up ancilla qubits.
- **Oracle**: which are binary functions implemented as unitaries that can be used for parallelizing their operation on all computational state basis (all combinations of 0s and 1s in part of a qubits register).
- **Linear equations**: and the famous HHL algorithm.

Classifying quantum algorithms is a tedious task due to the many dependencies they have with each other. For example, a QFT is used in HSP and phase estimate algorithms which themselves are used in integer factoring and linear equations solving. I have found many different if not inconsistent algorithms classifications in the available literature ([Wikipedia](#), [John Preskill](#), [Algorithm Zoo](#), etc). Some for example consider oracle-based algorithms as a separate algorithm class when others split these algorithms in various classes depending on the sub-algorithms they are using.



The relationship between these low-level algorithms and higher-level ones is showcased in the diagram below<sup>969</sup>. It shows qRAM for quantum RAM which is not an algorithm per se, but a hardware tool that is indispensable to run the related algorithms, particularly Grover algorithm and a lot of quantum machine learning algorithms.

The chart below shows a more detailed connection between the QFT and the many algorithms that rely on it<sup>970</sup>.

Algorithm	Description	Reference
<b>Algorithms Based on QFT</b>		
Shor's; $O(n^2 (\log N)^3)$	Integer factorization (given integer N find its prime numbers); discrete logarithms, hidden subgroup problem, and order finding	Peter W. Shor, "Algorithms for Quantum Computation Discrete Log and Factoring," AT&T Bell Labs, <a href="mailto:shor@research.att.com">shor@research.att.com</a>
Simon's; <i>exponential</i>	Exponential quantum-classical separation. Searches for patterns in functions	Simon, D.R. (1995), " <a href="#">On the power of quantum computation</a> ", Foundations of Computer Science, 1996 Proceedings., 35th Annual Symposium on: 116–123, retrieved 2011-06-06
Deutsch's, Deutsch's – Jozsa, an extension Deutsch's algorithm	Depicts quantum parallelism and superposition. "Black Box" inside. Can evaluate the input function, but cannot see if the function is balanced or constant	David Deutsch (1985). " <a href="#">Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer</a> ". Proceedings of the Royal Society of London A. 400: 97 David Deutsch and Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". Proceedings of the Royal Society of London A. 439: 553
Bernstein/Vazirani; <i>polynomial</i>	Superpolynomial quantum-classical separation	Ethan Bernstein and Umesh Vazirani. <i>Quantum complexity theory</i> . In Proc. 25th STOC, pages 11–20, 1993
Kitaev	Abelian hidden subgroup problem	A. Yu. Kitaev. <i>Quantum measurements and the Abelian stabilizer problem</i> , arXiv:quant-ph/9511026, 1995
van Dam/Hallgren	Quadratic character problems	Wim van Dam, Sean Hallgren, <i>Efficient Quantum Algorithms for Shifted Quadratic Character Problems</i> . CoRR quant-ph/0011067 (2000)
Watrous	Algorithms for solvable groups	John Watrous, Quantum algorithms for solvable groups, <a href="https://arxiv.org/abs/quant-ph/0011023">arXiv:quant-ph/0011023</a> (2001)
Hallgren	Pell's equation	Sean Hallgren. <i>Polynomial-time quantum algorithms for pell's equation and the principal ideal problem</i> , Proceedings of the thirty-fourth annual ACM symposium on the theory of computing, pages 653–658. ACM Press, 2002.
<b>Algorithms Based on Amplitude Amplification</b>		
Grover's; $O(\sqrt{N})$	Search algorithm from an unordered list (database) for a marked element, and statistical analysis	Lov Grover, <i>A fast quantum mechanical algorithm for database search</i> , In Proceedings of 28th ACM Symposium on Theory of Computing, pages 212–219, 1996
Traveling Salesman Problem; $O(\sqrt{N})$	Special case of Grover's algorithm	<a href="https://en.wikipedia.org/wiki/Travelling_salesman_problem">https://en.wikipedia.org/wiki/Travelling_salesman_problem</a>

Quantum algorithms are classifiable and explainable at a high level, but their detailed understanding is not easy. You must develop some conceptual capacity in a rather analog world<sup>971</sup>.

One key thing developers have to learn is how to translate customer needs into existing quantum algorithms. How to assemble various quantum algorithms, frequently combined with classical algorithms, is another key skill.

<sup>969</sup> Source of inspiration for the diagram on algorithms: [Quantum Computing Algorithms](#) by Andreas Baertschi, 2019 (45 slides).

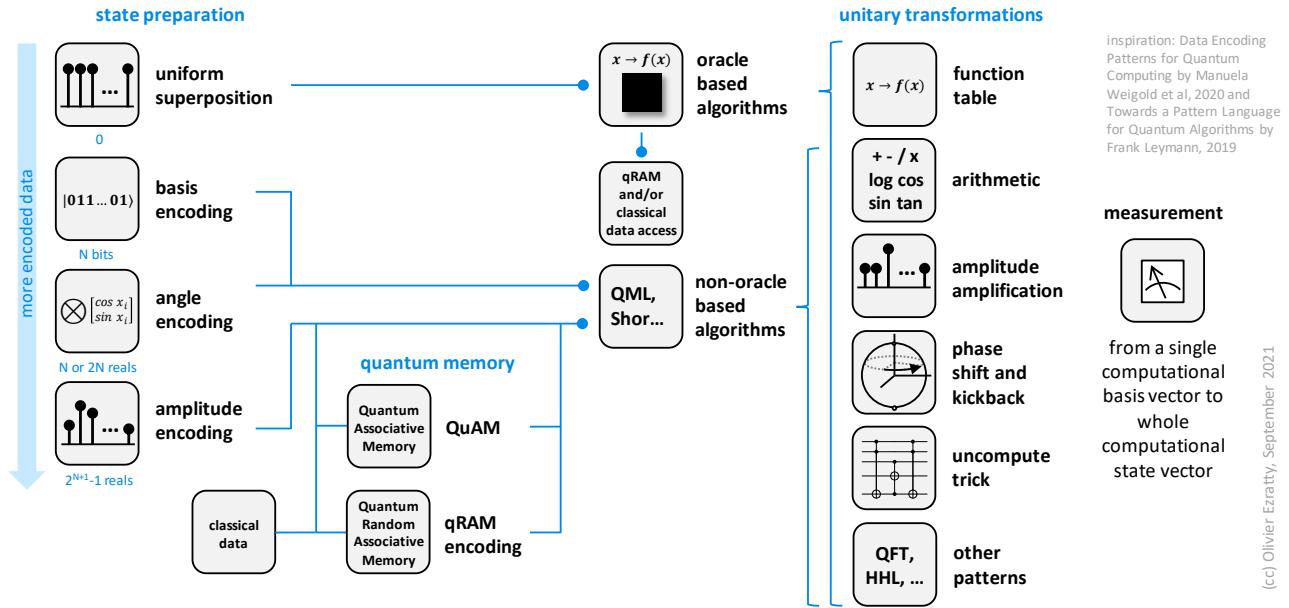
<sup>970</sup> See [Quantum computing \(QC\) Overview](#) by Sunil Dixit from Northrop Grumman, September 2018 (94 slides) from which the algorithm table on this page is extracted.

<sup>971</sup> Here are a few sources of information to explore the topic: [Quantum Computing Applications](#) by Ashley Montanaro from the University of Bristol, 2013 (69 slides), [Introduction to Quantum Information](#) by Yves Leroyer and Géraud Sénizergues from EN-SEIRB-MATMECA, 2016-2017 (110 pages), an interesting course on the algorithmic part, [An Introduction to Quantum Computing](#) by Phillip Kaye, Raymond Laflamme and Michele Mosca, Oxford, 2017 (284 pages), [Lecture Notes on Quantum Algorithms](#) by Andrew M. Childs, University of Maryland, 2017 (174 pages), [Quantum Computation and Quantum Information](#) by Nielsen and Chuang, 2010 (10th edition, 704 pages) and [A Course in Quantum Computing for the Community College](#) by Michael Locef, 2016 (742 pages) which sets out in great detail the mathematical foundations of linear algebra with complex numbers, Euler formulas, vector and Hilbert spaces, matrix calculus, tensors, eigenvectors and eigenvalues, and quantum algorithms. It takes several weeks to be browsed and understood. It is a course for the second and third year of the Foothill Community College in Los Altos Hills, California (so Bac+1/+2 in French equivalent). In addition, here are some videos on this subject: [Quantum Algorithms](#) by Andrew Childs in 2011 (2h31), [Language, Compiler, and Optimization Issues in Quantum Computing](#) by Margaret Martonosi, 2015 (39 minutes and slides) and [What Will We Do With Quantum Computing?](#) by Aram Harrow, MIT, 2018 (32 minutes).

# Basic algorithms toolbox

We'll describe here the overall structure of basic low-level gates-based quantum algorithms. We separate three stages: **data preparation**, **unitary transformations** (caveat: data preparation also relies on unitaries) and **measurement**.

We have already covered **error correction** in a [previous chapter](#) of this ebook, starting page 200.



## Data preparation

The data preparation stage is also named data loading. Its complexity covers a large range from the simple process of uniform superpositions associated to oracle-based algorithms like Deutsch-Jozsa, Simon or Grover to the most complicated, linked to quantum machine learning algorithms requiring full computational basis state vector amplitude encoding.

Data loading is only implemented with non-oracle-based algorithms. It may be a long process for large sets of inputs and significant number of qubits. It thus may require using some form of quantum memory, a sort of qubits buffer used only for data preparation.

It can use addressable qubits like with qRAM where a program can ask to “*put this information in qubits at index i*”. This memory can be a qubits register with a longer coherent lifespan than computing qubits or a classical data structure used along a quantum circuit to load a specific addressable quantum state. The data is not necessarily stored in some qubits. When the data is loaded in quantum memory, this one must be transferred to the computing qubits. This is a data transfer and not a data copy process due to the non-cloning theorem. All in all, quantum memory is just some sort of intermediate memory used before computing.

Let's first look at the various techniques used for data encoding<sup>972</sup>.

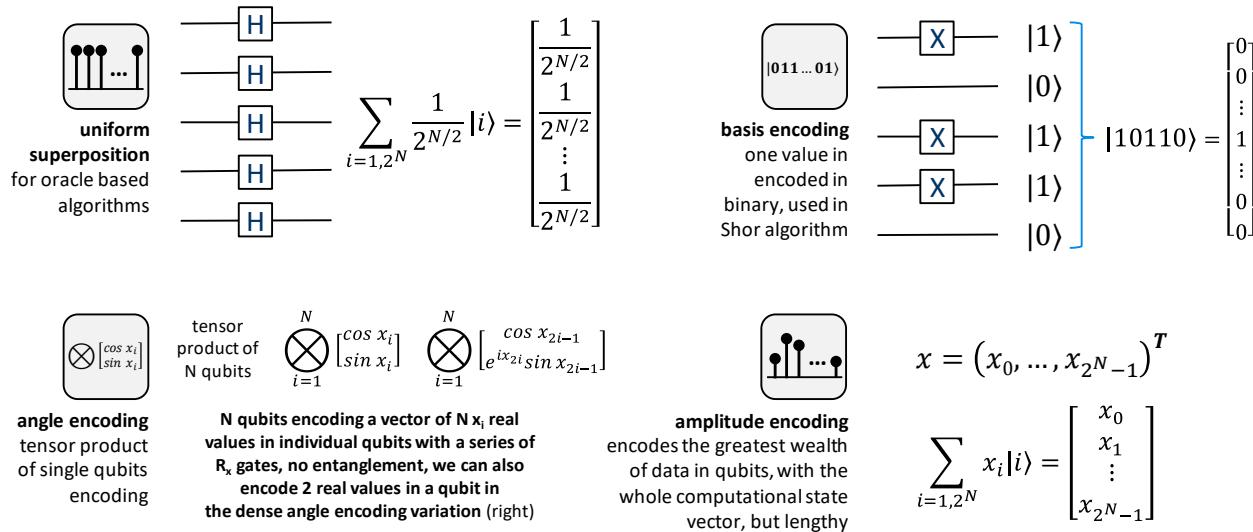
**Uniform superpositions** correspond to the simplest qubits register initialization with a register state where all the computational basis states have the exact same amplitude.

<sup>972</sup> Here are the various sources I used to reconstruct this map: [Loading Classical Data into a Quantum Computer](#) by John Cortese and Timothy Braje, 2018 (38 pages), [Circuit-centric quantum classifiers](#) by Maria Schuld, Krysta Svore et al, 2018 (17 pages), [Robust data encodings for quantum classifiers](#) by Ryan LaRose and Brian Coyle, 2018 (24 pages), [Towards a Pattern Language for Quantum Algorithms](#) by Frank Leymann, 2019 (12 pages), [Quantum linear systems algorithms: a primer](#) by Danial Dervovic et al, 2018 (55 pages) and [The Bitter Truth About Quantum Algorithms in the NISQ Era](#) by Frank Leymann and Johanna Barzen, 2020 (42 pages).

It is used by an oracle-based algorithm where the “real data” sits in the oracle function  $f(x)$  that outputs such and such values depending on the entry (usually, a 1 for a single entry and 0 for all the others). The oracle is able to evaluate this function simultaneously for all superposed computational basis values in the prepared superposed register. This superposition is done with applying Hadamard gates on all computing qubits where some data must be prepared.

**Basis encoding** consists in directly transferring N classical bits in N qubits, using a set of X gates (Y gates would also make it), to change individual qubits from  $|0\rangle$  to  $|1\rangle$ . It creates a simple encoding of a computational basis single state, combining 0s and 1s matching classical bits. The  $2^N$  dimensions computational basis state vector thus contains only zeros and a single one related to this combination. Before this encoding, we select the method to encode the problem data which can be for example a floating-point number or an integer in a given number of classical bits before converting them on a computational basis state. Such a basis encoding is used in Shor’s algorithm to provide the integer that must be factorized.

**Angle encoding** is about encoding a vector of real values of dimension N into N qubits. It’s also named product encoding. Each qubit is individually encoded with single qubit gates  $R_x$  (which themselves are usually decomposed in simple Pauli and T gates) to encode one of the (Bloch sphere) qubit angle. Since the register is the tensor product of each qubit, with no entanglement, we don’t have any exponential gain in the encoding. The dense angle encoding variation uses two angles in the encoding for each qubit and can make use, additionally of  $R_y$  and  $R_z$  gates for the sake of adding some phase in each qubit state. We end up here with a maximum of  $2N$  real numbers encoded in the N qubits register. And the qubit register is separable, its quantum state being separable into the quantum states of each of its qubits. It reminds us that without entanglement, you can’t benefit from the exponential storage (or, better, data handling) capacity of quantum computing. In that case, data encoding requires a depth of  $\log_2(N)$  gates.



**Amplitude encoding** is about creating an arbitrary superposed state associating computational basis states with given real number amplitudes. It is also called an arbitrary state preparation, quantum embedding or wavefunction encoding. It creates a computational state vector with real numbers in several rows. To encode a vector of L real values, you need  $N=\text{ceil}(\log_2(L+1))$  qubits. Meaning you round up the  $\log_2$  of the vector size and don’t use the left-over values in the register vector. Why +1? Because of the normalization constraint, the sum of amplitude being equal to 1. So with 3 qubits, you have 7 available values, not  $8=2^3$ . Since the size of your encoded vector may be smaller than the  $2^N$  states of your register, you’ll pad the encoded vector with 0s.

To create an arbitrary amplitude set for N qubits, you need at least  $\frac{1}{N} 2^N$  gates operations combining single and two qubit gates since an arbitrary amplitude encoding will create an entangled state contrarily to a simple product encoding. The usual encoding algorithms use  $2^N$  gates. So, unless the encoded data is sparse (with a lot of zeros), data preparation grows exponentially with the number of qubits, erasing any computing advantage we could get afterwards. It explains why quantum computing is not ideal for any big data computation task, and, at this point, for data intensive machine learning tasks!

**Encoding precision.** Angle and amplitude encoding theoretically deals with real numbers. But what is their precision, particularly on NISQ computers? It is at least bound by the cumulative error rates coming from the encoding qubit gates. It can easily reach a couple %, meaning the encoding precision is limited to a couple digits.

**Non linearities.** Quantum computing is based on using linear unitaries. This creates limitations on the kinds of computing that can be processed quantumly. But we can handle non-linearities indirectly. One way lies with the way real numbers are turned into the raw data to be encoded with angle or amplitude encoding. Another way is to use angle encoding with repetition, creating powers of encoded values in the computational state vector of the input vector. Finally, we can apply non linearities on the classical data before it's quantumly encoded. It can also be implemented as a classical Boolean non-linear circuit embedded in a quantum reversible circuit.

**How many registers?** In a classical microprocessor, the computing unit is handling data in multiple registers and the arithmetic logical unit can pull data from registers, make calculations and update registers with its results. In a quantum computer, there is usually only one register of N qubits. It can however be logically and dynamically partitioned by the algorithm. There are usually computing qubits and ancilla qubits. Computing qubits contain the input data related to the problem to be solved and that's on this data that most algorithm patterns will be executed, particularly with an oracle. The remaining qubits in the register will be used as accessory qubits and may also contain some part of the algorithm result. And this goes only with logical qubits. We've seen before that quantum error correction is using a lot of ancilla qubits.

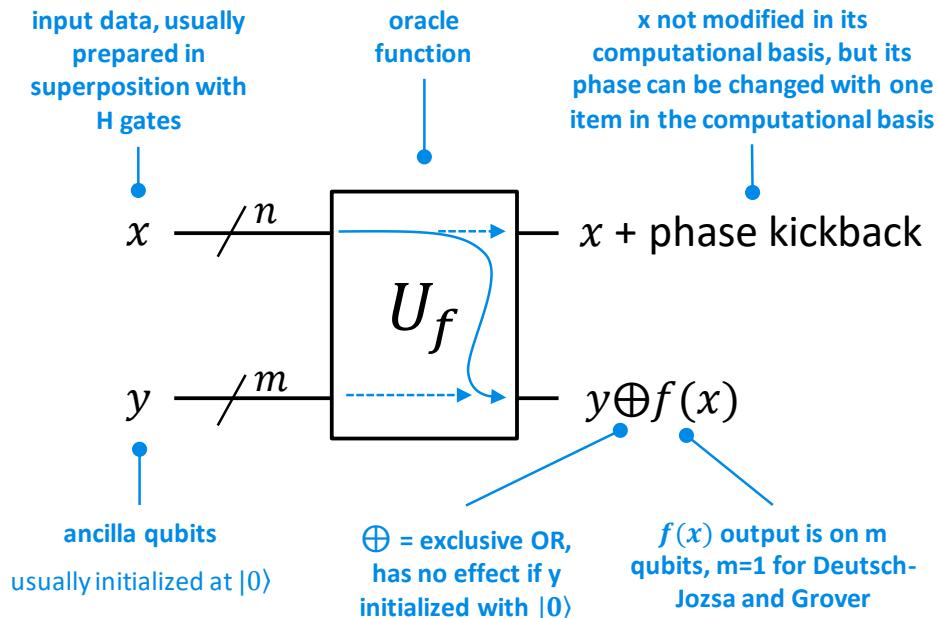
## Black boxes and oracles

A black-box based algorithm is a classical operation encoded with qubit gates that is applied simultaneously to various computational basis states. It's used in the famous Deutsch-Jozsa, Simon and Grover search algorithms. A black box contains reversible quantum equivalents of Boolean and arithmetic functions. It works on n entry qubits  $x$  in superposed states and merges its result with m ancilla qubits  $y$ , that are usually initialized at 0. It leverages quantum parallelism with input initialized with Hadamard gates. If  $m = 1$ , the black box outputs a yes or no (1 or 0) and is branded as an "oracle"<sup>973</sup>.

There are many ways to implement an oracle. It can be entirely encoded with qubit gates or access some classical memory or functions, presumably through some qRAM addressing scheme. Presumably since the technology doesn't exist yet. Even the cost of implementing an entirely quantum oracle is an unknown. For instance, just some complicated arithmetic functions can be highly costly in quantum gates since it may require implementing several QFTs (quantum Fourier transforms).

---

<sup>973</sup> See [Inverse Problems, Constraint Satisfaction, Reversible Logic, Invertible Logic and Grover Quantum Oracles for Practical Problems](#) by Marek Perkowski, May 2020 (62 slides).



$$|x\rangle|y\rangle \Rightarrow |x\rangle|y\rangle \oplus f(x)$$

Oracle-based algorithms speedup nearly never mention the potential computing overhead coming from the oracle itself. In an ideal world, the oracle implementation complexity should scale linearly and at worst polynomially with the number of handled qubits.

This overhead can be highly detrimental to any potential algorithm theoretical speedup. This is particularly concerning for Grover's algorithm that we'll look after later. This algorithm's speedup is only polynomial, before taking into account the oracle's cost, and of course, quantum error correction and non-Clifford gates generations as well. In the end, Grover's algorithm may not bring any acceleration at all.

In other words, touting some oracle-based algorithm speedup is like saying that a car drives fast thanks to its aerodynamism, without mentioning anything about its engine specifications and power.

## Output encoding

The literature covering quantum algorithms rarely explains what is the results format they are generating. There are as many variations as in data encoding. This section echoes the one that was dedicated on the various sorts of [qubits measurement](#), page 168. The most simple outcome of a quantum algorithm should be a computational basis vector with a series of  $|0\rangle$  and  $|1\rangle$ , generating a classical bit string like with Shor's factoring algorithm. In this case a single run and measurement provides full characterization of this outcome (modulo the error rate of the system). This is the case for many classical quantum algorithms as described in the table below.

However, some algorithms like HHL (linear equations) may generate data encoded in amplitude. Exploiting directly an amplitude encoded vector state doesn't make much sense since you lose any exponential advantage coming from the algorithm. Decoding a full vector state indeed requires running the algorithm several orders of magnitudes of an exponential of the number of qubits. But such an algorithm may be an intermediate one feeding another algorithm. If we keep using quantum data from end to end, then it makes sense to use and create algorithms that output amplitude encoded data.

algorithm	input	output
Deutsche-Josza	oracle function	function is balanced if all output qubits are at ground state $ 0\rangle$
Bernstein-Vazirani	oracle function	(integer) secret string in basis encoding
Grover	oracle function	searched item index as integer in basis encoding
Simon	oracle function	parameters for a linear equation used to find a period, with average of basis encoding
Shor factoring	integer in basis encoding	integer in basis encoding
Shor dlog	integers in basis encoding	integer in basis encoding
QFT	series of complex amplitudes with amplitude encoding (any quantum input state)	Fourier coefficients in amplitude encoding, enabling the recovery of the main frequency
HHL	one vector and one matrix amplitude encoding	characteristics of inverted matrix x entry vector (= one vector) in amplitude encoding
VQE	cost function parameters encoded as an Hamiltonian with unitaries (quantum gates)	researched ground state in amplitude encoding
QML classification	object vector to classify encoded in amplitude	prediction result as an integer index in basis encoding

(cc) Olivier Ezratty, October 2021

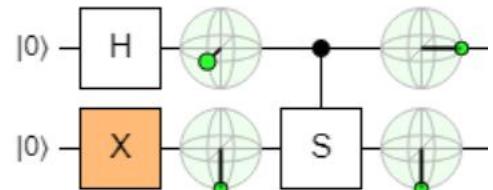
## Quantum phase kickback

The role of an oracle is to change the phase of the found item in the computational basis state vector  $x$ . Instead of sending the phase to the ancilla qubit  $y$ , it is applied to the found result in the source  $x$  qubits thanks to the phase kickback mechanism. It is implemented for example in the Grover algorithm that we'll see later.

The Grover operator then amplifies the amplitude of the found item and attenuates the amplitude of the other items in the computational basis, leveraging this phase information injected in the  $x$  computational basis vector state.

For this to work, the control qubits must be in a superposed state, created by Hadamard gates initialization, the target qubit  $|\psi\rangle$  must be an eigenvector of the operator  $U$  applied to the target qubit  $|\psi\rangle$  using the control qubits<sup>974</sup>.

This simple two qubits configuration explains what's happening. A control-phase gate ends up modifying the phase of the control qubit instead of the phase of the target qubit. It works in the example case since after the X gate being applied to the target qubit, the qubit state becomes an eigenvector of the control-S operation that is executed afterwards<sup>975</sup>.



It is not changed by a phase rotation. Since a control-phase changes the global phase of both qubits, the phase modification can only happen on the control qubit. Despite the entanglement created by the control-S gate, the qubits remain separable. So, in a general case, when the target qubit  $|\psi\rangle$  is an eigenvector of the unitary  $U$  (here, a S gate), the target qubit doesn't change after the control-U gate. Literally:  $U|\psi\rangle = e^{i\phi}|\psi\rangle$ . The control qubit changes and one of its computational state vector amplitudes gets multiplied by the eigenvalue of the eigenvector of  $U$ .

<sup>974</sup> As explained in [Phase Kickback](#) by Eduard Smetanin, November 2019 (4 pages).

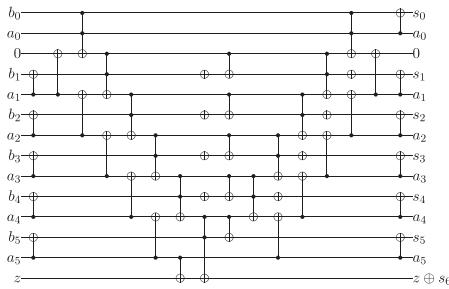
<sup>975</sup> This is explained in [A clever quantum trick](#) by Emilio Peláez, January 2021. See also [Quantum Phase Kickback - What I told you was true... from a certain point of view](#) by Frank Zickert, March 2021.

## Arithmetic

Arithmetic functions can be implemented in a quantum algorithm. It's mostly used in oracles. There are many quantum algorithms around that implement various arithmetic functions: adders, multipliers, dividers and even transcendental functions (exponential, logarithm, and trigonometric functions)<sup>976</sup>.

**arithmetic operations can be useful in many algorithms**

**quantum reversible adders/multipliers can be derived from their classical counterparts (ripple-carry adders) or use a QFT and IQFT (inverse QFT) to reduce the need for ancilla qubits**



The ripple-carry adder for  $n = 6$ .

**6-bit ripple-carry addition adder**

Adder type	Toffoli/T depth	Toffoli/T gates	Qubits required
Majority ripple [12]	$2n$	$2n$	$2n + 1$
Prefix-ripple [Section A.1]	$n$	$3n$	$2n + 1$
Carry look-ahead [13]	$4\log_2(n)$	$10n$	$4n - \log_2(n) - 1$
Fourier transform basis [33]	$3\log_2(1/\epsilon)$	$3n\log_2(1/\epsilon)$	$n$

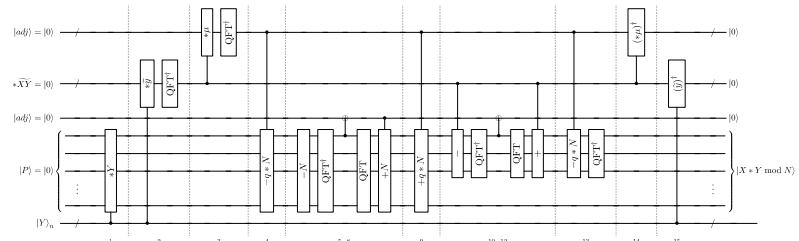


Figure 12: Barrett multiplication circuit using Fourier arithmetic. The numbers in the figure correspond to the steps of Algorithm 2.

**Barrett multiplication circuit using QFT**

sources: A new quantum ripple-carry addition circuit by Steven A. Cuccaro, Thomas G. Draper, Samuel A. Kutin and David Petrie Moulton, 2008 (9 pages) and High performance quantum modular multipliers, Rich Rinesyand and Isaac Chuang, 2017 (48 pages).

Quantum reversible adders and multipliers can be derived from their classical counterparts like with ripple-carry adders, or use a QFT and IQFT (inverse QFT) to reduce the need for ancilla qubits.

## Amplitude amplification

Amplitude amplification is a gate combination that is frequently connected to the phase kickback mechanism. It consists in amplifying one particular amplitude of the computational state vector of the control qubits that are submitted to an oracle function, at the expense of all the other amplitudes. It is used for example in the Grover operator from the Grover search algorithm as we'll see later.

In 2021, a researcher from the Fermi Lab at the DoE found a way to create an amplitude amplification working on a non-Boolean oracle<sup>977</sup>.

## Quantum Fourier Transform

Classical Fourier transforms are used to decompose a signal into its compound frequencies. In signal theory, this allows to identify the basic components of some sound by breaking it down into frequencies. In astrophysics, the atomic composition of stars is determined by a decomposition of the light spectrum, but this is done by an optical prism and not by Fourier transform. The same is true for Scio-type near-infrared sensors that determine the composition of food. A prism and the principle of diffraction therefore allow an optical Fourier transform to be performed.

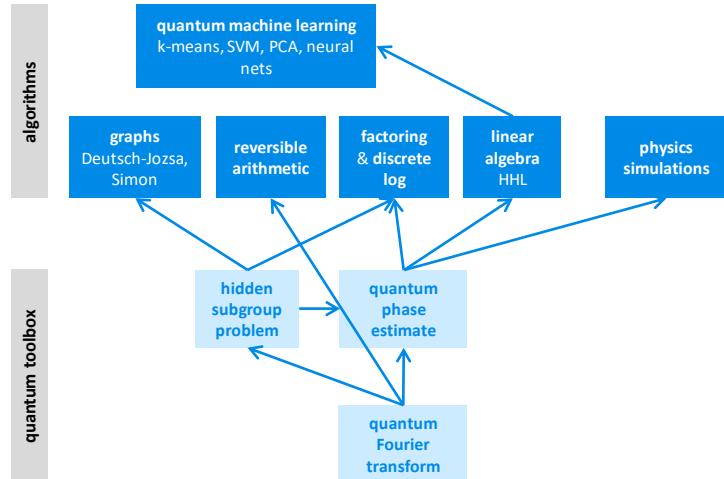
The quantum Fourier transform was invented by **Don Coppersmith** (USA) in 1994.

<sup>976</sup> Sources: [A new quantum ripple-carry addition circuit](#) by Steven A. Cuccaro, et al, 2008 (9 pages), [High performance quantum modular multipliers](#), Rich Rinesyand and Isaac Chuang, 2017 (48 pages) and [Quantum circuits for floating-point arithmetic](#) by Thomas Haener, Mathias Soeken, Martin Roetteler and Krysta Svore, 2018 (13 pages) which were [patented](#). See also [Arithmetic on Quantum Computers: Addition, Faster](#) by Sashwat Anagolum, October 2018 and [Arithmetic on Quantum Computers: Multiplication](#) by Sashwat Anagolum, December 2018.

<sup>977</sup> See [Non-Boolean Quantum Amplitude Amplification and Quantum Mean Estimation](#) by Prasanth Shyamsundar, February 2021 (36 pages).

A QFT is a quantum equivalent of a DFT or a FFT (Fast Fourier Transform). Its inverse operation, an inverse QFT is a QFT executed backwards, with its gates serialized in reverse order.

QFT is everywhere in the algorithm zoo! Many known quantum algorithms are using it, including QPE (quantum phase estimation), HHL (linear equations), Shor's factoring algorithm and most QML algorithms. QFT helps find periodicity in a series of numbers, which is particularly helpful in Shor's algorithm.



A QFT is decomposing a series of qubits computational base states complex amplitudes in frequencies<sup>978</sup>. The complex amplitude data encoding sits in the prepared register of qubits  $|x_i\rangle$  with  $i=0$  to  $n$ , as shown below.

These qubits contain a set of  $N=2^n$  amplitudes  $\alpha_j$  of the computational state basis orthogonal vectors  $|j\rangle$ , with  $j=0$  to  $N-1$ .

The QFT implements a Discrete Fourier Transform (DFT) on these discrete amplitudes and converts it into a new computational state vector with amplitudes being the result of the QFT. The initial vector state can be written as:

The QFT creates a new state vector  $\text{QFT}_N(|\psi\rangle)$  with  $\beta_k$  amplitudes of computational basis vectors  $|k\rangle$ .

The computed amplitudes  $\beta_k$  are computed with a big sum using all the amplitudes  $\alpha_j$  with the coefficient  $\omega^{jk}$ .

These coefficients  $\omega^{jk} = e^{\frac{-2\pi i}{N}jk}$  explain the heavy use of  $R_n$  phase rotation gates in the QFT algorithm as described below. And you remove the minus sign to get a reverse QFT.

In the end, the  $\text{QFT}_N$  is a unitary matrix transformation  $[\text{QFT}_N]$  with simple coefficients  $[\text{QFT}_N]_{jk}$ , as in a DFT.

When  $n=1$  and  $N=2$ , the QFT becomes a Hadamard gate transform. The QFT is indeed presented as a generalization of the Hadamard operation, applied to dimensions  $N>2$ .

Since preparing an arbitrary such vector could take an exponential time with regards to the number of qubits, it is usually done through some faster preparation mechanism like in Shor's algorithm.

What are we really getting out of a QFT? Let's say we have 4 qubits and complex amplitudes with a rotating phase by  $45^\circ$  steps. It means we'll have a full phase periodic rotation for each 8 amplitudes

$$|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$$

$$\text{QFT}_N(|\psi\rangle) = \sum_{k=0}^{N-1} \beta_k |k\rangle$$

$$\beta_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i \frac{jk}{N}} \alpha_j$$

$$\beta_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{jk} \alpha_j$$

$$[\text{QFT}_N]_{jk} = \frac{1}{\sqrt{N}} \omega^{jk}$$

<sup>978</sup> See [Quantum circuit for the fast Fourier transform](#) by Ryo Asaka et al, 2020 (20 pages) which describes a QFT variant using a faster basis encoding for the input register.

and 2 full rotations for the whole state vector. The QFT will then output a register with the third qubit at  $|1\rangle$  and all the others at  $|0\rangle$ .

This third qubit corresponds to the value 2, which is the frequency of the phase rotation. But we could have a more complex QFT with several added frequencies in the signal.

Getting all the  $\beta_k$  coefficients and frequencies still wouldn't make much sense. Indeed, recovering a whole computational basis state would require running the QFT at least one or two orders of magnitudes of  $2^N$ . We'd lose any quantum speedup. What is usually done is to directly reuse this vector in the remainder of another quantum algorithm like Shor. Otherwise, after running the QFT a limited number of times, we can extract the computational basis state with the highest frequency. In other words, it means we'll have the main frequency extracted from the QFT, but not all of them.

The QFT relies on two types of logic gates: Hadamard gates to perform an overlay and two-qubit phase-controlled R gates whose phase is inversely proportional to 1 up to N. This creates a huge problem of accuracy in the calculation: the larger N is, the smaller the angle of rotation of the qubit in its Bloch sphere will be and the more impacting the phase errors will be. This requires a very precise control of the activation of the qubits.

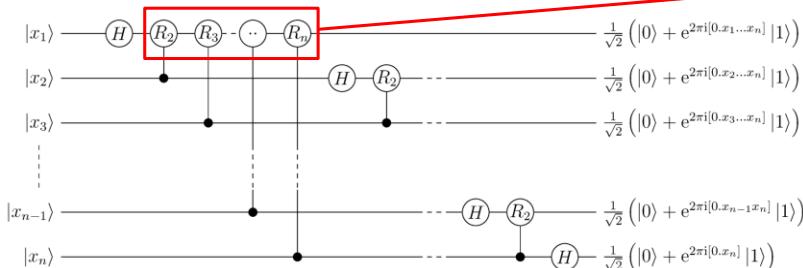
In practice, phase-controlled R gates are generated by a combination of H, Z and T gates, plus a CNOT for the entanglement of the control qubit with the target qubit.

And it takes a lot! For example, for an  $R_{15}$  gate, 127 H/Z/T gates must be used to obtain an accuracy of  $10^{-5}$ , which is enormous<sup>979</sup>. This can be optimized with auxiliary qubits. And of course, we must integrate the associated error correction codes that add a good order of magnitude to the number of quantum gates in the depth of the calculation. This mainly impacts the calculation duration since the error correction codes are supposed to lengthen the duration of the qubit coherence.

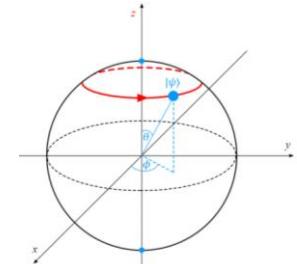
**decompose a series of qubits in frequencies**

**used in Shor algorithm and also arithmetic algorithms (adders, multipliers)**

$$R_m = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^m}} \end{pmatrix}$$



**controlled R phase gate**



$$N * \log(N) \Rightarrow \log^2(N)$$

**exponential speed gain**

nbr	classical time	quantum time
5	3,5	0,5
48	81	2,8
128	270	4,4
512	1387	7,3
1024	3082	9,1

For an  $R_{2048}$  gate, the last of a long series to break a 2048-bit RSA key? That's about the same number of gates. This comes from the Solovay-Kitaev theorem according to which this decomposition

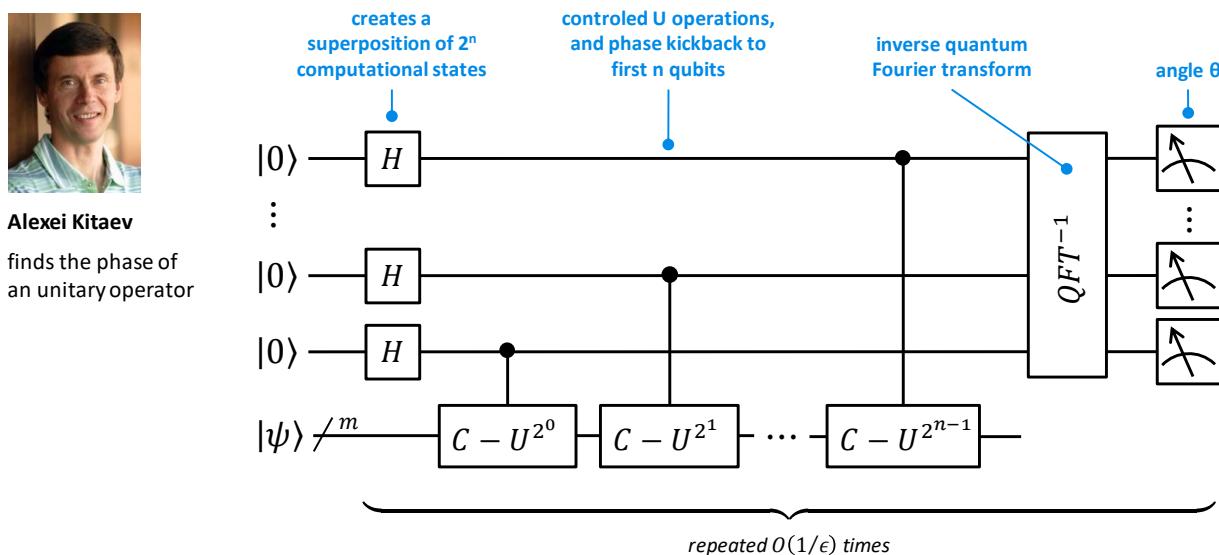
<sup>979</sup> See [Efficient decomposition methods for controlled-R n using a single ancillary qubit](#) by Taewan Kim et Byung-Soo Choi, 2018 (7 pages) and [Approximate quantum Fourier transform with O\(n log\(n\)\) T gates](#) by Yunseong Nam et al, 2020 (6 pages).

depends only on the targeted error rate<sup>980</sup>. In the case of superconducting qubits, the generation of variable phase gates is achieved by sending a shorter microwave pulse.

## Quantum phase estimation

Quantum phase estimation is an algorithm used to find the phase of an eigenvector of a unitary operator  $U$ . This operator can be implemented as an oracle function applied to a quantum state  $|\psi\rangle$  that is decomposed in  $n$  controlled-unitaries operating on  $m$  qubits from  $|\psi\rangle$ . We are then looking for the phase angle  $\theta$  according to  $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ .

This algorithm is based on an inverse QFT. Practically speaking, the QPE can estimate the angle  $\theta$  with a precision  $\epsilon$  with executing  $U$  for  $O(1/\epsilon)$  times (meaning, with a high probability within an error  $\epsilon$ ). The angle  $\theta$  is encoded over  $n$  classical bits at the exit of the inverse QFT.



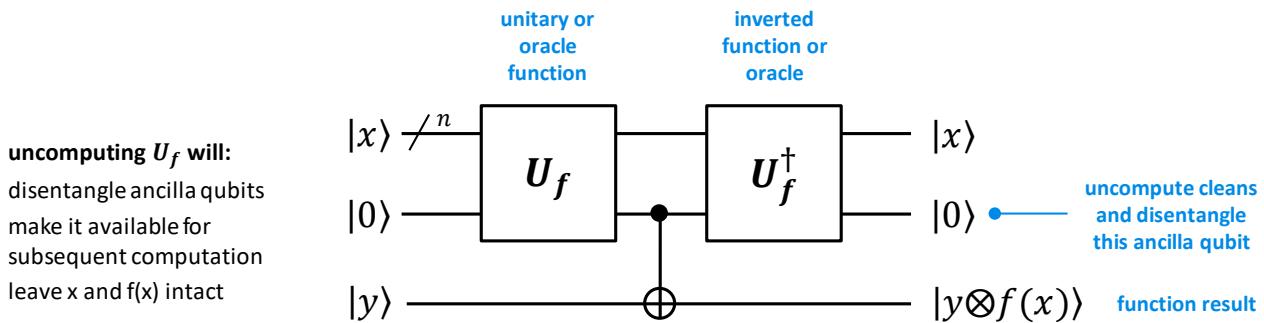
This algorithm was proposed by Alexei Kitaev in 1995<sup>981</sup>. It is used among other domains in quantum chemistry and in Shor's factoring algorithm.

## Uncompute trick

The uncompute trick was created by Charles Bennet in 1989. It is used to rewind some parts of an algorithm affecting ancilla or input qubits. It cleans up the state of a qubits register without requiring a qubit reset that may damage the stored values in the qubits with the algorithm results. It is also used to disentangle the ancilla qubits from the input qubits. It then makes it possible to go on using these ancilla qubits for the remainder of the algorithm. In a word, it cleans up the qubits register garbage at the end of some computing. The transformation works if the unitary  $U_f$  is a reversible circuit which is the case for any combination of quantum gates (without any measurement done in between).

<sup>980</sup> The main method of  $R_n$  gate decomposition is documented in [Optimal ancilla-free Clifford+T approximation of z-rotations](#) by Neil J. Ross and Peter Selinger, 2016 (40 pages). It's cotton!

<sup>981</sup> New versions appear from time to time like [Quantum Algorithm for the Direct Calculations of Vertical Ionization Energies](#) by Kenji Sugisaki et al, University of Osaka, March 2021 (6 pages).



The uncompute trick is often used when the algorithm is running an oracle function. But it presumes we are working with “clean” qubits with no error. In a NISQ setting, an oracle inversion would generate so many errors that it would invert nothing.

## Linear equations

Many other quantum algorithms exist that allow complex mathematical operations such as solving differential equations, inverting matrices, or processing various linear algebra problems. They are then used elsewhere as in QML.

The best-known algorithm is the **HHL**, named after its creators Harrow, Hassidim and Lloyd, and created in 2009. It allows to solve linear equations, with an exponential performance gain.

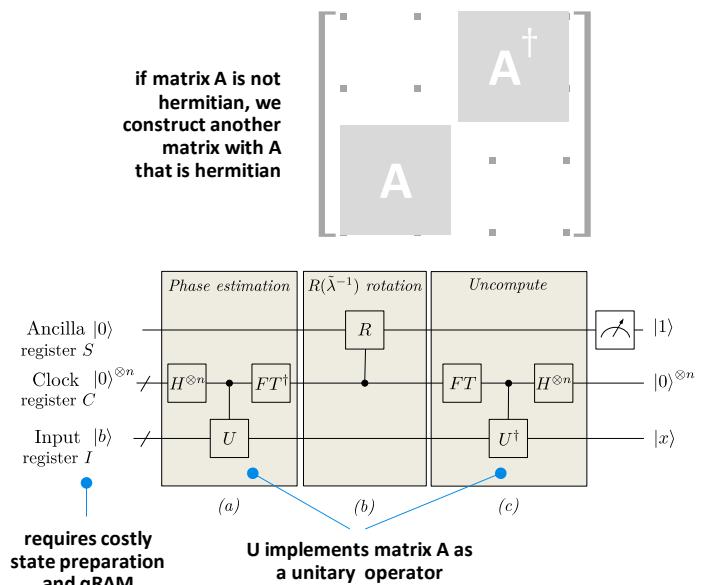
The HHL algorithm input is combining a  $2^N \times 2^N$  sparse Hermitian matrix  $A$  (or is prepared to be Hermitian, see schema below) and an input state  $|b\rangle$  with  $2^N$  amplitudes. Its output is  $|x\rangle = |A^{-1}b\rangle$ . Namely, it inverts matrix  $A$  and multiplies it by  $|b\rangle$ . The processing is done in time  $O(N)$  with an exponential speed-up. But the state  $|b\rangle$  must be prepared in some sort of qRAM that doesn’t exist yet or be prepared quantumly. Also, input matrix  $A$  must follow a lot of constraints, with a having only a few non zero values (sparsity).

**Harrow, Hassidim and Lloyd developed the HHL algorithm in 2009 which quantum mechanically inverts a system of linear equations. solves the system of equations  $A\vec{x} = \vec{b}$  where:**

- $A$  : sparse square hermitian matrix  $n \times n$
  - $\vec{b}$  : vector with  $n$  values
  - $\vec{x}$  : solution vector to be characterized
- requires inverting a matrix and uses a quantum phase estimate.**
- part of the QBLAS algorithms family**  
(Quantum Basic Linear Algebra Subroutines)  
**used in many QML algorithms.**

$$N * \log(N) \Rightarrow (\log(N))^2$$

exponential speed gain, but finding the full  $\vec{x}$  vector requires  $O(N)$  repetitions!



There's a caveat, that Scott Aaronson explained well in 2015<sup>982</sup>. The HHL output is a quantum state  $|x\rangle$  that can't be read right away. The vector can be read to get some statistical information about it or, among other stuff, an evaluation of a dot product between  $|x\rangle$  and another vector  $|z\rangle$ . If you want to know everything about  $|x\rangle$ , you'll need to repeat the operation  $2^N$  times and lose any exponential advantage gained in the first place. In the end, HHL is not really inverting the matrix A with a real exponential speedup.

## Hamiltonian simulation

Literally, as we've seen when describing [Schrödinger's wave equation](#), a Hamiltonian of a quantum system is its description and evolution of its total energy, including kinetic and potential energy, over time. It's hard to evaluate for a given single quantum object and even harder for a multi-objects system. That's what Hamiltonian simulations are all about. One of their goals is to find the total energy of a system and its approximate ground state configuration which usually corresponds to its natural lowest-energy equilibrium state. It is particularly important in condensed matter physics and in organic chemistry.

In that later case, it makes it possible to find the way molecules are naturally organized in three dimensions, from simple peptides to large proteins. It could also theoretically help simulate the interactions between different molecules.

Simulating a Hamiltonian was at the core of Richard Feynman's idea coined in 1981 when he wondered whether a quantum system could simulate another quantum system more efficiently than a classical computer, breaking down the fatal exponential growth of computing resources required to implement this kind of simulation on classical computers.

Such a simulation problem is described by a Hamiltonian which is a Hermitian matrix H of size  $2^N \times 2^N$ , when working with N qubits or N two-states quantum objects like spin-1/2 particles.

The quantum system evolves over time according to (1), given  $e^{itH}$  is the exponential of H (times i and t), is a unitary matrix. It is a solution to the Schrödinger equation (2):

$$(1) \quad |\psi(t)\rangle = e^{itH}|\psi(0)\rangle \quad (2) \quad i\hbar \frac{\partial \psi(t)}{\partial t} = E\psi(t).$$

Simulating a Hamiltonian consists in finding matrix H or some characteristics of H. That simple. Or not.

The technique of the local Hamiltonian problem is a simplification of a Hamiltonian simulation. Thanks to special and general relativity, a Hamiltonian evolves according to local interactions. All Hamiltonian evolutions with only local interactions can be simplified as a combination of Hamiltonians acting on a limited space with at most  $\ell$  of the total of N variables<sup>983</sup>.

Finding a system ground state of a local Hamiltonian is a QMA-complete class problem that can theoretically be efficiently solved on a quantum computer (QMA is defined later...)<sup>984</sup>. Efficiently means with a polynomial instead of exponential growth in qubits. It mandates the usage of some quantum certificate or quantum proof, a validation technique used with QMA problems processing<sup>985</sup>.

<sup>982</sup> See [Read the fine print](#) by Scott Aaronson, Nature Physics, 2015 (3 pages).

<sup>983</sup> See [Using Quantum Computers for Quantum Simulation](#) by Katherine L. Brown et al, 2010 (43 pages).

<sup>984</sup> See [QMA-completeness: the Local Hamiltonian Problem](#) by Paul Fermé, based on lecture notes by Umesh Vazirani and lecture notes by Thomas Vidick, 2015 (6 pages).

<sup>985</sup> See [Lecture 20: Local Hamiltonian ground state problems](#) by Richard Kueng, on a course from John Preskill, December 2019 (17 pages).

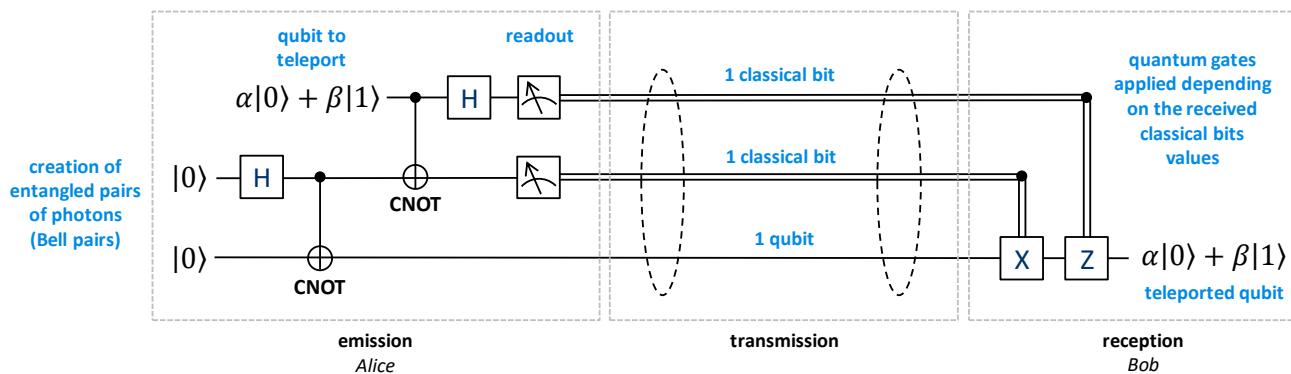
There are of course many variations of Hamiltonian simulations depending on the type of quantum system to emulate and the characteristics we want to extract from H. It includes hybrid solutions associating classical and gates-based quantum computing including the quantum adiabatic algorithms.

If the Hamiltonian is of the family of an Ising model, it can be simulated using quantum annealers or quantum simulators. There are other families of Hamiltonians that can be simulated on quantum simulators or coherent quantum annealers with more than one degree of freedom (see Qilimanjaro).

## Quantum teleportation

One of the most intriguing quantum gate-based quantum algorithms is qubit teleportation. It was created by Charles H. Bennett (USA), Gilles Brassard (Canada), Claude Crépeau (Canada), Richard Jozsa (USA), Asher Peres (Israel) and William K. Wootters (USA) in 1993<sup>986</sup>.

It allows to teleport the state of a qubit from one place to another. The principle of this algorithm consists in exploiting a pre-existing quantum entanglement channel to transmit the state of a qubit from one end of this channel to the other. Teleportation involves the transmission of two classical bits in the protocol that are used to reconstitute the qubit sent on arrival. As a result, the transmission of the latter cannot be faster than light.



(cc) Olivier Ezratty, 2020

Due to the quantum no-cloning theorem, this teleportation is a "move" and not a "copy" (or a "cut & paste" instead of a "copy & paste" to use an easy to understand analogy). The state of the transferred qubit is thus destroyed at its origin<sup>987</sup>. The main use case of this algorithm and its many variants are in quantum cryptography and telecommunications systems that we will discover later.

It could also be used in distributed quantum computer architectures. Note that this algorithm can be tested locally in a quantum computer, as proposed by IBM in its Q Systems with Qiskit.

## Higher level algorithms

We'll now cover higher level algorithms which are based on the algorithms toolbox described in the previous part<sup>988</sup>. Quantum software engineering requires three main set of skills: having an understanding of both low and high-level algorithms, then some know-how about the way these algorithms can be assembled and also coupled with classical algorithms, and then, above all, how to find the ways to translate "business problems" into these algorithms.

<sup>986</sup> See [Teleportation as a quantum computation](#) by Gilles Brassard, 1996 (3 pages).

<sup>987</sup> See [Quantum Teleportation in a Nutshell](#) by Fabian Kössel, 2013 (35 slides).

<sup>988</sup> See [Quantum Algorithms](#) by Ashley Montanaro, July 2016 (62 slides), [Quantum algorithms: an overview](#) by Ashley Montanaro, 2015 (16 pages), [Quantum Algorithm Implementations for Beginners](#), 2020 (94 pages).

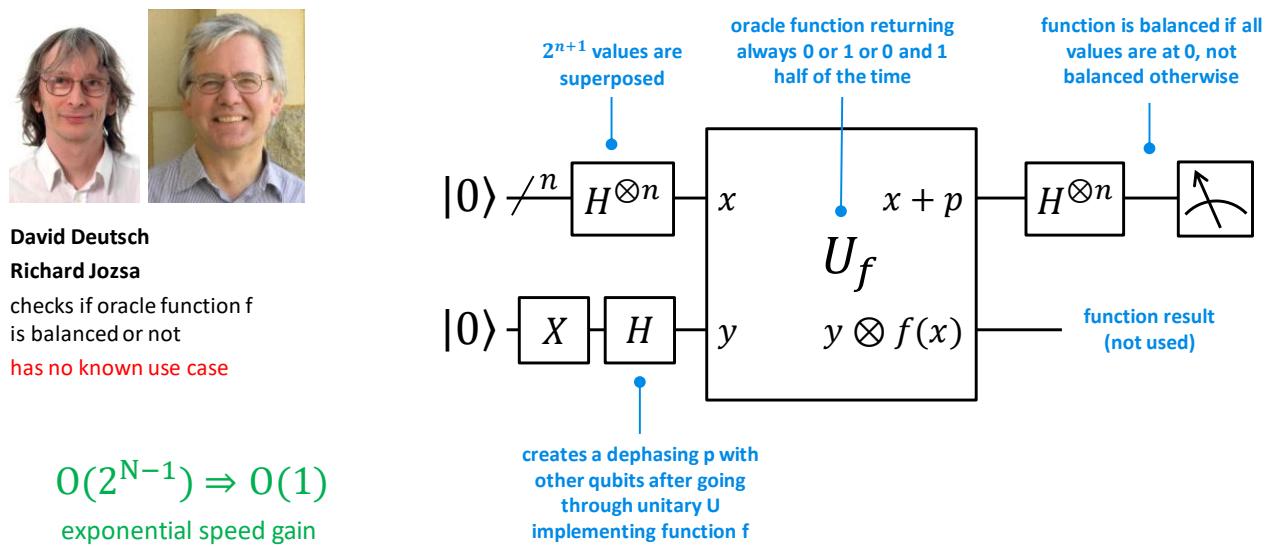
## Oracle-based algorithms

One of the first quantum algorithms invented comes from David Deutsch, with its derivative called **Deutsch-Jozsa**, co-invented with Richard Jozsa and created in 1992. This algorithm makes it possible to characterize a function  $f()$  called an "oracle" for which we know in advance that it will return for all its inputs, either always the same value, 0 or 1, or the values 0 and 1 in equal parts. The algorithm makes it easy to determine if the function  $f()$  is balanced or not. It is working to a set of qubits  $n$ . Function  $f()$  is making some classical computing on each  $2^N$  values from the computational basis of  $n$  qubits.

The input qubits are all initialized to  $|0\rangle$  except one which is initialized to  $|1\rangle$ . They are then all superposed between  $|0\rangle$  and  $|1\rangle$  with Hadamard gates. The qubits are thus said to have simultaneously all possible  $2^{N+1}$  combinations of values.

It is easy to understand why this quantum algorithm is much more efficient than its traditional version: in traditional computation, more than half of the possible input values would have to be scanned sequentially, whereas in the quantum version, they are all analyzed at the same time by the oracle function working on all  $2^N$  values of the first  $N$  qubits. The result is obtained with a few series of quantum gates, almost instantaneously, and it is perfectly deterministic.

These superposed qubits are processed by the oracle which contains a set of gates implementing function  $f()$  to be evaluated. The output is then measured to see if the function is balanced or not thanks to other Hadamard gates.



The initialization of the last qubit to  $|1\rangle$  is used to generate an interference with the other qubits that will impact the values leaving the H gates after passing through the oracle. The function  $f()$  is constant if the final measurement gives  $|000 \dots 0000\rangle$  and unbalanced otherwise<sup>989</sup>.

What is the practical interest of such an algorithm given there are rather few functions  $f()$  of this kind? This is an example of an ultra-powerful algorithm that has no known practical use to date. On top of that, there are very efficient classical probabilistic algorithms that are fast and cancel a good part of the quantum power gain coming from the Deutsch-Jozsa algorithm.

This is particularly the case with the Monte Carlo search algorithm which evaluates the oracle function on a limited number of randomly selected inputs.

<sup>989</sup> To find out how it works in detail, you can see the [associated mathematical formulas](#) as well as Eisuke Abe's [Deutsch-Jozsa Algorithm](#) presentation, 2005 (29 slides). But it is not that obvious!

The probability of errors depends on the number of evaluations and decreases very quickly<sup>990</sup>.

So quantum computing is useless? Of course not. Other algorithms, less powerful but much more useful, have emerged since this patient zero of quantum algorithmics!

**Bernstein-Vazirani's** algorithm is less talked-about in textbooks. This algorithm created by Ethan Bernstein and Umesh Vazirani in 1992 is a variant of the Deutsch–Jozsa algorithm. Instead of using two different classes of functions, it tries to learn a secret string encoded in an oracle function. The algorithm was designed to prove an oracle separation between complexity classes BQP and BPP. The speedup of this algorithm is polynomial but a derivative recursive version of the algorithm has an exponential speed gain<sup>991</sup>. The algorithm has not much practical use cases although it could be used in some cryptography cases<sup>992</sup>.

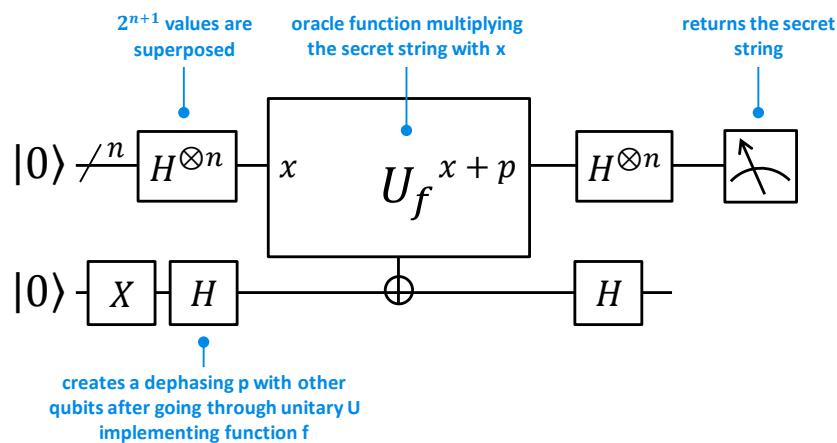


Ethan Bernstein and Umesh Vazirani - 1992

learns a secret string encoded in an oracle function

$O(n) \Rightarrow O(1)$

exponential speed gain



**Simon's** algorithm is a more sophisticated variant of the Deutsch–Jozsa algorithm<sup>993</sup>. It consists in finding the combinations of values that verify a condition imposed by the oracle function. It solves the so-called hidden subgroup problem (HSP). Its performance gain is very interesting and, this time, the algorithm is useful, particularly to solve path problems in graphs like with quantum walks. The gain in performance is typical of what quantum computing can bring: we go from a classical calculation which is exponential time ( $2^{N/2}$ ) to a linear time in N.



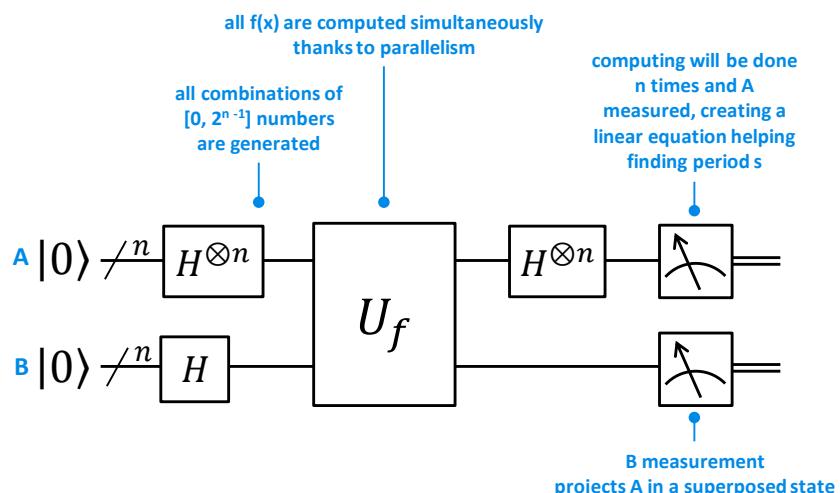
Daniel Simon

search a subset of numbers matching a condition imposed by unknown oracle function f, so that  $f(x')=f(x)$  if  $x'=x \oplus s$

indirectly used in QFT and Shor

$2^N \Rightarrow N$

exponential speed gain



<sup>990</sup> See on this subject the document [Quantum Computation Models](#) (30 pages).

<sup>991</sup> The algorithm is well explained in the [Qiskit documentation](#).

<sup>992</sup> See [Using Bernstein–Vazirani algorithm to attack block ciphers](#) by Huiqin Xie et al, 2019 (22 pages).

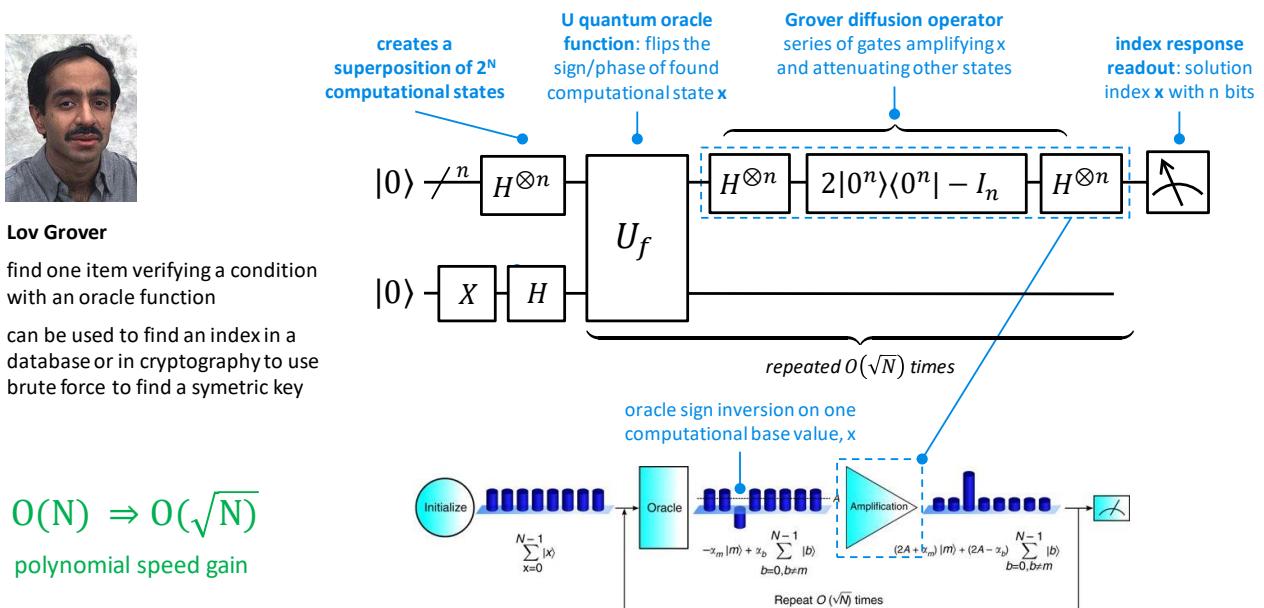
<sup>993</sup> It is documented in [On the power of quantum computation](#) by David Simon, 1997 (10 pages).

The other best-known algorithm in this category is **Grover's algorithm**, created in 1996 by Lov Grover. It allows to perform a fast quantum search in a database. It's however more generic: it can find an item in a long list that matches some specific criteria specified by an oracle function like finding the minimum item of an unsorted list of N integers, determining if a graph of N vertices is connected, or doing pattern matching searches, which can be useful in genomics.

The Grover oracle function is supposed to return 1 only for one combination of 0 and 1 with N bits. It also uses qubit state superposition to speed up processing compared to a traditional sequential search in an unsorted and non-indexed database. The performance improvement is significant compared to an unsorted database, except that in real life, we usually use indexed databases!

The question is to know if a 1 is yielded once and to which input combining 0 and 1s it corresponds. To do this, again with Hadamard gates, the algorithm will gradually amplify the combination of qubits of the result to an amplitude approaching 1 and make the other combinations of qubits converge to 0.

It will then be possible to measure the result and obtain the combination of qubits with the desired value (still, with repeating the algorithm several times and making an average of the results). This is well explained in the diagram *below*<sup>994</sup>.



The computing time is proportional to the square root of the base size and the storage space required is proportional to the logarithm of the base size. A classical algorithm has a computation time proportional to the size of the base. Going from a time  $N$  to  $\sqrt{N}$  is therefore an interesting gain, but it will not transform an exponential size problem into a polynomial size problem ( $2^N$  to  $N$  power M).

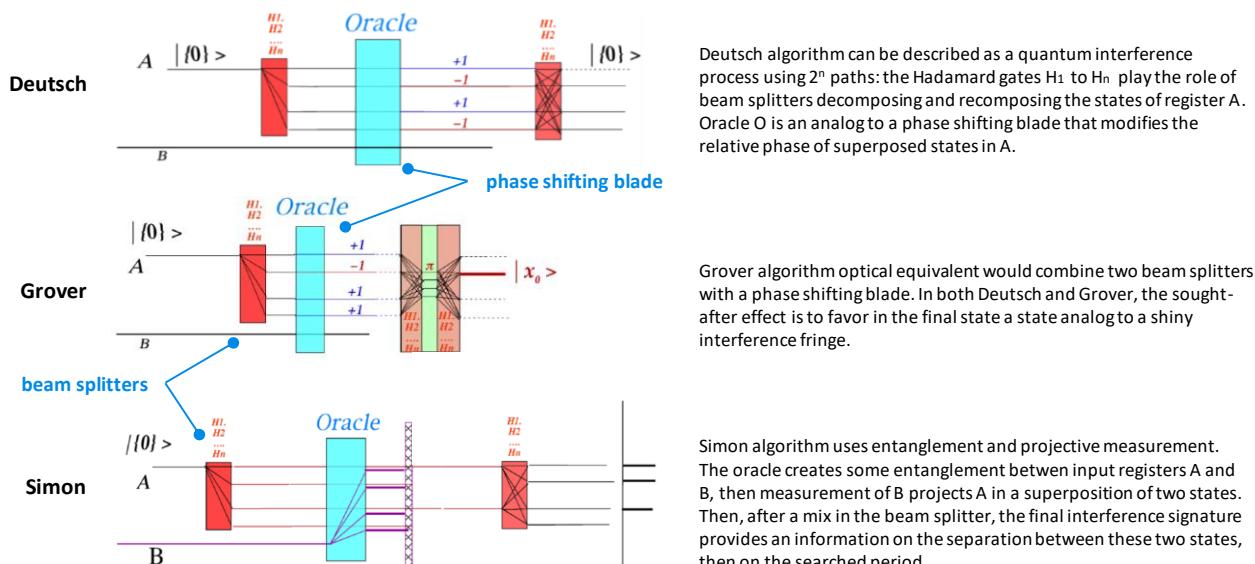
On the other hand, this algorithm can be exploited to be integrated into other algorithms such as those that allow the discovery of the optimal path in a graph or the minimum or maximum number of a series of N numbers. Grover's algorithm is also used in some quantum machine learning algorithms like for measuring min/max/mean distance or other metrics between set so of data points and for automatic clustering.

<sup>994</sup> Schematic source: [Quantum Computing Explained for Classical Computing Engineers](#) by Doug Finke, 2017 (55 slides). The link does not seem to be operational in July 2019.

Note that Grover's search algorithm requires the use of quantum memory (qRAM) to "load" the related database in memory, in the oracle function<sup>995</sup>! There are however some available optimization techniques available for quantum state preparation in the Grover oracle<sup>996</sup>.

In a 2002 lesson, **Serge Haroche** points out the known fact that these search algorithms have quantum optical equivalent implementations, as described *above* with 4 qubits. This has been described for a while, even trying to use only classical optical elements.

Various papers argue that, from a practical standpoint, these implementations don't scale well with a growing number of qubits, but they remind us that quantum algorithms are toying with waves and interferences and that optical analogies are well suited to understand their underlying processes<sup>997</sup>.



from: Serge Haroche, Chaire de Physique quantique. Année 2001-2002. 8 ème leçon. 26 Février 2002. Les algorithmes quantiques.

At last, let's remind again the reader that an oracle-based algorithm is efficient if the oracle itself is efficient, which depends on its implementation. If it is accessing some classical data or function, the algorithm's efficiency may questionable in the end.

### Shor integer factoring

Shor's factoring allows you to decompose integers into prime numbers much faster than with a traditional computer. It works in three stages: a QFT (quantum Fourier transform) that decomposes the integer to factorize, a period finding problem solver that looks to some repetition and an inverse QFT that reformats the result obtained by the period finding part of the algorithm. The algorithm operation is described in the diagram *below*<sup>998</sup> and in this rather clear explanation seen in a [video from PBS](#)<sup>999</sup>.

<sup>995</sup> This is notably documented in [Quantum algorithms for linear algebra](#) by Anupam Prakash, 2015 (92 slides).

<sup>996</sup> See [Black-box quantum state preparation without arithmetic](#) by Yuval R. Sanders et al, UNSW and Microsoft Research, 2018 (5 pages).

<sup>997</sup> See [Grover's search algorithm: An optical approach](#) by P. G. Kwiat et al, 1999 (6 pages), [Implementation of quantum search algorithm using classical Fourier optics](#) by N. Bhattacharya and al, 2002 (4 pages) and [Classical wave-optics analogy of quantum information processing](#) by Robert J. C. Spreeuw, 2001 (9 pages).

<sup>998</sup> Diagram source: [Quantum Annealing](#) by Scott Pakin, NSF/DOE Quantum Science Summer School June 2017 (59 slides).

<sup>999</sup> See also [On Shor's algorithms, the various derivatives, their implementation and their applications](#) by Martin Ekera, 2019 (135 slides) which describes in detail how Shor's algorithm works.

The gain in speed generated by Shor's algorithm compared to conventional calculation? The computation time goes from  $N \log(N)$  for the best simple Fourier transforms to  $\log_2(N)$  for the QFT. We thus go from a linear order of magnitude to a logarithmic order of magnitude. But the state of the art of classical integers factoring is much better than the usual  $O(\sqrt{N}/2)$  pointed out in textbooks, like :

$$\exp((1.923 + o(1))(\log N)^{1/3} (\log \log N)^{2/3})$$

One of the first implementations of Shor's algorithm took place in 2001 at IBM with an experimental quantum computer of 7 qubits, to factorize the number 15. Since then, we have just moved to a 5-digit number,  $56153^{1000}$ , but with a different factoring algorithm than Shor's algorithm. It is in fact an optimization algorithm that was running on a D-Wave quantum annealer! A record was reached in 2016 with the factorization of 200,099 with 897 qubits on a D-Wave but with yet another algorithm than Peter Shor's<sup>1001</sup>.

It is important to remember that Shor's algorithm theoretically allows to break the public keys of the RSA cryptography that is commonly used in Internet security. Public keys work by sending a very long integer number to a recipient who already has its divisor.

He just has to divide the large number received by his divisor to retrieve the other divisor and use it to decipher the encrypted message. Whoever does not have the divisor cannot exploit the complete key unless he has enormous traditional computing power to find his divisors.

Until now, only NSA supercomputers have officially been able to break reasonably sized keys in the 256 to 800 bits range. But at 1024 bits and beyond, the task is inaccessible in a reasonable amount of time for these supercomputers. As far as we know!

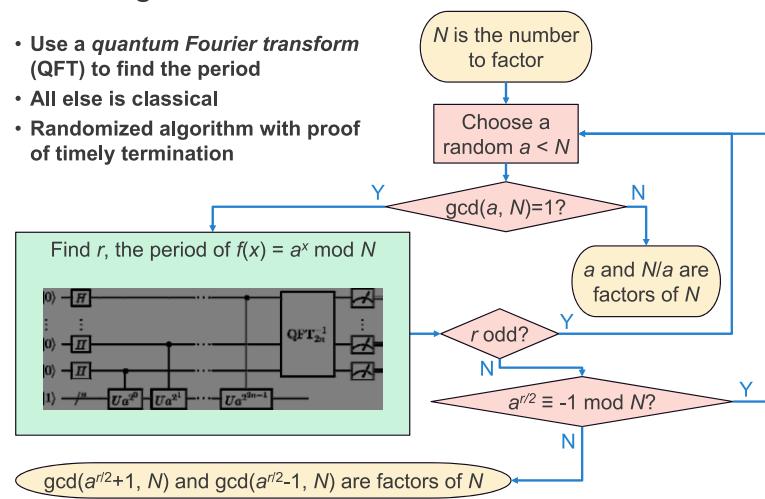
In theory, this would become accessible someday to scalable quantum computers. To break a good 2048-bit RSA public key, one will still have to be patient because it requires to create quantum computers with a very large number of corrected qubits.

It takes about twice as many logical qubits as there are bits in an RSA key. To factorize a 2048-bit RSA key, a minimum of 4098 logical qubits are required<sup>1002</sup>. Because of qubit noise, it is estimated that hundreds to tens of thousands of physical qubits per logical qubit would be needed.

Thus, such a RSA key break would require about 20 million qubits according to a famous Google algorithm from 2019. Another option would be to use some addressable quantum memory and reduce the qubits count to 13436<sup>1003</sup>.

### Shor's Algorithm

- Use a *quantum Fourier transform* (QFT) to find the period
- All else is classical
- Randomized algorithm with proof of timely termination



<sup>1000</sup> This is documented in [Quantum factorization of 56153 with only 4 qubits](#), 2014 (6 pages).

<sup>1001</sup> The record was beaten in 2019, it was beaten by engineers from Zapata and IBM with the factoring of 1,099,551,473,989 into  $1,048,589 * 1,048,601$ , but using a variational hybrid algorithm on a few qubits, and with an undocumented speedup. See [Analyzing the Performance of Variational Quantum Factoring on a Superconducting Quantum Processor](#) by Amir H. Karamlou et al, 2019 (14 pages).

<sup>1002</sup> The formula is  $2xN+2$  qubits. See [Factoring using 2n + 2 qubits with Toffoli based modular multiplication](#) by Thomas Haner et al, 2017 (12 pages) and [Circuit for Shor's algorithm using 2n+3 qubits](#) by Stephane Beauregard, 2013 (14 pages)..



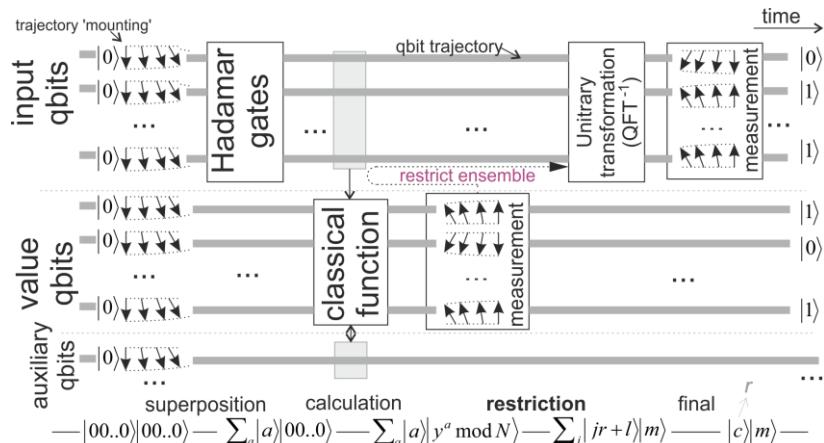
### factors an integer in prime numbers

algorithm relies on a period finding algorithm and an inverse quantum Fourier transform

**breaking RSA 2048 bits key requires 20 millions qubits with an error rate of 0,1% and 8 compute hours.**

$$O\left(\frac{\sqrt{N}}{2}\right) \Rightarrow O(\log(N)^3)$$

exponential speed gain



Yet, another option would be to rely on qubits like cat-qubits for which the physical/logical qubits ratio would be much lower, in the 10-100 range.

Note that Shor's algorithm also allows to break cryptography using elliptic curves, which competes with RSA cryptography. By the way, some of the cryptography used in the [Bitcoin protocol](#) would also be broken by Shor, which we will see [later](#) in this document, page 595.

In any case, Shor's algorithm has been terrorizing security specialists for a couple decades. This explains the interest in exploiting quantum keys distribution, which are supposed to be tamper-proof because their interception can be detected by their legitimate recipient, as well as post quantum cryptography, consisting in classical cryptographic algorithms and methods to make them (theoretically) tamper-proof by quantum computers using Shor's or any other algorithm.

But Shor's factoring is not the only quantum factoring algorithm created so far. Several other options are investigated like the **Variational Quantum Factoring** algorithm alternative that maps the factoring problem to the ground state of an Ising Hamiltonian that could be solved in a hybrid manner using the quantum approximate optimization algorithm (QAOA), running on a gates-based NISQ processor<sup>1004</sup>. But so far, the scalability of this algorithm with a large number of qubits and integer numbers is not proved.

### Shor dlog

Peter Shor did create his quantum dlog (*aka* discrete logarithm) algorithm simultaneously with his factoring algorithm in 1994 and solves another classically intractable problem. The discrete logarithm  $k = \log_b(a)$  (or logarithm of  $a$  in base  $b$ ) is an integer  $k$  such that  $b^k = a$ , where  $a$  and  $b$  are given integer numbers. You understand that this problem is intractable with digging in group isomorphisms logic, which I won't cover.

The dlog algorithm can help break Diffie-Hellman signatures, including those using elliptic curves.

Integer factoring and finding a dlog are both special cases of the hidden subgroup problem for finite Abelian groups (as seen just below).

<sup>1003</sup> See [Factoring 2048 RSA integers in 177 days with 13436 qubits and a multimode memory](#) by Élie Gouzien and Nicolas Sangouard, March 2021 (18 pages). It requires some quantum memory of 2 hours storage time and qubits with a  $10^{-3}$  error rate. The authors suggest realizing such an architecture with a microwave interface between a superconducting qubits processor and some multiplexed addressable quantum memory using the principle of photon echo in solids doped with rare-earth ions like Erbium or NV centers. Their physical qubits would use some 3D gauge color error correction codes.

<sup>1004</sup> See [Variational Quantum Factoring](#) by Eric R. Anschuetz, Alán Aspuru-Guzik et al, 2018 (18 pages).

## Hidden subgroup problems

The hidden subgroup problem is a generic problem which encompasses Shor's order finding, Simon's, the discrete log and the graph isomorphism problems. The definition of this problem is the following: let  $G$  be a group and  $H \subseteq G$  one of its subgroup. Let  $S$  be any set and  $f: G \rightarrow S$  a function that distinguishes cosets of  $H$ , meaning that for all  $g_1$  and  $g_2$  in  $G$ ,  $f(g_1) = f(g_2)$  means  $g_1H = g_2H$  (left cosets of  $H$  are equal). The hidden subgroup problem (HSP) is about determining the subgroup  $H$  using calls to function  $f$  with any combinations of  $g$ 's in  $G$ .

Verstanden? Well, not really if you have no idea what's a group, a subgroup, a set and a coset. So let's define these:

- **Set**: arbitrary ensemble of elements.
- **Subset**: ensemble of some elements from a set.
- **Group**: a set coupled with an operation on the elements in the set, where any combination of two elements with this operation gives another item from the group. One example is the group  $\mathbb{Z}$  of all integers associated with the addition. Any addition of integers yields an integer. A group also has an identity element (0 for integers) and all elements have an inverse element (inverse of integer  $a$  is  $-a$ ). Operations are also associative: the order in which the operation is done is not important. For example, with integers:  $a + (b + c) = (a + b) + c$ .
- **Subgroup**: subset of the group  $G$  being also a group with regards to its associated operation. For example, with integers, the even set is a subgroup with addition since adding even numbers always give even numbers. It's however not true with uneven numbers given adding two uneven numbers gives an even number.
- **Coset**: set or ensemble of elements from  $G$  that contains all elements of  $H$  multiplied by a given item  $g$  from  $G$ . If you multiply all elements of  $H$  on the left by one element  $g$  of  $G$ , the set of products is a left coset. If multiplied by the right, it's a right coset (these operations may be non-commutative with some non-integer elements like matrices). A subgroup  $H$  of a group  $G$  may be used to decompose  $G$  into disjoint equal-size cosets.  $H$  cosets have the same number of elements as  $H$ .

Another definition of the hidden subgroup problem is: given a function  $f$  that is constant with all cosets of some subgroup  $H$ , find the subgroup  $H$ .

In its quantum version, the function  $f$  is usually implemented as an oracle. Solving HSP takes an exponential time classically with the size of  $\log(|G|)$  whereas it can be solved efficiently for certain types of groups with quantum versions if done in a polynomial time of  $\log(|G|)$ , given  $\log(|G|)$  is the logarithm of the number of elements in the group  $G$ <sup>1005</sup>.

There are HSPs for Abelian and non-abelian groups given a group  $G$  is Abelian if  $xy = yx$  for all  $x, y$  in  $G$ . There is actually not a single quantum HSP algorithm but many of these that are applicable to different classes of groups and subgroups. It's a whole specialized field in itself.

One famous HSP problem is Pell's equation, a quadratic Diophantine equation of the form  $x^2 - ny^2 = 1$  with  $n$  being a positive nonsquare integer, and  $x, y$  being integer solutions to the equation. A quantum algorithm to Pell's equation was created by **Sean Hallgren** at Princeton in 2002. It is based on a QFT<sup>1006</sup>. It has the particularity to be applied to an infinite group given we don't know in advance what are the bounds for  $x$  and  $y$ .

---

<sup>1005</sup> See a good overview of various HSP algorithms in [The Hidden Subgroup Problem Master's Project](#) by Frédéric Wang, 2010 (99 pages).

<sup>1006</sup> See [Polynomial-Time Quantum Algorithms for Pell's Equation and the Principal Ideal Problem](#) by Sean Hallgren, 2006 (21 pages).

Is solving that equation useful? It may be for some cryptographic purposes. The Hallgren algorithm finds one solution to the Pell equation, who has many. It has a (roughly) polynomial time vs an exponential time for its classical version, so we're in for some exponential speedup.

## Fluid mechanics

Fluid mechanics simulations are mostly based on solving Navier-Stokes equations. These are non-linear partial differential equations, whose solution is essential to the aerospace industry, weather forecasting, plasma magneto-hydrodynamics and astrophysics. The problem with Navier-Stokes is nonlinear and quantum computing is implementing linear algebra. But there are some tricks available to turn nonlinear equations into linear ones.

Various quantum algorithms have been designed to solve Navier-Stokes equations:

- **Hybrid computing** in [Variational quantum algorithms for nonlinear problems](#) by Michael Lubasch et al, 2019 (15 pages). It makes use of a quantum nonlinear processing unit (QNPU) that is a unitary transformation implementing nonlinear operations.
- **Continuous variable qubits** in [Quantum algorithm for nonlinear differential equations](#) by Seth Lloyd et al, 2020 (17 pages). They implement non-linearities with using multiple copies of the vector representing the state of the system to be investigated. Polynomial values are obtained with creating tensor products of all or part of these multiple copies of the vector state. It can simulate the dynamics of the nonlinear Schrödinger equation with quantum linear differential equation solvers.
- **Differentiable quantum circuits**: in [Solving nonlinear differential equations with differentiable quantum circuits](#) by Oleksandr Kyriienko et al, 2020 (22 pages).
- **Converting a nonlinear system into a linear one** with transforming nonlinear problems into an array of linear equations. In [Efficient quantum algorithm for dissipative nonlinear differential equations](#) by Jin-Peng Liu, Andrew M. Childs et al, March 2021 (36 pages)<sup>1007</sup>.
- **Quantum annealing for laminar plane channel flow problem** in [Towards Solving the Navier-Stokes Equation on Quantum Computers](#) by N. Ray et al, April 2019 (16 pages), which presents a solution using a D-Wave quantum annealer.

The diagram illustrates the Navier-Stokes equations and related vector calculus concepts. At the top, it shows the momentum equation and the incompressibility condition. The momentum equation is given as:

$$\frac{\partial \mathbf{u}}{\partial t} + \mathbf{u} \cdot \nabla \mathbf{u} + \frac{1}{\rho} \nabla p = \mathbf{g} + \nu \nabla \cdot \nabla \mathbf{u}$$

The terms are labeled: change experienced by "particle" (blue arrow), advection (blue box), pressure (red box), gravity (green box), viscosity (orange box), and momentum equation (blue text). The incompressibility condition is  $\nabla \cdot \mathbf{u} = 0$ .

Below the momentum equation, the components of velocity, density, pressure, body forces, and viscosity are listed:

$\mathbf{u}$	$\rho$	$p$	$\mathbf{g}$	$\nu$
velocity	density	pressure	body forces	viscosity

At the bottom, the gradient and divergence are defined:

$$\nabla f = \left( \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z} \right)$$

gradient Gives vector of spatial derivatives of function

$$\nabla \cdot \vec{G} = \left( \frac{\partial G_x}{\partial x}, \frac{\partial G_y}{\partial y}, \frac{\partial G_z}{\partial z} \right)$$

divergence measures convergence/divergence of vectors at a point

The curl is also defined:

$$\nabla \times \vec{G} = \left( \frac{\partial G_z}{\partial y} - \frac{\partial G_y}{\partial z}, \frac{\partial G_x}{\partial z} - \frac{\partial G_z}{\partial x}, \frac{\partial G_y}{\partial x} - \frac{\partial G_x}{\partial y} \right)$$

curl: measures how much a vector field rotates around a point

<sup>1007</sup> See also [New Quantum Algorithms Finally Crack Nonlinear Equations](#) by Max G Levy, January 2021.

Worth mentioning, **Vorticity** (2001, USA) is developing custom (classical) DSA (domain specific accelerators) to solve Navier-Stokes equations with a  $10^5$  speed gain over classical methods. They don't provide any technical information on their technology (FPGA, ASIC?).

## Quantum walks

Quantum walks are yet another weird beast of the quantum protocols zoo, based on sophisticated mathematical grounds. All in all, quantum walks are search algorithms in graphs. The concept was introduced in 1993 by Yakir Aharonov et al<sup>1008</sup>. They have many applications like searching a triangle in a graph or even Hamiltonian simulations<sup>1009</sup>.

Andrew Childs demonstrated that quantum walks can be viewed as a universal quantum programming primitive, showing that an arbitrary set of qubit gates could be reduced to solving a quantum walk, which could be interesting with quantum systems implementing quantum walks at the hardware level one with photonic settings or even superconducting qubits<sup>1010</sup>.

### Theorem [Childs et al '02]

- A continuous-time quantum walk which starts at the entrance (on the LHS) and runs for time  $\mathcal{O}(\log N)$  finds the exit (on the RHS) with probability at least  $1/\text{poly}(\log N)$ .
- Any classical algorithm given black-box access to the graph requires  $\mathcal{O}(N^{1/6})$  queries to find the exit.

Quantum walks can be used to solve many different search problems, such as:

- Finding a triangle in a graph:  $\mathcal{O}(n^{1.25})$  queries, vs. classical  $\mathcal{O}(n^2)$  [Le Gall '14] [Jeffery et al '12] [Magniez et al '03]



- Matrix product verification:  $\mathcal{O}(n^{5/3})$  queries, vs. classical  $\mathcal{O}(n^2)$  [Buhrman and Špalek '04]

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 3 \\ -2 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 5 & -2 \\ -1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} -1 & 4 & -3 \\ 1 & 5 & 4 \\ 1 & -9 & 5 \end{pmatrix}$$

Other applications of continuous-time quantum walks:

- Spatial search [Childs and Goldstone '03]
- Evaluation of boolean formulae [Farhi et al '07] [Childs et al '07]

That was the case with a 62 qubits system presented in China in 2021 that was dedicated to implementing a random quantum walk. The project was driven by Jian-Wei Pan. The processor is based on a 8x8 matrix of transmon superconducting qubits. It simulates a Mach-Zehnder interferometer. The matrix use a nearest-neighbor connectivity like with Google Sycamore. Like Google's processor, two qubits were malfunctioning and deactivated, thus we have 62 instead of 64 qubits plus a nonfunctioning coupler. It runs at 10 mK and used 186 control lines, including 16 readout output lines with lines shared by 4 qubits<sup>1011</sup>. Quantum walks can also be implemented with photon qubits<sup>1012</sup>.

In classical computer science, random walk or Markov chain are algorithmic tools applied to search and sampling problems. Their quantum walks equivalent provide a framework for creating fast quantum algorithms. Quantum walks are based on the simulated coherent quantum evolution of a particle moving on a graph. Quantum walk algorithms use faster hitting (the time it takes to find a target vertex from a source vertex) and faster mixing (the time it takes to spread out over all vertices after starting from one source vertex)<sup>1013</sup>. The quantum time gain can be exponential for hitting and

<sup>1008</sup> See [Quantum random walks](#) by Yakir Aharonov (father of Dorit Aharonov), L. Davidovich and N. Zagury, 1993 (4 pages). See also this overview in [Quantum walks](#) by Martin Štefanák, 2020 (44 slides).

<sup>1009</sup> See [On the relationship between continuous- and discrete-time quantum walk](#) by Andrew M. Childs, 2008 (22 pages).

<sup>1010</sup> See [Universal computation by quantum walk](#) by Andrew M. Childs, 2008 (9 pages).

<sup>1011</sup> See [Quantum walks on a programmable two-dimensional 62-qubit superconducting processor](#) by Ming Gong et al, 2021 (18 pages).

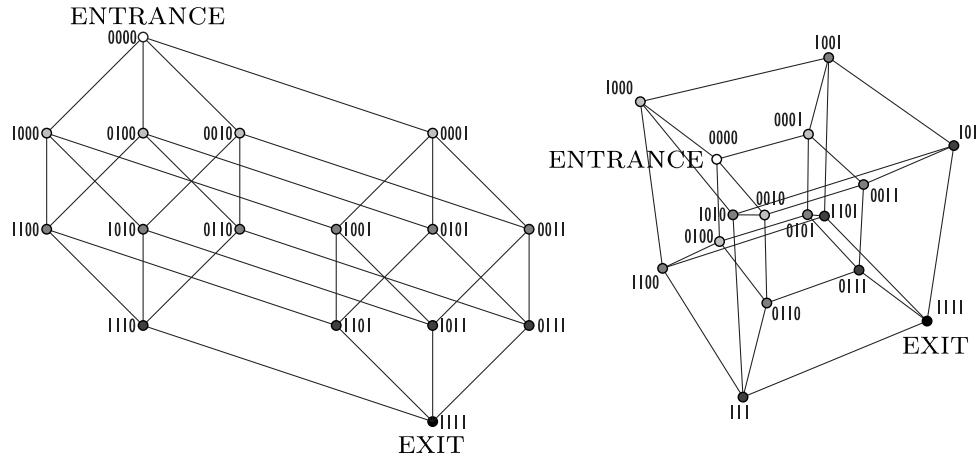
<sup>1012</sup> See [Two-dimensional quantum walks of correlated photons](#) by Zhi-Qiang Jiao et al, 2021 (22 pages).

<sup>1013</sup> I'm summarizing here the quantum walks description from [Quantum algorithms an overview](#) by Ashley Montanaro 2015 (16 pages).

quadratic for mixing. Since quantum walks are efficient ways to evaluate Boolean formulae, it can be used to solve satisfaction problems (MaxCut, SAT, 3-SAT).

In gate-based systems, quantum walks can be solved using a Grover search with an oracle function using an adjacency matrix for the searched walk. It can help find the shortest path in a graph (we're back at the traveling salesperson's problem)<sup>1014</sup>, finding if a graph is bipartite (with all edges in one vertex connected to the edges in the other), finding subgraphs such as a triangle and solving maximal clique problems (used for example in social networks to find groups of people who know each other).

Then, you have quantum random walks that help reduce quantum walks query complexity to search and find graph properties, with the discrete time and continuous time variations<sup>1015</sup>. These are equivalent of the famous Galton's board.



On top of Andrew M. Childs, let's mention three great contributors to the quantum walk domain: **Stacey Jeffery**<sup>1016</sup>, **Julia Kempe** and **Frédéric Magniez**.

## Quantum machine learning

What if quantum computing could accelerate machine learning and deep learning training and inferences? This is one of its potential domains of applications, but it is not that obvious.

First, quantum computing does not seem to enable machine learning tasks that are impossible to implement with classical computing, including the many specialized hardware (tensors processing units, spiking neurons).

Various quantum algorithms have been created in the last decades that cover the field of classical machine learning and with some variations in neural networks and deep learning<sup>1017</sup>. Many are based on linear algebra algorithms like HHL.

Here are a few quantum algorithms from this vast field of QML, which for the moment covers the domain of supervised machine learning:

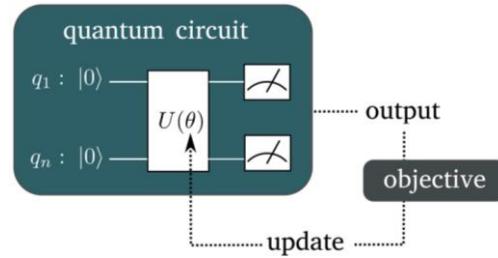
<sup>1014</sup> Illustration coming from: [Quantum Walks](#) par Daniel Reitzner, Daniel Nagaj and Vladimir Bužek, 2012 (124 pages).

<sup>1015</sup> See [Quantum Algorithm Implementations for Beginners](#) by Abhijith J. et al, 2020 (98 pages) provides many references related to quantum walks and quantum random walks algorithms.

<sup>1016</sup> See her thesis: [Frameworks for Quantum Algorithms](#) by Stacey Jeffery, 2014 (166 pages) and a lot of subsequent work in quantum walks algorithms.

<sup>1017</sup> See [Machine Learning in the Quantum Era - Machine Learning unlocks the potential of emerging quantum computers](#) by Loïc Henriet (Pasqal), Christophe Jurczak (Quantonation) and Leonard Wossnig (Rahko), November 2019. It highlights the potential of cold atom-based qubits for QML.

- Hybrid **quantum nonlinear regression** algorithm, one of the basic quantitative value prediction methods of the learning machine<sup>1018</sup>.
- **Variational circuits** are a family of hybrid algorithms that combine a quantum algorithm and a traditional algorithm that drives the latter<sup>1019</sup>. VQE is one of them<sup>1020</sup>. In particular, it allows finding global minimums more quickly. These algorithms would be suitable for applications on NISQ accelerators. But their true quantum acceleration is not proven yet.
- **SVM** (Support Vector Machine), a traditional method of segmentation that often relies on matrix inversions, based on its use of HHL<sup>1021</sup>.
- **PCA** (Principal Component Analysis) is used to determine the key variables in a data set<sup>1022</sup>. This is similar to searching for eigenvectors of a data set. Again, HHL is behind it.
- **Recommendation** systems useful in marketing or content<sup>1023</sup>.
- **Gradient descent** used during training phase of neural network<sup>1024</sup>.
- Quantum **convolutional neural networks**, still modest in size for the moment<sup>1025</sup>. It could also use D-Wave quantum annealing systems<sup>1026</sup>.
- Quantum **graph neural networks** have many applications, particularly in chemistry and biology<sup>1027</sup>.
- **Feature mapping** in deep learning and convolutional neural networks, to detect patterns efficiently<sup>1028</sup>.



<sup>1018</sup> See [Nonlinear regression based on a hybrid quantum computer](#), 2018 (7 pages), from researchers in several laboratories in China.

<sup>1019</sup> See [Universal Variational Quantum Computation](#) by Jacob Diamonte, 2019 (5 pages).

<sup>1020</sup> See [Accelerated Variational Quantum Eigensolver](#) by Daochen Wang, Oscar Higgott, and Stephen Brierley, 2019 (11 pages) which proposes a machine learning method to reduce the depth of the quantum circuits used (number of quantum gates to be executed). See also [Quantum advantage with shallow circuits](#) by Robert König et al, 2018 (97 slides). This list of quantum machine learning algorithms can be found in [Quantum Machine Learning What Quantum Computing Means to Data Mining](#) by Peter Wittek, 2014 (178 pages).

<sup>1021</sup> See [Support Vector Machines on Noisy Intermediate-Scale Quantum Computers](#) by Jiaying Yang, 2019 (79 pages) which discusses the use of SVM on NISQ computers and [Quantum Machine Learning with Support Vector Machines](#) by Anisha Musti, April 2020.

<sup>1022</sup> See [Quantum principal component analysis](#) by Seth Lloyd, Masoud Mohseni and Patrick Rebentrost, from MIT and Google, July 2013 (9 pages) which lays the groundwork on the matter.

<sup>1023</sup> See [Quantum Recommendation Systems](#) by Iordanis Kerenidis and Anupam Prakash, 2016 (22 pages, and [video](#)) is a proposed quantum machine learning algorithm for recommendation. The quantum algorithm of Iordanis Kerenidis had been challenged by a classical algorithm proposal by Ewin Tang in 2018. She “dequantized” Kerenidis’s algorithm, meaning, she found a classical efficient equivalent. But Iordanis pointed out that with certain recommendation parameters, the quantum algorithm was still clearly superior. Always, as long as a machine is there to execute it. Both these algorithms are investigated in [Exponential Advantages in Quantum Machine Learning through Feature Mapping](#) by Andrew Nader et al, December 2020 (16 pages).

<sup>1024</sup> See [Quantum algorithms for feedforward neural networks](#) by Jonathan Alcock, Iordanis Kerenidis et al, 2018 (18 pages) and [Quantum Circuit Parameters Learning with Gradient Descent Using Backpropagation](#) by M Watabe et al, 2020 (15 pages).

<sup>1025</sup> See [Quantum Convolutional Neural Networks](#) by Iris Cong et al, May 2019 (12 pages), [Quantum Neurons: analyzing the building blocks of quantum deep learning algorithms](#) by Zachary Cetinic et al, December 2019 (12 pages) and [Quantum Algorithms for Deep Convolutional Neural Networks](#) by Iordanis Kerenidis, Jonas Landman and Anupam Prakash, 2019 (31 pages). Also, [Advances in Quantum Deep Learning: An Overview](#) by Siddhant Garg and Goutham Ramakrishnan, May 2020 (17 pages) is focused on quantum neural networks including quantum convolutional neural networks and contains a good introduction to classical neural networks.

<sup>1026</sup> See [Adiabatic Quantum Computation Applied to Deep Learning Networks](#) by Jeremy Liu et al, May 2018 (28 pages).

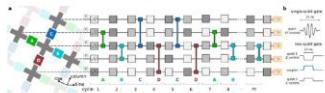
<sup>1027</sup> See [Quantum Graph Neural Networks](#) by Guillaume Verdon et al, 2019 (10 pages).

- **Recurrent Neural Networks** used for MNIST handwriting recognition, an existing common task for classical OCR (optical character recognition)<sup>1029</sup>.
- **Generative Machine Learning** models, including the models based on so-called quantum circuit Born machines (QCBM). It can be used to create (quantumly generated) synthetic training data sets used in classical machine learning models<sup>1030</sup>.
- Quantum **GAN** (Generative Adversarial Networks) algorithms that generate synthetic content from existing content by checking its plausibility via a network of recognition neurons<sup>1031</sup>.

### Case Study: Quantum GANs [LW18, etc]

classical distributions

*quantum circuits are good at sampling!*



*most quantum supremacy proposals (Google's random circuits, Boson sampling, etc) are sampling tasks*

quantum data

*only quantum circuits can generate q. data!  
probing unknown quantum materials w/ GANs!  
surprising quantum applications!*



► Implementation: simple prototypes of quantum GANs are likely implementable on near-term noisy-intermediate-size-quantum (NISQ) machines.

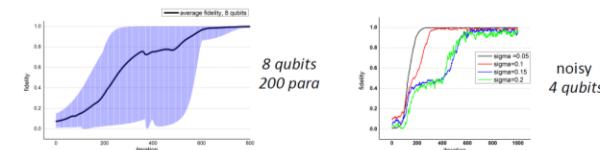
### Robust Training of Quantum Generative Models

Training of classical GANs is delicate and unstable!

*due to the property of the loss function*

Training quantum data could be even worse!

*existing quantum GANs scale up poorly (limited #qubits, #para, very slow convergence) in [BGWS19, DK18, Hu et al. 19]*



Contribution: [CHLFW19, NeurIPS 19]

- (1) more robust and scalable training even with noisy qubits
- (2) a 52-gate circuit approximating a 10k-gate circuit (product-formula)

- Unsupervised learning algorithm for **automatic data clustering**<sup>1032</sup>.
- Some **Federated Machine Learning**, which distributes training on several quantum computers to improve the training time while preserving privacy, with distributing and sharing the learned model instead of the training data<sup>1033</sup>.
- There is even a quantum algorithm for **spiking neurons** emulation although its speedup is not obvious<sup>1034</sup>.

This table positions the different quantum accelerations associated with various algorithms used in machine learning and deep learning<sup>1035</sup>. Accelerations in log(N) are more important than those expressed as the square root of N<sup>1036</sup>.

<sup>1028</sup> See [Supervised learning with quantum enhanced feature spaces](#) by Aram Harrow et al, 2018 (22 pages) which describes the use of quantum to detect complex shapes, far beyond what convolutional neural networks ("feature mapping") can do.

<sup>1029</sup> See [Recurrent Quantum Neural Networks](#) by Johannes Bausch (12 pages).

<sup>1030</sup> See [Quantum versus Classical Generative Modelling in Finance](#) by Brian Coyle, Elham Kashefi et al, August 2020 (17 pages) and [The Born Supremacy: Quantum Advantage and Training of an Ising Born Machine](#) by Brian Coyle, Daniel Mills, Vincent Danos and Elham Kashefi, April 2021 (47 pages).

<sup>1031</sup> This is well documented in [Quantum generative adversarial learning](#) by Seth Lloyd and Christian Weedbrook, 2018 (5 pages) and [Quantum generative adversarial learning in a superconducting quantum circuit](#), 2018 (5 pages).

<sup>1032</sup> See [Quantum spectral clustering](#) by Iordanis Kerenidis and Jonas Landman, April 2021 (20 pages). The method named spectral clustering consists in building a similarity graph with using distances between data vectors, extracting the eigenvectors from a matrix built with this graph and projecting the data onto this new orthogonal space and applying a classical k-means clustering method. But as seen frequently with QML algorithms, the best acceleration requires using some qRAM.

<sup>1033</sup> See [Federated Quantum Machine Learning](#) by Samuel Yen-Chi Chen and Shinjae Yoo, March 2021 (25 pages).

<sup>1034</sup> See [An artificial spiking quantum neuron](#) by Lasse Bjørn Kristensen, Alán Aspuru-Guzik et al, April 2011 (7 pages).

<sup>1035</sup> The table is from [The prospects of quantum computing in computational molecular biology](#) by Carlos Outeiral, April 2020 (23 pages) which covers both QML algorithms and quantum simulation ones. It also mentions protein structures predictions. See also [Quantum Machine Learning](#) by Jacob Biamonte et al, May 2018 (24 pages).

Note the need for quantum memory for many of these algorithms, a type of memory that doesn't yet exists. None of these algorithms have been tested on a large scale, due to the absence of a quantum processor with more than fifty qubits.

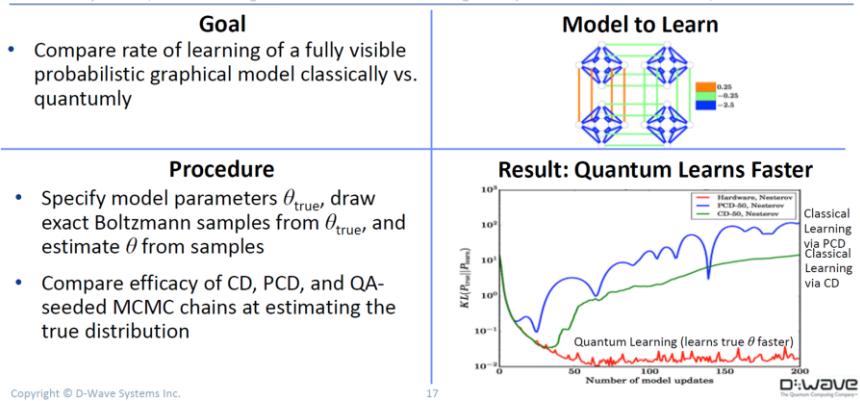
**TABLE 1** Overview of the main quantum machine learning algorithms that have been reported in the literature, and complexities

Algorithm	Classical	Quantum	QRAM
Linear regression	$\mathcal{O}(N)$	$\mathcal{O}(\log N)^*$	Yes
Gaussian process regression	$\mathcal{O}(N^3)$	$\mathcal{O}(\log N)^\dagger$	Yes
Decision trees	$\mathcal{O}(N \log N)$	Unclear	No
Ensemble methods	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Support vector machines	$\approx \mathcal{O}(N^2) - \mathcal{O}(N^3)$	$\mathcal{O}(\log N)$	Yes
Hidden Markov models	$\mathcal{O}(N)$	Unclear	No
Bayesian networks	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Graphical models	$\mathcal{O}(N)$	Unclear	No
$k$ -Means clustering	$\mathcal{O}(kN)$	$\mathcal{O}(\log kN)$	Yes
Principal component analysis	$\mathcal{O}(N)$	$\mathcal{O}(\log N)$	No
Persistent homology	$\mathcal{O}(\exp N)$	$\mathcal{O}(N^5)$	No
Gaussian mixture models	$\mathcal{O}(\log N)$	$\mathcal{O}(\text{polylog } N)$	Yes
Variational autoencoder	$\mathcal{O}(\exp N)$	Unclear	No
Multilayer perceptrons	$\mathcal{O}(N)$	Unclear	No
Convolutional neural networks	$\mathcal{O}(N)$	$\mathcal{O}(\log N)$	No
Bayesian deep learning	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Generative adversarial networks	$\mathcal{O}(N)$	$\mathcal{O}(\text{polylog } N)$	No
Boltzmann machines	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No
Reinforcement learning	$\mathcal{O}(N)$	$\mathcal{O}(\sqrt{N})$	No

QML is also one of the fields of application of quantum annealing at D-Wave. The latter is adapted to the search for a minimum energy which is equivalent to searching for a minimum level of errors in the adjustment of the weight of neurons in a network<sup>1037</sup>. So far, they have tested an RBM (Restricted Boltzmann Machine) model<sup>1038</sup>.

## Quantum Sampling Accelerates Learning

D. Korenkevych et al., "Benchmarking Quantum Hardware for Training of Fully Visible Boltzmann Machines," arXiv:1611.04528



<sup>1036</sup> Also see [Application of Quantum Annealing to Training of Deep Neural Networks](#) (2015), [Machine learning &... artificial intelligence in the quantum domain](#), 2017 (106 pages), [On the Challenges of Physical Implementations of RBMs](#), 2014, with Yoshua Bengio and Ian Goodfellow among the authors, illustrating the interest of AI specialists for quantum and [Quantum Deep Learning](#), 2014, all extracted from [Near-Term Applications of Quantum Annealing](#), 2016, Lockheed Martin (34 slides). See also [Quantum machine learning for data scientists](#), 2018 (46 pages).

<sup>1037</sup> Examples source: [D-Wave Quantum Computing - Access & application via cloud deployment](#) by Colin Williams, 2017 (43 slides).

<sup>1038</sup> See [Benchmarking Quantum Hardware for Training of Fully Visible Boltzmann Machines](#) by Dmytro Korenkevych et al, Kin-dred AI et D-Wave, 2016 (22 pages).

They also did it with a hybrid algorithm for image recognition in a neural network, based on a variational circuit and a hybrid algorithm. But with very low-resolution images!

D-Wave offers machine learning services in its Leap quantum cloud computing offering.

But they are not the only ones. Many startups are specialized in Quantum Machine Learning, such as **QC Ware**.

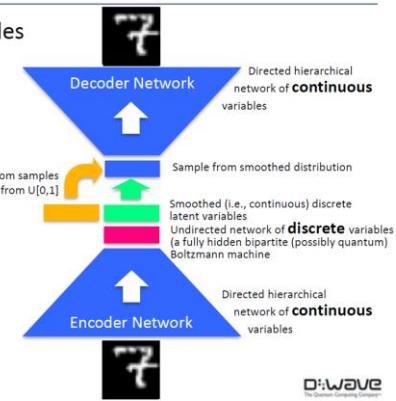
Many issues remain to be addressed to operationalize QML beyond the emergence of sufficiently powerful and reliable quantum processors<sup>1039</sup>:

- **Loading training data** may take time and have a negative impact on the acceleration provided by QML. It also requires quantum random access memory (qRAM) which does not yet exist, even if some Quantum Data Loaders are proposed to circumvent this need<sup>1040</sup>.

- **Reading the results** of QML algorithms, particularly when they are classical data that take the form of real numbers.

## Discrete Sampling in Complex Architectures (DVAE/QVAE)

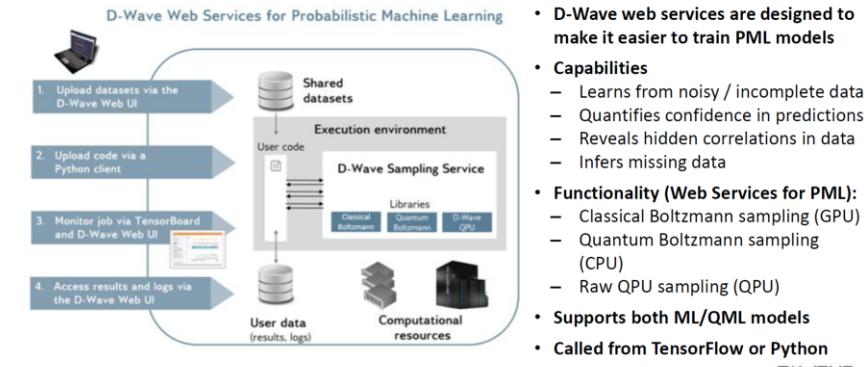
- Real data has discrete & continuous variables
- Natural to want discrete hidden variables
- Can't backpropagate through discrete variables
- DVAE solves this problem
  - See J. Rolfe, "Discrete Variational Autoencoders", arXiv:1609.02200
- **Exceeds state of the art on three standard machine learning datasets**
- DVAE (classical) / QVAE (quantum)



Copyright © D-Wave Systems Inc.

34

## Quantum/Classical Machine Learning Services



Copyright © D-Wave Systems Inc.

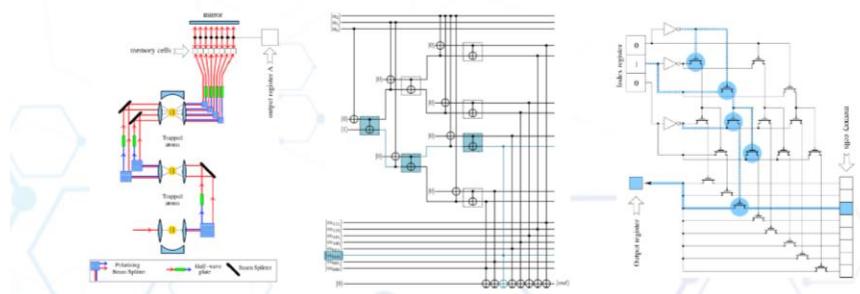
37

- **D-Wave web services are designed to make it easier to train PML models**
- **Capabilities**
  - Learns from noisy / incomplete data
  - Quantifies confidence in predictions
  - Reveals hidden correlations in data
  - Infers missing data
- **Functionality (Web Services for PML):**
  - Classical Boltzmann sampling (GPU)
  - Quantum Boltzmann sampling (CPU)
  - Raw QPU sampling (QPU)
- **Supports both ML/QML models**
- **Called from TensorFlow or Python**

**D-Wave**  
The Quantum Computing Company™

## Why do we need data loaders?

- ML data is CLASSICAL (images, texts, preferences, stocks, internet data,...)
- QML depends on loading classical data efficiently into quantum states.



<sup>1039</sup> See [Quantum machine learning: a classical perspective](#) by Ciliberto et al, 2020 (26 pages). It concludes with: "Despite a number of promising results, the theoretical evidence presented in the current literature does not yet allow us to conclude that quantum techniques can obtain an exponential advantage in a realistic learning setting".

<sup>1040</sup> See [Quantum embeddings for machine learning](#) by Seth Lloyd, January 2020 (11 pages). Illustration source: [Quantum Computing Applications](#), presentation by Iordanis Kerenidis from Qc-Ware at the Lab Quantique, June 2, 2020 (52 slides). In [Nearest Centroid Classification on a Trapped Ion Quantum Computer](#) by Sonika Johri, Iordanis Kerenidis et al, December 2020 (15 pages), the QML algorithm "Nearest Centroid Classification" is implemented on a 11 trapped ions IonQ processor with an efficient amplitude data loader.

- The use in classical neural networks of **non-linear activation functions** such as sigmoids. While quantum gates all apply linear transformations<sup>1041</sup>. However, there are workarounds, on which Iordanis Kerenidis has worked<sup>1042</sup> and some others<sup>1043</sup>. For example, quantum measurement can create the sought-after activation function nonlinearity in neural networks. There are also suggestions to use continuous variables qubits architectures to handle neural networks with nonlinearity provided by non-Gaussian qubit gates<sup>1044</sup>.
- QML can take advantage of the **errors and noise** generated by quantum computation rather than be subjected to them. Work is going in this direction.
- QML must prove that it brings a real **gain in computing time** compared to today's most advanced processors<sup>1045</sup>.
- QML must also take into account the **algorithms explicability** growing expectations. The decomposition of the training and inference process of these quantum neural networks will probably be different from their implementation in more traditional processors<sup>1046</sup>.

IBM published in 2021 a mathematical proof of a potential quantum advantage for a **quantum machine learning classification** task done with a quantum kernel method based on the Shor dlog algorithm.

There was no actual experiment done due to the inexistence of sufficiently powerful quantum computers<sup>1047</sup>. We'll probably be stuck in this situation for several years from now.

On the other hand, QML's algorithm developments have served as a source of inspiration to improve algorithms that work with classical computation. As we will see in the section on quantum software vendors, page 566, there is no shortage of those who have specialized in QML. In general, they provide development tools and means to create QML proofs of concept.

In the AI domain, the European project H2020 **Quromorphic** launched in July 2019 aims to create a quantum processor dedicated to the execution of neural networks inspired by the brain<sup>1048</sup>. It reminds us of the very controversial European flagship Human Brain Project led by Henri Markram from Switzerland.

<sup>1041</sup> The trick is explained in [Quantum Neuron: an elementary building block for machine learning on quantum computers](#) by Yudong Cao, Gian Giacomo Guerreschi and Alan Aspuru-Guzik in 2017 (30 pages).

<sup>1042</sup> See [Quantum Algorithms for Deep Convolutional Neural Network](#) by Iordanis Kerenidis et al, 2020 (36 pages) which is discussed in [Deep Convolutional Neural Networks for Quantum Computers](#) by Jonas Landman, 2020.

<sup>1043</sup> See for example [Continuous-variable quantum neural networks](#) by Nathan Killoran et Al, June 2018 (21 pages).

<sup>1044</sup> See [Continuous-variable quantum neural networks](#) by Nathan Killoran, Maria Schuld, Seth Lloyd et al, 2018 (21 pages).

<sup>1045</sup> See [Quantum Machine Learning: Algorithms and Practical Applications](#) by Iordanis Kerenidis, QC Ware, Q2B Conference, December 2019 (34 slides) which makes an inventory of some potential gains with QML algorithms.

<sup>1046</sup> These techniques will be challenged by future memristor-based neuromorphic processors that will allow networks to converge more rapidly with backpropagation. Memristors will make it possible to place the neuron's computational functions and the associated memory in the same location in a semiconductor circuit, accelerating access to memory by several orders of magnitude during computations. This is another area of research, operated notably by Julie Grollier of the CNRS laboratory located at Thales TRT in Palaiseau.

<sup>1047</sup> See [IBM shows quantum computers can solve these problems that classical computers find hard](#) by Daphne Leprince-Ringuet, ZDNet, July 2021 that refers to [Quantum kernels can solve machine learning problems that are hard for all classical methods](#), IBM Research, July 2021, itself referring [A rigorous and robust quantum speed-up in supervised machine learning](#) by Yunchao Liu, Srinivasan Arunachalam and Kristan Temme, Nature Physics, July 2021 (27 pages).

<sup>1048</sup> See [Quantum computer: We're planning to create one that acts like a brain](#) by Michael Hartmann and [Heriot-Watt leads on next-gen computers](#), November 2018. The project is led by Michael Hartmann of IPaQS (Institute of Photonics and Quantum Sciences) at Heriot Watt University in the UK, together with ETH Zurich, Delft University (Netherlands), Basque University (Spain), IBM Zurich and Volkswagen (Germany). 2.2M€ from the FET Open program were allocated to the project by the European Commission (details). My interpretation? The objective of the project has been adapted to the sauce of science fiction in order to recover community funding. The rest is photonics.

Quromorphic involves IBM Zurich, ETH Zurich, TU Delft, Volkswagen and Spanish and German Universities. Given the participants, we can guess that this will be based on superconducting qubits. The project got a funding of 2.9M€ in 2019 and is scheduled to end in 2022<sup>1049</sup>. This is quite reasonable.

We'll probably discover new fancy claims combining artificial intelligence and quantum computing and the devil will always be in complicated details<sup>1050</sup>. For instance, how about using these QML algorithms in robotics? Not so fast<sup>1051</sup>! It's still science fiction and *click-bait*.

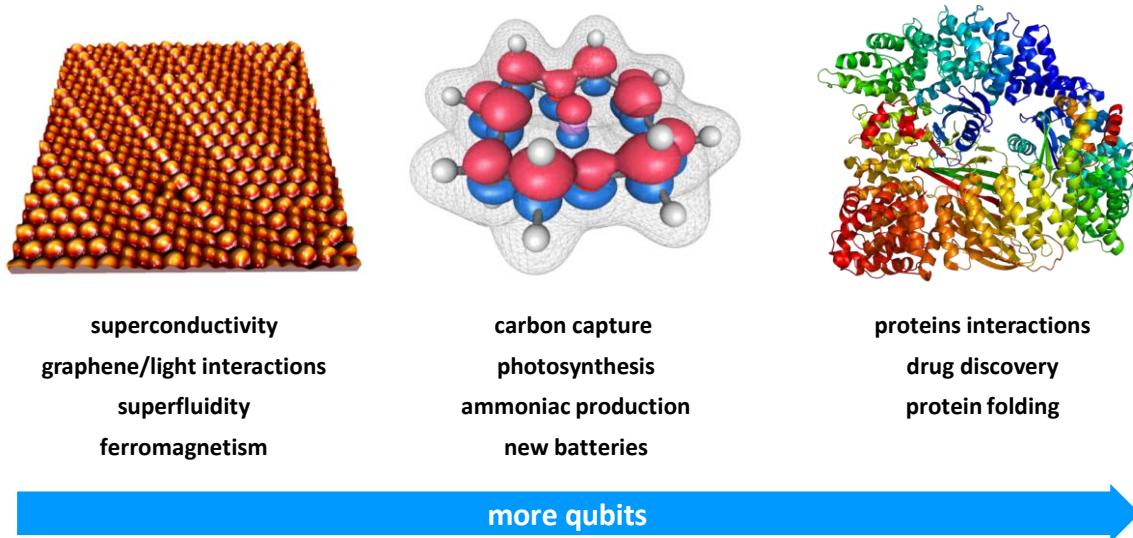
On the other end, classical learning machine can be useful for quantum physics and quantum computing. We saw that Google used a deep learning algorithm to optimize the microwave frequency plan of the Sycamore processor's qubit control. Machine learning can also be used to model and simulate condensed matter, with an impact on the development of various qubits, especially superconducting qubits<sup>1052</sup>.

Let us note finally the existence of an association promoting the field of AI and quantum computing, the **IAIQT** foundation based in Switzerland.

## Quantum physics simulation

Quantum simulation algorithms are used to reproduce matter at the quantum level in a computer. It can be used to simulate the interaction between atoms in molecules for the creation of new materials.

They can also simulate physical phenomena related to magnetism or the interaction between photons and matter. This amounts to solving "N-body problems", i.e. calculating the interaction between several particles according to the physical laws governing their interaction.



<sup>1049</sup> See [Quantum computer: we're planning to create one that acts like a brain](#), January 2019.

<sup>1050</sup> Here is one good example with [Using Pioneering Quantum Machine Learning Methods, CQC Scientists Offer Bright Forecast For Quantum Computers That Can Reason](#) par Matt Swayne, 2021 referring to [Variational inference with a quantum computer](#) by Marcello Benedetti, April 2021 (17 pages) which is about apply some quantum version of MCMC (Markov-Chain Monte Carlo) algorithm using Born machines. These are described in [The Born Supremacy: Quantum Advantage and Training of an Ising Born Machine](#) by Brian Coyle, Elham Kashefi et al, April 2021 (10 pages).

<sup>1051</sup> As described in Daniel Manzano's [The Rise of Quantum Robots](#), April 2018. And with [Qubit or Qubot? Quantum Technology May Help Robots Learn Faster](#) par Matt Swayne, 2021, [Robots learn faster with quantum technology](#) by University of Vienna, March 2021 pointing to [Experimental quantum speed-up in reinforcement learning agents](#) by V. Saggio et al, Nature, March 2021 (10 pages).

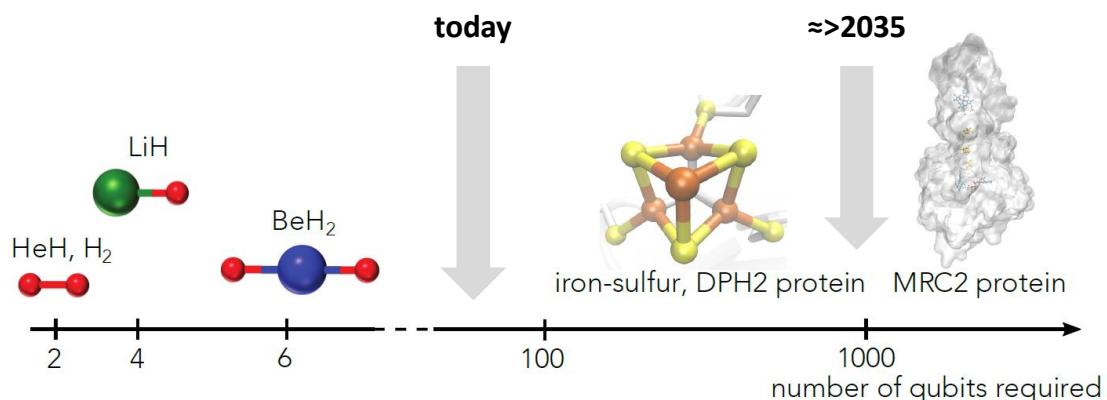
<sup>1052</sup> See [Machine learning & artificial intelligence in the quantum domain](#) by Vedran Dunjko and Hans J. Briegel, 2017 (106 pages).

Quantum simulation also helps studying how superconducting materials behave, particularly at (relatively) high temperature, superfluids at low temperature, the temperature-dependent magnetism of certain materials and the interactions between graphene and light<sup>1053</sup>.

These algorithms run in qubit-based universal quantum computers as well as on quantum simulators and quantum annealers and we still lack data to compare their respective performance.

Starting with 50 electrons in a molecule, classical computers can no longer simulate their dynamics, which corresponds to just a few atoms. For simple molecules, the applications are in the field of materials physics: carbon or nitrogen capture, new batteries, discovery of superconducting mechanisms that can then be used in medical scanners, ideally operating at room temperature.

This should be accessible with universal quantum computers with 50 to a few hundred corrected logical qubits. For molecular biology simulations, it will probably take much longer before this is possible. We may need thousands or even hundreds of thousands of corrected qubits, which is far away in time. The diagram *below* positions the number of qubits needed to simulate the functioning of a mitochondrial protein, MRC2, in a fairly optimistic way<sup>1054</sup>.



source: Quantum optimization using variational algorithms on near-term quantum devices, 2017

Here are some examples of quantum simulation algorithms:

- [Simulating a quantum field theory with a quantum computer](#) by John Preskill, 2018 (22 pages) which deals with the simulation of quantum fields governing the interaction of matter at very low-levels.
- [Computation of Molecular Spectra on a Quantum Processor with an Error-Resilient Algorithm](#), 2018 (7 pages) on the simulation of hydrogen atoms in quantum computers with superconducting qubits.
- [Researchers succeed in the quantum control of a molecule](#) by Román Ikonickoff, May 2017 (38 pages), pointing to [Preparation and coherent manipulation of pure quantum states of a single molecular ion](#), 2017 (38 pages), describing a hybrid simulation algorithm combining classical and quantum computation to study the hydrogen spectrum. The quantum part uses only two superconducting qubits!
- An example of simulation of a beryllium hydride molecule (3 atoms, BeH<sub>2</sub>) with only 6 qubits by IBM in 2017 in [Tiny Quantum Computer Simulates Complex Molecules](#) by Katherine Bourzac.

<sup>1053</sup> See this interesting lecture by Jacqueline Bloch at the Academy of Sciences which makes an excellent overview: [Quantum Simulators: Solving Difficult Problems](#), May 2018 (29 mn).

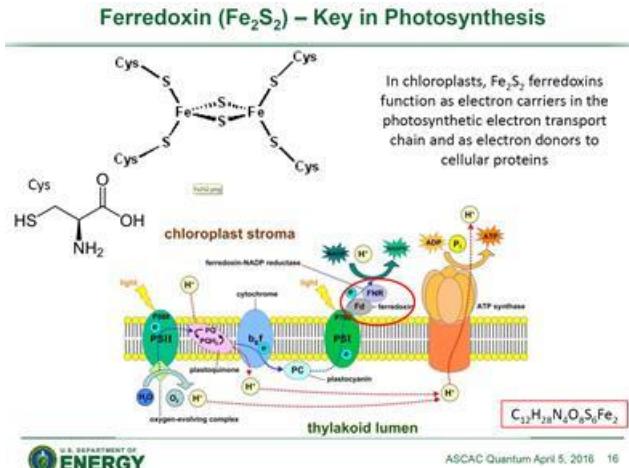
<sup>1054</sup> It comes from [Quantum optimization using variational algorithms on near-term quantum devices](#) by IBM researchers in 2017 (30 pages).

- The simulation of water electrolysis caused by light with use cases for the production of storable energy, particularly in fuel cells (hydrogen-based). This is one of the many examples from the presentation [Enabling Scientific Discovery in Chemical Sciences on Quantum Computers](#), December 2017 (34 slides) by Ber De Jong from Berkeley.
- [Solving strongly correlated electron models on a quantum computer](#) by Wecker, Troyer, Hastings, Nayak and Clark, 2015 (27 pages), which uses quantum annealing to simulate semiconductor dynamics.
- [Simulated Quantum Computation of Molecular Energies](#) by Wiebe, Wecker and Troyer, 2006 (21 pages) which deals with the determination of the equilibrium state of simple molecules.
- The improvement of algorithms for the simulation of catalytic chemical processes proposed by researchers from Microsoft and ETH Zurich in [Quantum computing enhanced computational catalysis](#) by Vera von Burg, Matthias Troyer et al, July 2020 (104 pages). The orders of magnitude of the requirements are about 4000 logical qubits, or millions of physical qubits.
- [Simulation of Electronic Structure Hamiltonians Using Quantum Computers](#) by James Whitfield, Jacob Biamonte and Alan Aspuru-Guzik, 2010 (22 pages) which also deals with simple molecules simulation. Alan Aspuru-Guzik is one of the world's leading authorities in the field.
- Hybrid molecular simulations combining classical and quantum algorithms as seen in [Quantum Machine Learning for Electronic Structure Calculations](#), October 2018 (16 pages).

In [Quantum Computation for Chemistry](#) by Alán Aspuru-Guzik, 2009 (51 slides), it is shown that the simulation of organic molecules of medium complexity such as cholesterol would require 1500 corrected qubits and, above all, the ability to use billions of quantum gates<sup>1055</sup>. The VQE algorithm can also be used there. It is executable with a universal gate quantum computer with a reasonable depth of quantum gates (number of steps in the algorithm)<sup>1056</sup>.

One of the applications of molecular quantum simulation is to better understand how photosynthesis works in order to improve or imitate it, the involvement of different forms of ferredoxin, relatively simple iron and sulfur-based molecules that serve to transport electrons from the photoelectric effect used in photosynthesis in plants<sup>1057</sup>.

Algorithmic research on this molecule simulation have downsized the duration of quantum theoretical simulation from 24 billion years to one hour in a few years!



The simulation of photosynthesis can pave the way for better carbon capture, among others to produce synthetic fuel. Research is also advancing in this field, without quantum computation for the moment<sup>1058</sup>. Matthias Troyer explains how this algorithm has been optimized<sup>1059</sup>.

<sup>1055</sup> See also [Quantum Computation for Chemistry and Materials](#) by Jarrod McClean, Google 2018 (36 slides).

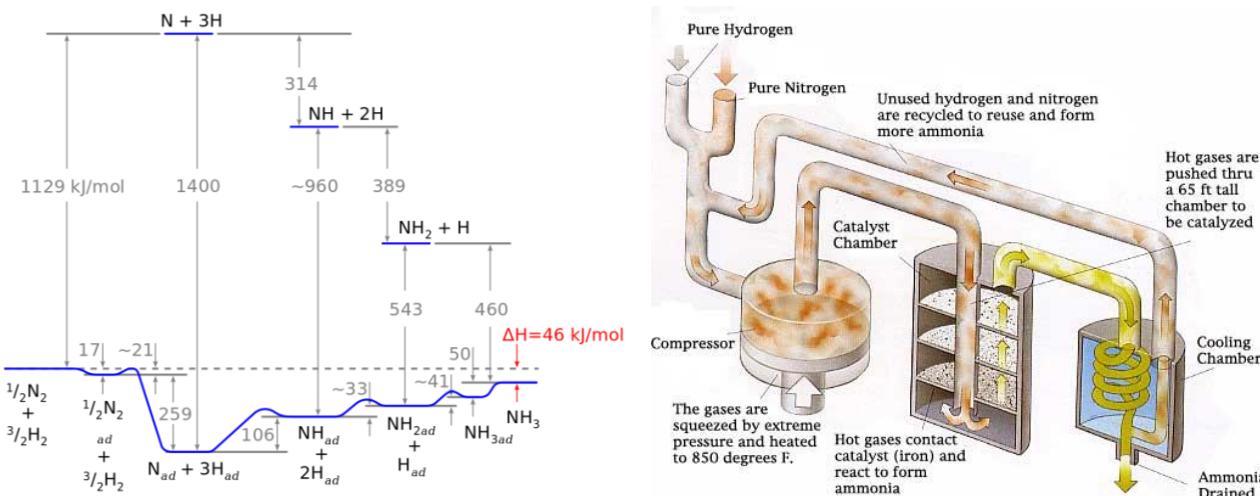
<sup>1056</sup> Voir [An adaptive variational algorithm for exact molecular simulations on a quantum computer](#) by Sophia Economou et al, 2019 (9 pages) which indicates in particular that "VQE is much more suitable for NISQ devices, trading in the long circuit depths for shorter state preparation circuits, at the expense of a much higher number of measurements".

<sup>1057</sup> The schema on ferredoxin comes from [Quantum Computing \(and Quantum Information Science\)](#) by Steve Binkley, US Department of Energy, 2016 (23 slides).

<sup>1058</sup> As seen in [Semi-Artificial Photosynthesis Method Produces Fuel More Efficiently Than Nature](#), September 2018

Another chemical process that could benefit from quantum simulation would be to find a way to produce ammonia more efficiently. It's used in the production of fertilizers (88% of total) and also explosives.

Right now, ammonia ( $\text{NH}_3$ ) is produced using the famous Haber-Bosch chemical process that uses  $\text{N}_2$  coming from the atmosphere and hydrogen usually coming from methane ( $\text{CH}_4$ ). The nitrogenase process uses a catalyst that is usually some iron doped with potassium and fixed on silica or alumina. Its natural equivalent is FeMoCo, a natural cofactor of nitrogenase. The Haber-Bosch process is highly energy-consuming particularly in the part producing pure  $\text{H}_2$  and due to the heat and pressure needed in the main reactor ( $500^\circ\text{C}$  and 100 bars). This production is responsible for about 1.5% of annual energy consumption worldwide<sup>1060</sup>.



Two processes could be developed thanks to quantum simulation for improving the energy efficiency of ammonia production. The first would be to simulate the nitrogenase enzyme, FeMoCo, that converts nitrogen into ammonia in cyanobacteria. The second would be to invent new catalysts serving to operate the Haber-Bosch process at lower temperature and pressure. One example is the design of Fe/K mixtures supported on carbon nanotubes<sup>1061</sup>. But the number of qubits and gates to implement for solving these problems seems quite mind boggling, even with corrected qubits<sup>1062</sup>.

#### The result of quantum software optimization

- Estimates for an example molecule:  $\text{Fe}_2\text{S}_2$  with 118 spin-orbitals

Gate count	$10^{18}$	Reduced gate count	$10^{11}$
Parallel circuit depth	$10^{17}$	Parallel circuit depth	$10^{10}$
Run time @ 10ns gate time	30 years	Run time @ 10ns gate time	2 minutes

- Attempting to reduce the horrendous runtime estimates we achieved  
Wecker *et al.*, PRA (2014), Hastings *et al.*, QIC (2015), Poulin *et al.*, QIC (2015)

- Reuse of computations:  $\mathcal{O}(N)$  reduction in gates
- Parallelization of terms:  $\mathcal{O}(N)$  reduction in circuit depth
- Optimizing circuits: 4x reduction in gates
- Smart interleaving of terms: 10x reduction in time steps
- Multi-resolution time evolution: 10x reduction in gates
- Better phase estimation algorithms: 4x reduction in rotation gates

#### From materials to models on quantum computers

	Material	Model
Orbitals per unit cell	$\approx 50$	1
Unit cells needed	20x20	20x20
Number of orbitals	$N \approx 20'000$	$N \approx 800$
Number of terms	$N^4$	$\mathcal{O}(N)$
Scaling of algorithm	$\mathcal{O}(N^{5.5})$	$\mathcal{O}(N^{0.5})$
Estimated runtime	age of the universe	seconds

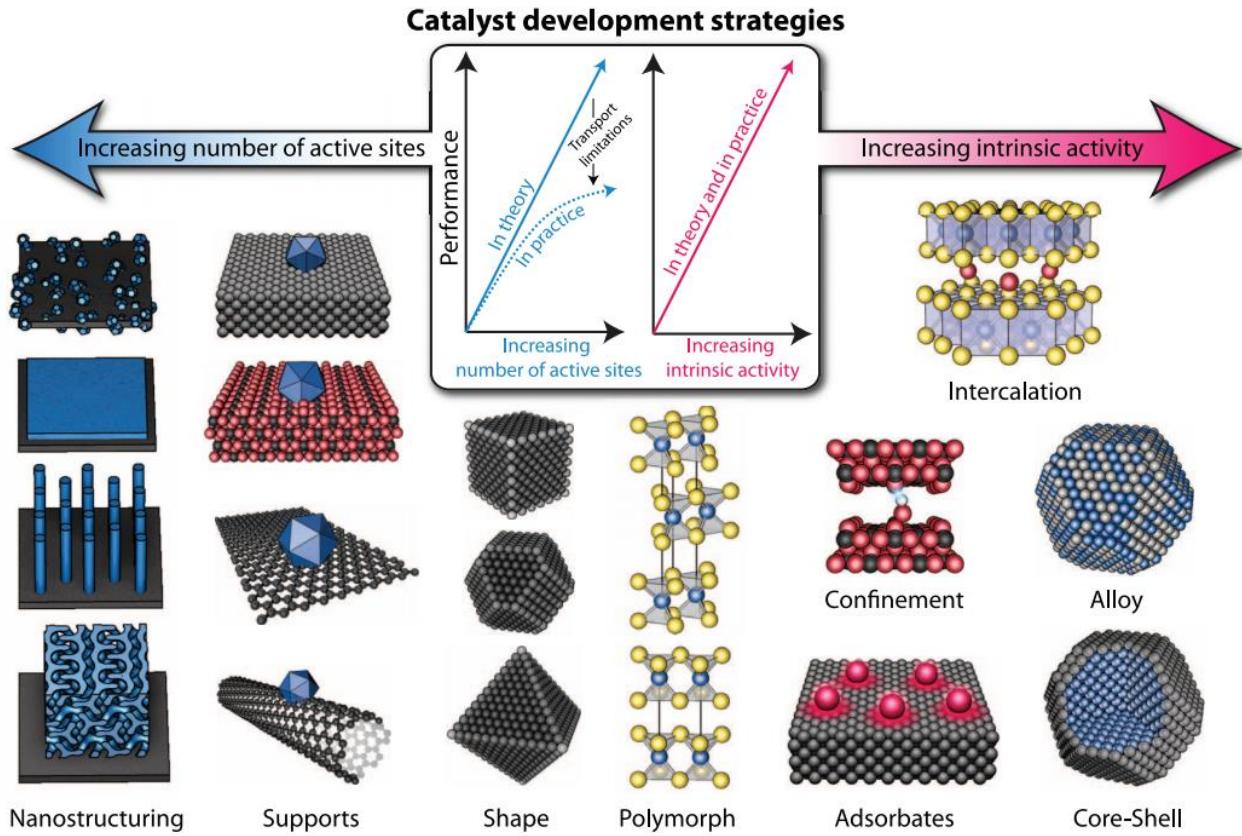


<sup>1059</sup> In [What Can We Do with a Quantum Computer](#), Matthias Troyer, ETH Zurich, 2016 (41 slides), source for the illustration on the right.

<sup>1060</sup> Illustration source [Catalysis How Dirt and Sand Catalyze Some of the Most Important Transformations](#), by Justin J. Teesdale, Harvard Energy Journal Club, September 2017.

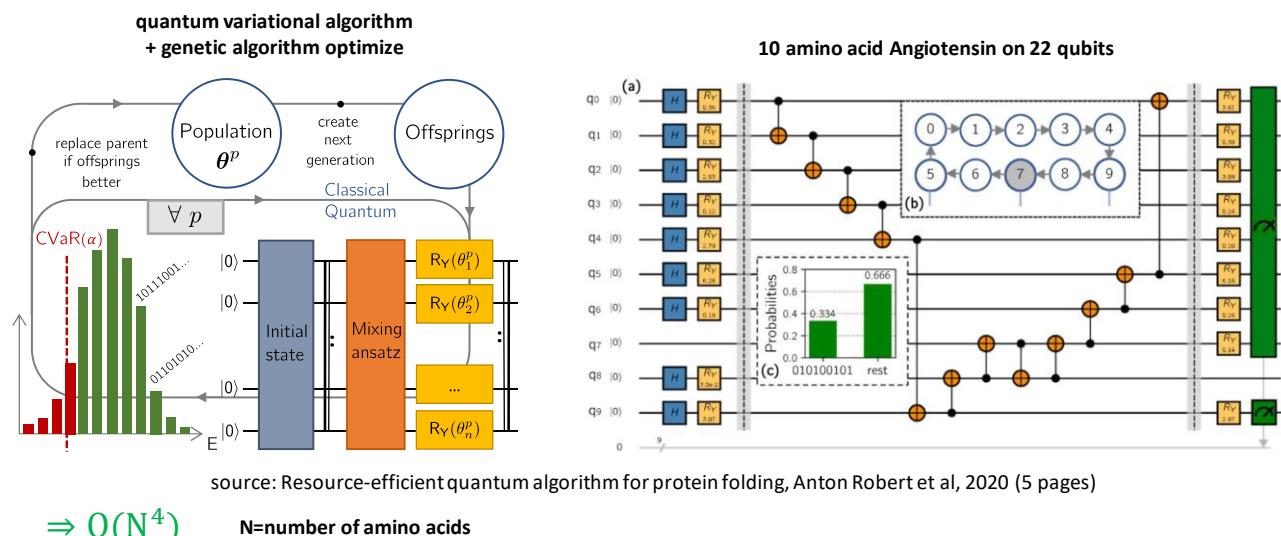
<sup>1061</sup> Illustration source: [Combining theory and experiment in electrocatalysis: Insights into materials design](#) by Jens Jaramillo et al, Science, 2017 (33 pages).

<sup>1062</sup> See [Even More Efficient Quantum Computations of Chemistry Through Tensor Hypercontraction](#) by Joonho Lee et al, July 2021 (62 pages). With this recent method, 4 million physical qubits with an error rate of 0,1% would still be necessary.



At a higher abstraction level sits the simulation of atomic interactions in organic chemistry and molecular biology, going progressively from the smallest to the largest molecules: amino acids, peptides, polypeptides, proteins and perhaps much later, ultra-complex molecules such as ribosomes that fabricates proteins with amino acids using messenger RNA code.

Like classical algorithms, quantum simulation algorithms use approximation models based on known molecules, like what AlphaFold 3 from DeepMind does to predict the 3D structure of folded proteins. It works well for proteins which are close to those proteins used to train the model. For entirely new proteins (*aka* “de-novo proteins”), quantum simulation is required<sup>1063</sup>.



<sup>1063</sup> See [Evolution, energy landscapes and the paradoxes of protein folding](#) by Peter Wolynes, 2015 (13 pages).

Various quantum algorithms have already been created for this purpose, including the Harvard [As-puru-Guzik](#) algorithm in 2012, which has even been tested on a small scale on the first adiabatic quantum computer, the D-Wave One. In 2020, researchers from IBM Zurich and from Institut Pasteur in France created an algorithm able to predict the 3D structure of a peptide, angiotensin, made of 10 amino acids and on just 22 qubits<sup>1064</sup>.

The orders of magnitude of the quantum computers needed to solve these organic chemistry problems for large proteins have yet to be evaluated. It is not impossible that they are either impossible or extremely long-term even with the various optimizations that are proposed<sup>1065</sup>!

## Hybrid algorithms

Hybrid algorithms are another branch of quantum algorithms that has been steadily growing in recent years. These algorithms combine a classical and a quantum part. Any quantum algorithm requires the support of a classical computer for the control of the quantum computer and the activation of its quantum gates<sup>1066</sup>. Hybrid algorithms distribute actual computing on both sides and ensure that the quantum part of the algorithm only covers what cannot be executed efficiently as classical computing. Eventually, it is likely that a majority of quantum algorithms will be hybrid<sup>1067</sup>.

These hybrid algorithms can be implemented in development tools and languages capable of controlling both the classical and the quantum part of a supercomputer or a distributed system.

This is particularly the case with the **XACC** (eXtreme-scale ACCelerator) programming model<sup>1068</sup>. It enables the development of hybrid code that takes into account the characteristics of the quantum computer, and in particular its error rate. It interfaces with IBM and Rigetti quantum accelerators programming models.

### Variational Quantum Eigensolver

One of the most pre-eminent hybrid algorithm class is the VQE (**Variational Quantum Eigensolver**), invented in 2013 by Alán Aspuru-Guzik<sup>1069</sup>. It allows the discovery of an energetic minimum of a complex equation<sup>1070</sup>. In particular, it is used to simulate the structures of molecules in inorganic and organic chemistry.

---

<sup>1064</sup> Illustration source: [Resource-efficient quantum algorithm for protein folding](#), Anton Robert et al, 2020 (5 pages).

<sup>1065</sup> See [Quantum Information and Computation for Chemistry](#), 2016 (60 pages), which provides a good inventory of the various algorithmic works on quantum simulation of organic chemistry, [A Comparison of the Bravyi–Kitaev and Jordan–Wigner Transformations for the Quantum Simulation of Quantum Chemistry](#) by Andrew Tranter et al, 2018 (14 pages) that provides some solutions to reduce the gates count for quantum chemistry simulation with gate-based quantum computers and [Creating and Manipulating a Laughlin-Type v=1/3 Fractional Quantum Hall State on a Quantum Computer with Linear Depth Circuits](#) by Armin Rahmani et al, November 2020 (7 pages).

<sup>1066</sup> See [A Hybrid Quantum-Classical Approach to Solving Scheduling Problems](#), Tony T. Tran et al, (9 pages), [Hybrid Quantum Computing Apocalypse](#) 2018 (6 pages) according to which some Chinese team supposedly succeeded in running a Majorana fermion qubit, [The theory of variational hybrid quantum-classical algorithms](#) by Jarrod McClean et al (23 pages).

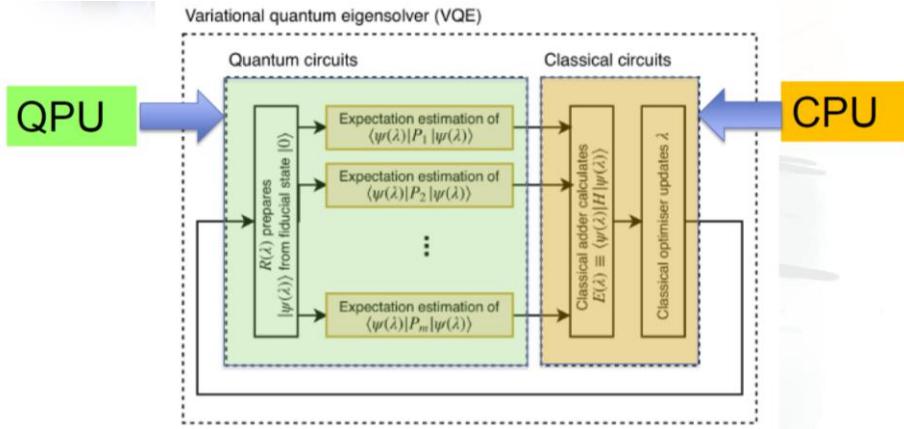
<sup>1067</sup> As such, the quantum algorithm patents filed by Accenture are worrying because they are at the limit of *troll patents*. See for example the [Multi-state quantum optimization engine](#) patent, USPTO 10,095,981B1, validated in October 2018 (20 pages). A second patent validated in April 2019 deals with a machine learning solution that helps an algorithm to decide which part to execute as classical and which part to execute as quantum. It is USPTO 10,275,721.

<sup>1068</sup> See [Hybrid Programming for Near-term Quantum Computing Systems](#) by A. J. McCaskey et al, Oak Ridge Laboratory, 2018 (9 pages).

<sup>1069</sup> VQE now belong to a broader category of hybrid algorithms, Variable Quantum Algorithms (VQA). See [Variational Quantum Algorithms](#) by M. Cerezo et al, Nature Reviews Physics, August 2021 (29 pages).

<sup>1070</sup> Diagram source: [Accelerated Variational Quantum Eigensolver](#) by Daochen Wang, Oscar Higgott and Stephen Brierley, 2019 (11 pages). See an history timeline on [Towards an experimentally viable variational quantum eigensolver with superconducting qubits](#), 2016 (18 slides). See also [Variational Quantum Eigensolver explained](#), November 2019,

It combines a classical part that determines an approximate starting point and a quantum part that refines the result. More precisely, the classical part prepares a so-called ansatz which is a set of parameters defining a quantum state, with using some non-linear optimization techniques.

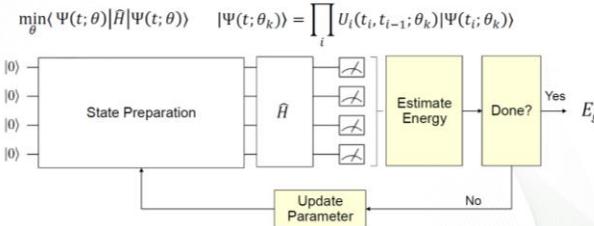


The quantum side of the algorithm is used to compute a cost function outputting a real number that we seek to minimize with varying the parameters of the ansatz in the classical part.

This type of algorithm has the advantage of being able to be processed in distributed architectures with several classical and quantum processors. The gain in VQE comes from the ability of quantum computing to explore the space of possibilities in parallel. The approach is iterative and the speed of convergence depends on factors related to the simulated physical system, the numerical modeling and the desired quality of the result<sup>1071</sup>.

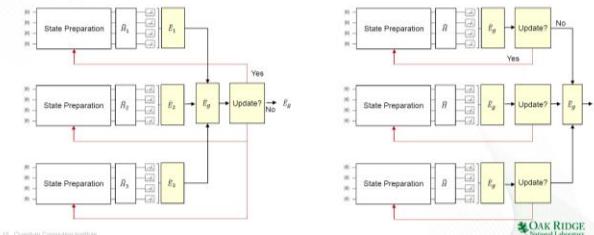
### Computational Chemistry with Quantum Computers

- More economical algorithms using the variational principle are available, which searches for the quantum state that minimizes the energy defined by a molecular Hamiltonian.



### Algorithmic Decomposition for Accelerator Architecture

- VQE may be classically parallelized across sample space or search space but which choice gives the best performance?



VQE can also be used to train a machine learning model<sup>1072</sup>.

### Quantum Approximate Optimization Algorithm

Another famous hybrid algorithm is the Quantum Approximate Optimization Algorithm (**QAOA**), created by Edward Farhi in 2014. It is a combinatorial optimization algorithm used in particular in graph and slice management problems (MaxCut). It has the advantage of requiring a low depth of quantum gates<sup>1073</sup>.

<sup>1071</sup> Schemas source: [Quantum Computing for Scientific Discovery: Methods, Interfaces, and Results](#) by Travis Humble du Quantum Computing Institute, Oak Ridge National Laboratory, March 2018 (47 slides).

<sup>1072</sup> It is now possible to get rid of the classical part of the algorithm as explained in [An adaptive variational algorithm for exact molecular simulations on a quantum computer](#), by Sophia Economou et al, 2019 (9 pages).

<sup>1073</sup> See [Quantum Approximate Optimization Algorithm explained](#), May 2020, [An Introduction to Quantum Optimization Approximation Algorithm](#) by Qingfeng Wang and Tauqir Abdullah, December 2018 (16 pages), [QAOA: Quantum Approximate Optimization Algorithm](#) by Peter Shor (25 slides), [Quantum Approximate Optimization Algorithm: Performance, Mechanism, and Implementation on Near-Term Devices](#), by Leo Zhou, Mikhail Lukin et al, 2019 (23 pages) and [Quantum approximate optimization of non-planar graph problems on a planar superconducting processor](#) by Matthew P. Harrigan et al, 2021 (19 pages) which uses a QAOA algorithm on Google's 53 qubits Sycamore.

# Quantum inspired algorithms

Quantum inspired algorithms are classical algorithms whose design is inspired by quantum algorithms and interference management, but not programmed as quantum algorithms run through a classical emulator. Quantum inspired algorithms can be helpful in solving linear algebra problems, simulating quantum systems, with portfolio optimization, recommendation systems (like with the famous solution from Ewin Tang) and machine learning.

They are used in finance, healthcare and by many startups<sup>1074</sup>. Quantum software startups find in quantum inspired algorithms a way to monetize their know-how while waiting for sufficiently powerful quantum computers. Creating a quantum inspired algorithm is said to rely on “dequantizing” a quantum algorithm<sup>1075</sup>.

**classical algorithms designed with inspiration coming from quantum algorithms**

**in specific cases, they are more efficient than classical algorithms**

*“quantum-inspired algorithms can perform well in practice provided that stringent conditions are met: low rank, low condition number, and very large dimension of the input matrix. By contrast, practical datasets are often sparse and high-rank, precisely the type that can be handled by quantum algorithms”.*

**examples:**

- **Qi genetic algorithms** – 1996
- **Qi evolutionary algorithm** - 2002
- **linear systems of equations**
- **portfolio optimization**
- **recommendation systems**

A quantum-inspired classical algorithm for recommendation systems

Ewin Tang

May 10, 2019



## Complexity theories

So far, we have reviewed a lot of the most common quantum algorithms and their theoretical acceleration.

Quantum computing is sometimes presented as a miracle solution to extend computing capacities beyond the limits of classical supercomputing. It allows solving so-called "intractable" problems on conventional computers.

But what is the nature of the problems that can be solved with a quantum computer and that cannot be solved with classical computers? And above all, what are the limits of quantum computers? Do we still have computational limits?

We will see that these limits are rather blurred and shifting over time. This deals with **complexity theories**, a rather cryptic field of science and mathematics. It is a very abstract world involving a cryptic semantic made of P, NP, BQP and other complexities classes. Mathematicians have been discussing for half a century whether **P = NP** or not. This is the science of problem complexity classes. Behind these mathematics of complexity lie key technical but also philosophical considerations that are fundamental to Man and his omnipotence and control desires.

<sup>1074</sup> See the review paper [Quantum inspired algorithms in practice](#) by Juan Miguel Arrazola, Seth Lloyd et al, 2020 (24 pages).

<sup>1075</sup> See one example in [Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing quantum machine learning](#) by Nai-Hui Chia, Ewin Tang et al, October 2019 (79 pages).

Problem complexity classes are Russian dolls more or less nested with each other that describe the range of time it takes to solve a problem, to verify given solutions and also on the associated required memory space, with regards to the problem size. The size of a problem is often formulated as an integer N, giving the number of items in the problem.

As far as time scales are involved, there are many ways in which this problem solving time scale can grow with N. The key ones are : constant, logarithmic, linear, polynomial and exponential. In this time scale, a time is considered reasonable if it is polynomial or below polynomial in the growing scale. A polynomial time is proportional to a given power of N.

Quantum computing allows under certain conditions to solve certain exponential problems in a polynomial time. It must be translated in : a given problem that would require an exponential time to be solved on a classical computer would require a polynomial time to be solved on a quantum computer.

But what lies beyond exponential time? There are still various inaccessible problems with, for example, exponential of exponential time scales. And we have also exponential memory space which can add another complexity dimension. Quantum computers will not be able to solve all these problems, even when we will be able to align gazillions of logical qubits.

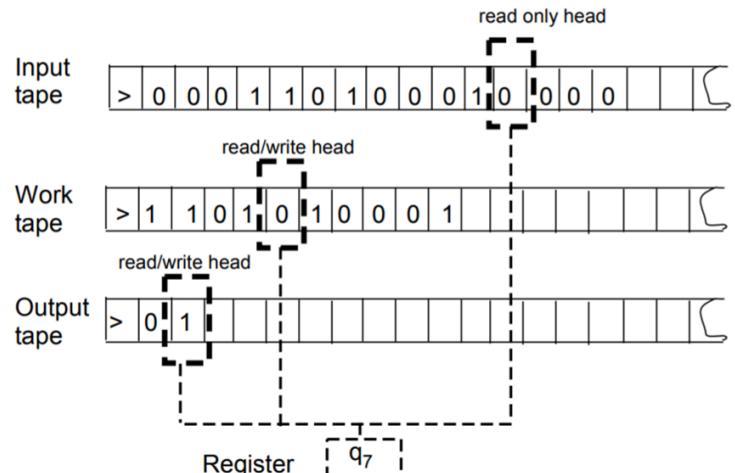
These limitations have an indirect impact on predictions about the creation of some omniscient artificial intelligences capable of transcending human reasoning and solving all problems. This hypothetical AGI (Artificial General Intelligence) will be limited by the data and concepts that feed it and by the impossibility of solving all complex problems.

Mankind will continue to confront impossible computing tasks. It will not be able to solve all the complex problems around! Quantum computing does not allow us to dominate nature, to put the whole Universe in equations and to predict how it will run with quantum precision. Chance and the unexpected will continue to play a role in a very indeterministic world, and for the better. It is a small lesson in humility for Mankind.

## Problem Complexity Classes

To dive into complexity classes, you need to define the main classes of problems by level of complexity. Here I am trying to simplify complexity, this time in the literal sense of the word.

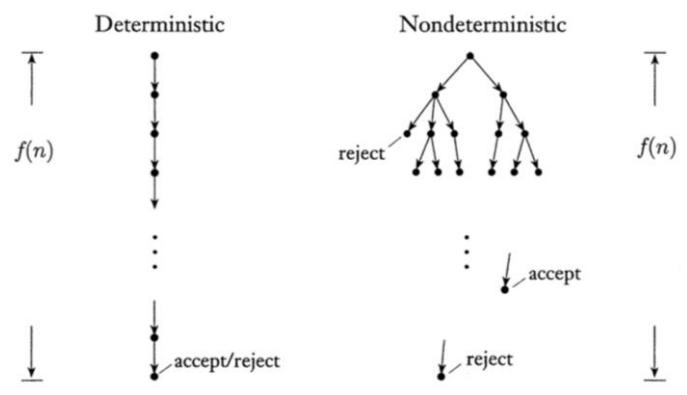
Complexity classes often describe problems that are solved by using brute force with testing several combinations to find the ones matching some criteria (like with the so-called SAT problems) or with using mathematical equations defining complex systems (differential equations, Schrödinger's equation, ...). Problem classes use the notion of Turing's deterministic and non-deterministic machines. Turing machines are conceptual models of computers created by Alan Turing before the Second World War.



They model computer processing based on the notion of programs and data, embodied by continuous and infinite rolls of paper, the first for the program, the second for the input data and the third for generating the results<sup>1076</sup>. Turing's theoretical model has long been used to define classes of problems that can or cannot be solved by a computer.

Computers are all metaphorically Turing machines, reproducing this logic by reading program instructions and managing data in random access memory (RAM) or persistent storage (hard disk, SSD, ...). Associated with the notion of Turing machine is the notion of **Church-Turing's thesis**, named after Alonzo Church and Alan Turing, according to which there is an equivalence between computational problems that can be solved manually and with unlimited resources, those that can be handled with a Turing machine and those that can be solved with so-called recursive functions.

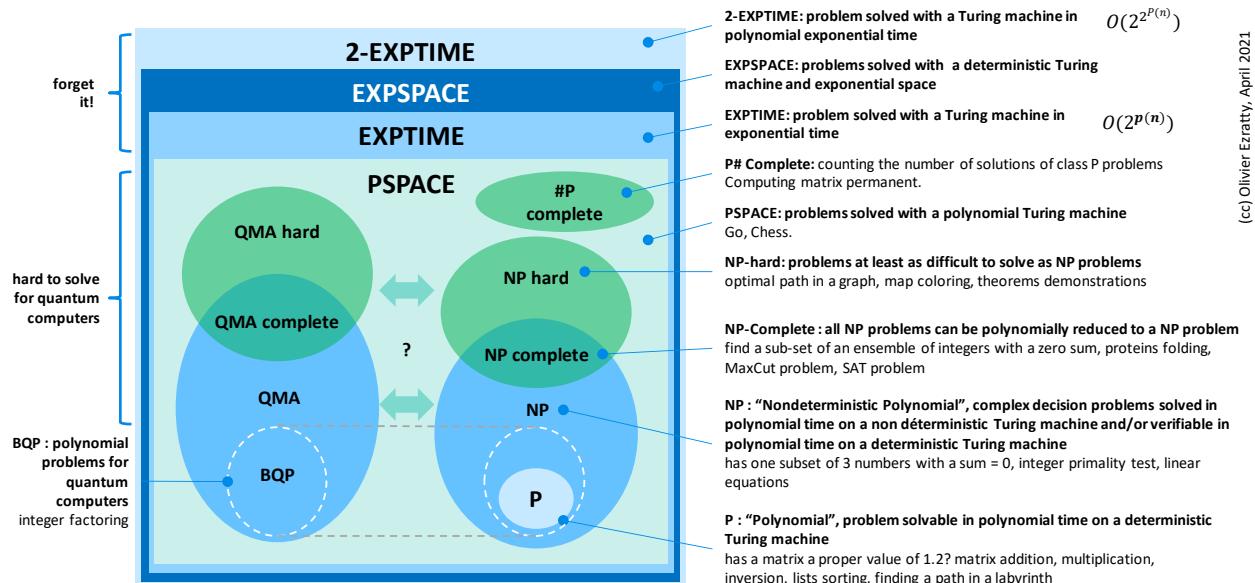
In a deterministic machine, the sequence of actions to be performed is predetermined and sequential. In the non-deterministic Turing conceptual machine model, computational rules can lead to execute several different operations for each evaluated situation. Basically, by exploring several paths in parallel and looking for a positive response to an algorithm component and closing parallel test loops once the sub-solutions are found.



A non-deterministic machine increases the computational combinatorics compared to a deterministic machine. And this combinatorics usually jumps from polynomial to exponential.

## Generic complexity classes

The level of complexity refers to the computing time and memory space required for these calculations. We are usually limited by computing time long before being limited by the available memory. However, some problems such as scheduling reach memory limits before computation limits.



<sup>1076</sup> Source for the diagram: [Computational Complexity: A Modern Approach](#) by Sanjeev Arora and Boaz Barak, 2007 (489 pages). This is a good reference document on complexity theories. Students of a master's degree from ENS Lyon made a Turing machine in Lego in 2012 to celebrate the centenary of Alan Turing's birth ([video](#)) and it wasn't the only one of its kind ([video](#))! Another one was made with wood in 2015 ([video](#)).

The association of a problem to a complexity class is related to the performance of the best-known algorithms to solve problems in that class.

Problem class levels in complexity theories are often based on black box or oracle models to which a system asks questions and gets answers based on the data provided. This is a logic of "brute force" and hypothesis scanning. The scale of the tested combinations depends on problem class.

So here are these classes by increasing level of complexity knowing that we will spend more time on NP related classes.

**L**: or LSPACE, or DLOGSPACE, defines the class of problems that can be solved on a logarithmic scale of consumed memory and on a deterministic Turing machine, that is, on a traditional computer. Computational complexity increases slowly with the size of the problem. Unfortunately, very few complex problems sit in this class. These include queries in previously indexed relational databases, searches for DNA sequences, and generally speaking, search techniques that use pointers and optimize the use of computer memory.

**NL**: is the class of problems solved on a logarithmic time scale on a non-deterministic machine. Complexity theory specialists are still trying to figure out whether  $L=NL$  or not! But they are less busy here than on determining whether  $P \Leftrightarrow NP$ .

**P**: covers problems that can be solved with a time growing polynomially with data to process and on a deterministic machine. If  $N$  is the size of the problem, the processing time is proportional to  $N^M$ , with  $M$  being an integer, preferably 2. It's an easy problem to solve and said to be "tractable". This includes sorting lists, validating the existence of a path in a graph, searching for a minimum path in a graph, multiplying matrices or evaluating a number to see if it is prime.

**BPP**: is a class of problems that can be solved by random approaches ("Bounded-Error Probabilistic Polynomial-Time"). It would seem that  $BPP=P$  but this has not yet been demonstrated.

**NP**: describes the class of problems for which it is easy to check the validity of a solution, i.e. that it can be realized in polynomial time by a deterministic machine. The other definition of the class is that it contains problems whose solution time is polynomial on a non-deterministic machine. These more complex problems have a computing time that is at least exponential when the method used is said to be naive, testing all possible combinations. These are "intractable" problems. In practice, these are problems particularly suited to quantum computers because of their ability to evaluate in parallel  $2^N$  combinations of some classical computation.

Some examples of NP problems are the Steiner tree to determine whether an electrical network can connect a number of houses at a certain price, checking that a DNA sequence is found in several genes and the distribution of tasks to different agents to minimize the time it takes to complete them.

These problems have very concrete equivalents in logistics, planning, production, transportation, telecom, utilities, finance and cryptography.

Note that a "decidable" problem, i.e. one that requires exploring a finite space of options, is not necessarily feasible from a practical point of view. Even if it can be solved in a finite amount of time, its resolution may take too long. An exponential problem has an elegant solution if one can find one solution that has a polynomial or, at best, linear duration. Polynomial times scale better than exponential times!

A big debate has been going on since 1956 (Kurt Gödel) as to whether class P equals class NP. If  $P = NP$ , it would be as simple to find a result when one can also simply verify it. The general consensus is that P is not equal to NP.

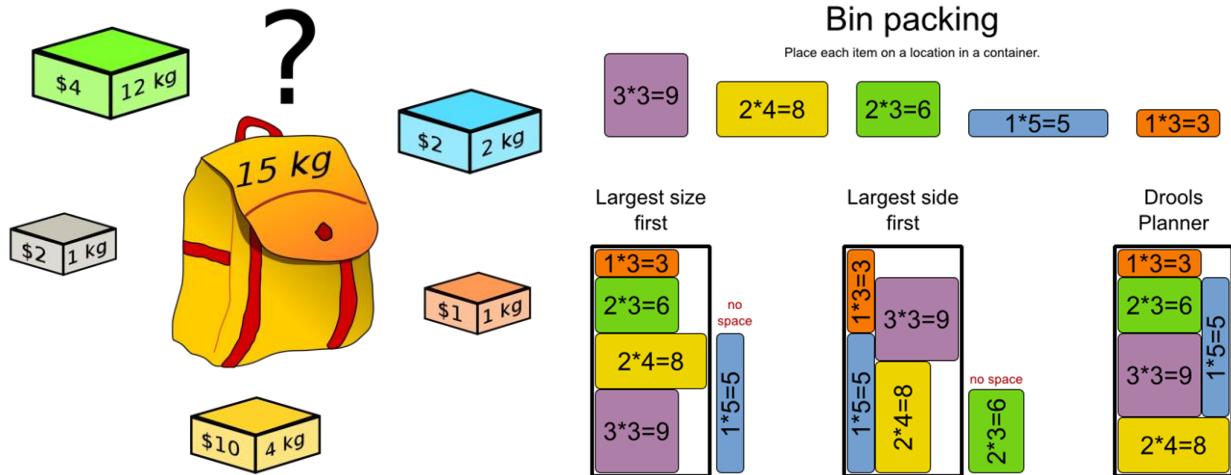
The demonstration of whether or not  $P \neq NP$  is part of one of the seven [Clay Mathematics Institute mathematical challenges](#) launched in 2000, each with a prize of \$1M (*below*)<sup>1077</sup>.

Among these challenges are the demonstration of the Navier-Stokes fluid mechanics equations and of Riemann's hypothesis on the distribution of prime numbers.

On the  $P$  vs  $NP$  side, the [wording of the challenge](#) provides an example of such a problem: you have to allocate 50 rooms of two students to 400 candidates but some candidates do not need to live in the same room. The combinatorial choice of 100 students among 400 is huge, so the problem is not easily handled with a supercomputer and brute force. It is indeed an  $NP$  problem because a given solution is easy to verify because it is simple to check that none of the rooms contains a forbidden pair of individuals. It is a bit like an all-or-nothing theory because if  $P = NP$ , all  $NP$  problems have an efficient polynomial solution. If  $P \neq NP$ , none of the  $NP$  problems have a "pure" efficient solution<sup>1078</sup>.

The definition of the problem classes  $NP$  and  $NP$ -Complete is relatively recent<sup>1079</sup>.

**Complete  $NP$ :** according to Richard Karp, it is defined as problems in which other  $NP$  problems can be polynomially reduced. They have no known  $P$  (polynomial) solution. They are not accessible to quantum computers. It is in this class that we find the SAT or 3SAT type Boolean logic problems! More than 3000  $NP$ -Complete problems are identified to date ([list](#)).



<sup>1077</sup> A Brazilian researcher, André Luiz Barbosa, published in 2010 his [P ≠ NP Proof](#) (25 pages) as well as a paper invalidating Cook's theorem that a Boolean SAT problem is  $NP$ -Complete, [The Cook-Levin Theorem Is False](#), 2010 (11 pages). But this work seems ignored by specialists.

<sup>1078</sup> The classical method for solving these problems is to use heuristics allowing to obtain a satisfiable approximate solution, therefore not necessarily optimal, and in particular via probabilistic approaches.

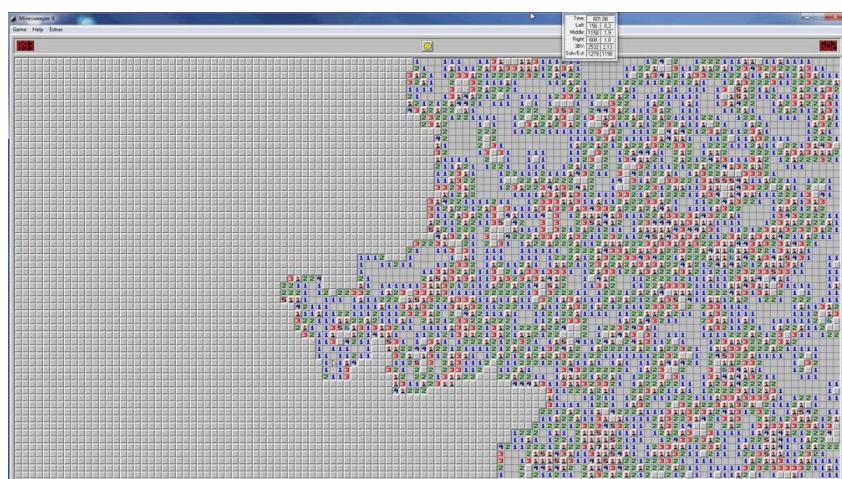
<sup>1079</sup> It is derived from [The complexity of theorem-proving procedures](#) by Stephen Cook of the University of Toronto, 1971 (8 pages), best popularized in [An overview of computational complexity](#) (8 pages) and [Reducibility among combinatorial problems](#) by Richard Karp, 1972 (19 pages) and in [Complexity and calculability](#) by Anca Muscholl of the LaBRI, 2017 (128 slides).

One of the typical problems is filling up the trunk of a car when you go on vacation or when you come back from Christmas with a bunch of presents for your family. And then the **bin packing** problem consisting in filling a backpack in an optimal way with a set of objects, to obtain the largest load and without exceeding a maximum weight (*aka* "bin packing" or "knapsack" problems)<sup>1080</sup>.

It also includes the **subset sum problem** of finding a subset of a set of integers whose sum is equal to an arbitrary integer.

The **deminer's problem** consists in locating hidden mines in a field with only the number of mines in adjacent areas and the total number of mines in the field as an indication. All this without detonating them. It is a game well known by Windows users, launched in 1989<sup>1081</sup>!

The simulation of complex protein folding is also a NP-Complete problem<sup>1082</sup>.



So this would be a potentially very difficult problem to solve with a quantum computer with large proteins.

It is demonstrated that if an optimal solution to an NP-Complete problem could be found, all the solutions to problems in this class would be found. This is the important notion of problem reduction.

Graphs coloring with different colors for knots, branches or surfaces is part of the NP, NP-Complete and NP-Hard problems. The first two cases requiring a number of colors depending on the maximum number of connections between elements of the graph and the last case, relating to the coloring of maps in different adjacent colors which requires a maximum of four, thanks to the computer demonstration of the four-color theorem done in 1976 by Kenneth Appel and Wolfgang Haken.

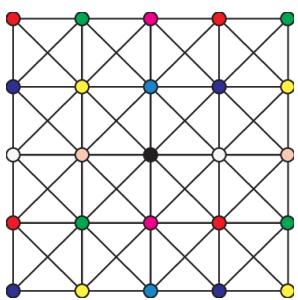
- **Graph nodes** coloring has applications in the placement of mobile antennas and in the allocation of memory registers for a compiler. The problem is NP-Complete for its resolution and NP-Difficult to find its optimal solution.
- **Branch** coloring has applications in the frequency allocation of multimode fiber optic networks. It also allows to optimize the placement of objects or persons according to their compatibility or incompatibility (*aka* : the wedding tables problem). Optimum coloring is a NP-Hard problem.
- **Area map** coloring is used to define the coverage areas of mobile radio antennas or telecommunications satellites. It can even be used to allocate microwave frequencies for the activation of superconducting qubits. The coloring with three colors is an NP-Complete problem.

---

<sup>1080</sup> Illustration sources: [Wikipedia](#) and [Stackoverflow](#).

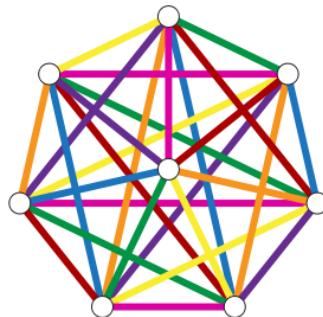
<sup>1081</sup> [Source](#) of the illustration.

<sup>1082</sup> See [Is protein folding problem really a NP-complete one ? First investigations](#), 2013 (31 pages).



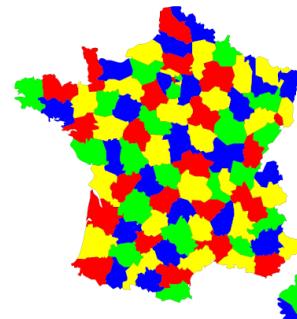
**nodes**  
k colors coloring: **NP-complete**  
find the minimum number of colors :  
**NP-hard**

telecom radio frequencies  
allocations



**segments**  
k colors coloring: **P**  
optimum coloring: **NP-hard**

WDM optical fiber frequency  
allocations



**zones**  
determine if coloring is possible with 3 colors:  
**NP-complete**  
coloring with 4 colors: **P**

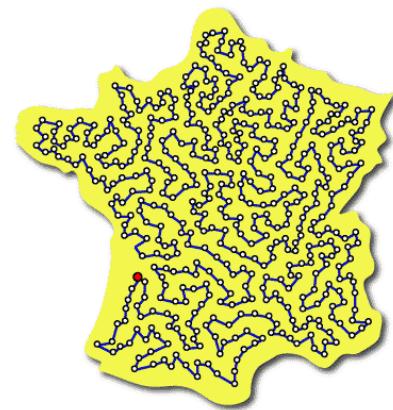
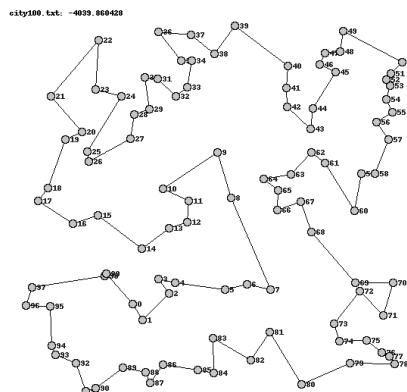
define antenna coverage zones for telecom  
cellular networks, allocating micro-wave  
frequencies in superconducting qubits

In general, many C problem classes have a subclass C-Complete and C-Hard. A problem is C-Hard if there is a type of reduction of problems from class C to this problem. If the problem C-Hard is part of class C, then it is said to be "C-Complete"<sup>1083</sup>.

**NP Hard:** covers optimization problems where a minimum or a maximum is sought with a large combinatorics. A problem is NP-Hard if all NP-Complete problems can be reduced by polynomial simplification to this problem. It is the case of the solution of the **traveling salesman problem** where one must test a large combination of routes to find the quickest one passing through a fixed number of cities. In this case, all solutions must be tested.

If a traveler has to go through 125 cities in less than 30 days, if there is a solution that works in that time frame, then the problem is NP.

But nothing says that all the solutions have been found. Solving the problem below an arbitrary travel time with a return to the starting point is an NP-complete problem. This is called a Hamiltonian circuit: a path running a graph passing once and only once through each of the nodes and returning to its starting point. The determination of the shortest travel time is NP Hard.



what is the shortest possible route that visits each place exactly once and returns to the origin place : **NP-hard**

The brute force algorithm to solve it has a time that depends on  $N!$  where N is the number of nodes in the network. The known optimum time is  $N^2 2^N$ . The problem is difficult to solve beyond 20 steps<sup>1084</sup>!

<sup>1083</sup> For more information, see in particular Complexity Theory [Part I](#) (81 slides) and [Part II](#) (83 slides), which is part of a [Stanford course on Complexity Theories, Calculability and Complexity- Some Results I Know](#) by Etienne Grandjean of the University of Caen, 2017 (43 slides) as well as this [video](#) by Olivier Bailleux (2017, 20 minutes).

<sup>1084</sup> See [The Traveling Salesman Problem](#) site which provides some examples of such problems such as the itinerary of all 49,687 English pubs or 49,603 tourist places in the USA.

The NP-Hard problem class also contains a number of **Nintendo** games like Super Mario Bros, The Legend of Zelda and Pokemon<sup>1085</sup>. Quantum computing would not be able to solve the most complex NP-Hard problems.

**PSPACE**: is the class of problems that can be solved in polynomial space on a deterministic machine. **NPSPACE** is the class of problems that can be solved in polynomial space on a non-deterministic machine. And **NPSPACE = PSPACE** according to [Savitch's theorem](#).

**EXPTIME**: is the class of problems decidable in exponential time by a deterministic machine. Precisely, the computation time of these problems is  $2^{p(N)}$  where  $p(N)$  is a polynomial of  $N$ ,  $N$  being the level of complexity of the problem. They are intractable with traditional machines. Some of these problems can be converted into problems that can be treated polynomially by quantum computers. Chess and Go games on arbitrarily sized grids belong to this category. In size-limited grids, the exponential effect has limits. These were exceeded for Deep Blue's chess game in 1996 and for DeepMind's AlphaGo game of Go in 2016 and 2017.

**NEXPTIME**: is the class of problems decided in exponential time by a non-deterministic machine with unlimited memory space.

**EXPSPACE**: is the class of problems that can be solved in exponential space. In other words, they are difficult to access on today's and even tomorrow's machines.

**2-EXPTIME**: is a class including the previous ones that covers decision problems that can be solved by a deterministic Turing machine in double exponential time with an order of magnitude of  $O(2^{2^{P(n)}})$  where  $P(n)$  is a polynomial of  $n$ . In other words, it's an exponential of an exponential problem.

We should add the class #P of problems for counting the number of solutions of class P problems, which are solved in polynomial time. Proposed in 1979 by Leslie Valiant, it obviously has its associated classes #P Hard and #P Complete. The computation of the permanent of a square matrix filled with 0 and 1 is a complete #P problem according to Ben-Dor and Halevi's theorem demonstrated in 1993. In 2011, Scott Aaronson demonstrated that the calculation of the permanent of a matrix is a #P Difficult problem<sup>1086</sup>. All this is related to the numerical simulation of the boson sampling which is compared to its resolution by photon-based systems that we study in a section on [photon qubits](#), page 340.

The classes PSPACE, EXPTIME, NEXPTIME, EXPSPACE and 2-EXPTIME do not correspond to practical problems that are easy to identify in everyday life. They cover the problems of predicting the behavior of ultra-complex systems with strong interactions. If it is possible that modeling the folding of a protein is an NP problem, what would be the class of problem to simulate the functioning of a whole living cell, or even a multicellular organism? There are so many interactions at the atomic, molecular and cellular level that the class of this kind of problem is probably well beyond NP-Hard level.

There are many other problem complexity classes that won't be described here: EXP, IP, MIP, BPP, RP, ZPP, SL, NC, AC0, TC0, MA, AM and SZK! You can find them in the [ComplexityZoo](#) site which inventories the zoo of problem complexity classes. There seems to be more than a hundred of them<sup>1087</sup>.

---

<sup>1085</sup> See [Classic Nintendo Games are \(Computationally\) Hard](#), 2012 (36 pages).

<sup>1086</sup> In [A Linear-Optical Proof that the Permanent is #P-Hard](#) par Scott Aaronson, 2011 (11 pages).

<sup>1087</sup> To learn more about the subject of complexity theories, you can read the well-documented [Computational Complexity A Modern Approach](#) by Sanjeev Arora and Boaz Barak of Princeton University, 2007 (489 pages).



Navigation

[Main page](#)  
[Community portal](#)  
[Current events](#)  
[Recent changes](#)  
[Random page](#)  
[Help](#)

Toolbox

[What links here](#)  
[Related changes](#)  
[Special pages](#)  
[Printable version](#)  
[Permanent link](#)

## Complexity Zoo:F

[Back to the Main Zoo - Complexity Garden - Zoo Glossary - Zoo References](#)[Complexity classes by letter: Symbols - A - B - C - D - E - F - G - H - I - J - K - L - M - N - O - P - Q - R - S - T - U - V - W - X - Y - Z](#)[Lists of related classes: Communication Complexity - Hierarchies - Nonuniform](#)[FBQP](#) - [FERT](#) - [FPERT](#) - [Few](#) - [FewEXP](#) - [FewP](#) - [FH](#) - [FIXP](#) - [FNL](#) - [FNL/poly](#) - [FNP](#) - [FO](#) - [FO\(DTC\)](#) - [FO\(LFP\)](#) - [FO\(PFP\)](#) - [FO\(TC\)](#) - [FO\( \$t\(n\)\$ \)](#) - [FOLL](#) - [FP](#) - [FP<sup>NP\[log\]</sup>](#) - [FPL](#) - [FPR](#) - [FPRAS](#) - [FPT](#) - [FPT<sub>nu</sub>](#) - [FPTAS](#) - [FQMA](#) - [friP](#) - [F-TAPE\( \$f\(n\)\$ \)](#) - [F-TIME\( \$f\(n\)\$ \)](#)

### **FBPP: Function BPP**

Has the same relation to [BPP](#) as [FNP](#) does to [NP](#). Equivalently, it is the randomised analogue of [FP](#).

### **FBQP: Function BQP**

Has the same relation to [BQP](#) as [FNP](#) does to [NP](#).

There exists an oracle relative to which [PLS](#) is not contained in [FBQP](#) [Aar03].

### **FERT: Fixed Error Randomized Time**

[FERT](#) and [FPERT](#) are parameterized classes. [FERT](#) formally defined as the class of decision problems of the form  $(x, k)$ , decidable in polynomial time by a probabilistic Turing Machine such that

1. If the answer is yes, the probability of acceptance is at least  $1/2 + \min(f(k), 1/|x|^c)$
2. If the answer is no, the probability of acceptance is at most  $1/2$

Here,  $f$  is an arbitrary function (from the reals to  $<0, 1/2]$ ).

Defined in [KW15]. Contains [BPP](#) and is contained in [para-PP](#) and in [FPERT](#).

## Quantum complexity classes

Let's now discuss the classification of problems that are theoretically addressable by quantum computers, the correspondence with the *above* classes being still a problem that is not entirely solved!

The classification is different because quantum computers can parallelize processing in an exponential way while classical computers like Turing machines cannot do it.

This is still very theoretical since it doesn't take into account known constraints of quantum computers: their short coherence time and creates constraints on the number of quantum gates that can be chained together to solve a problem. This is a constraint that traditional computers do not have. But again, theoretically, this computation time constraint could be removed with using correction error codes.

**PH:** is a class of problems that generalizes the [NP](#) class. PH means "Polynomial Hierarchy".

**BQP:** defines a class of problem that is processable in polynomial time on a quantum computer with a constrained error rate. This may in some cases correspond to [P](#) problems. The class was defined in 1993, when the first quantum algorithms appeared.

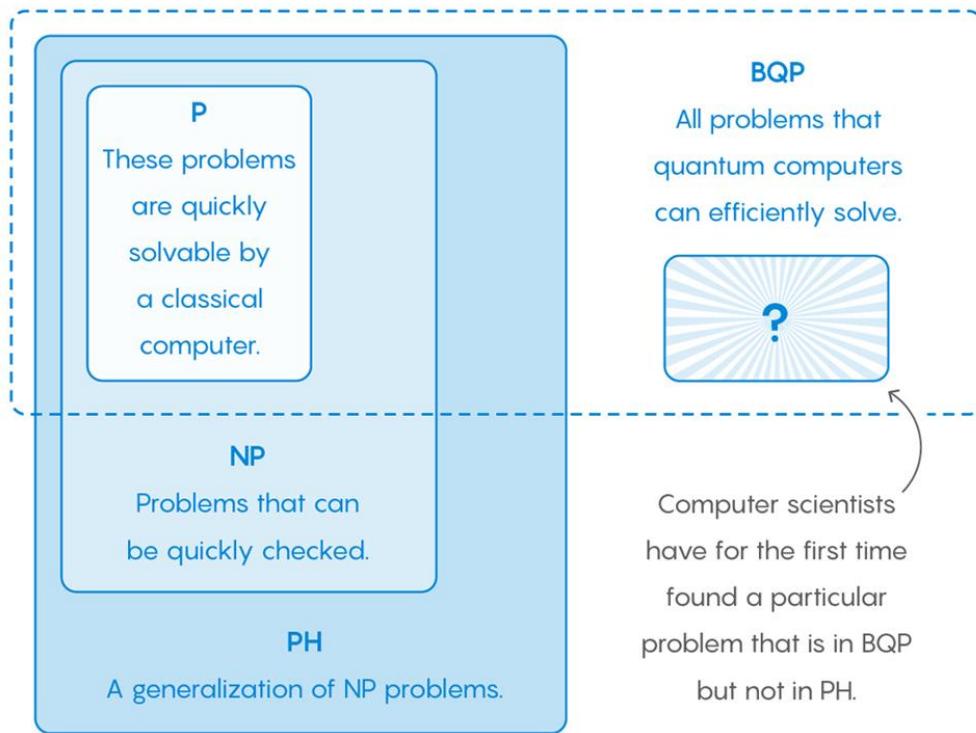
Whether the BQP class is really different from the P class is an ongoing debate. It has already been shown that the P class of polynomial problems is in BQP. But is NP in BQP? Seems not. It is however difficult to prove it in a generic way. The exact relationship between BQP and NP is still unknown.

The key point is to find algorithms that are part of BQP (processable in quantum) and that are not in PH (processable with any present and future classical architecture). This uncertainty has been removed only very recently<sup>1088</sup>. Oracle-based algorithms were found that are in BQP but not in PH.

<sup>1088</sup> See [Finally, a Problem That Only Quantum Computers Will Ever Be Able to Solve by Kevin Hartnett](#), 2018, referring to [Oracle Separation of BQP and PH](#) by Ran Raz and Avishay Tal, May 2018 (22 pages), presented in the Electronic Colloquium on Computational Complexity conference. This is the source of the illustration on this page.

## A New Island on the Complexity Map

What can a quantum computer do that any possible classical computer cannot? Computer scientists have finally found a way to separate two fundamental computational complexity classes.



Therefore, these algorithms have a polynomial resolution time on quantum computers which remains exponential on their equivalent crafted for classical computers.

By the way, what about a possible complexity difference for problems manageable with universal gate quantum accelerators vs. quantum annealing accelerators? According to several researchers, there is no difference<sup>1089</sup>. Various theorems show that a problem that can be solved with universal quantum gates can also be solved with a D-Wave quantum annealing architecture and vice versa with only a polynomial time difference.

**QMA** (for Quantum Merlin Arthur) defines a class of problems that is verifiable in polynomial time on a quantum computer with a probability greater than 2/3. It is the quantum analog of the "traditional" NP complexity class. The QMA class contains the classes P, BQP and NP<sup>1090</sup>. Like the NP class, the QMA class has two derived subclasses, QMA Complete and QMA Hard. In practice, these are difficult problems to solve with quantum computers. Unfortunately, the literature on the subject does not describe its nature or provide examples. This is a pity for those who appreciate a practical sense of things!

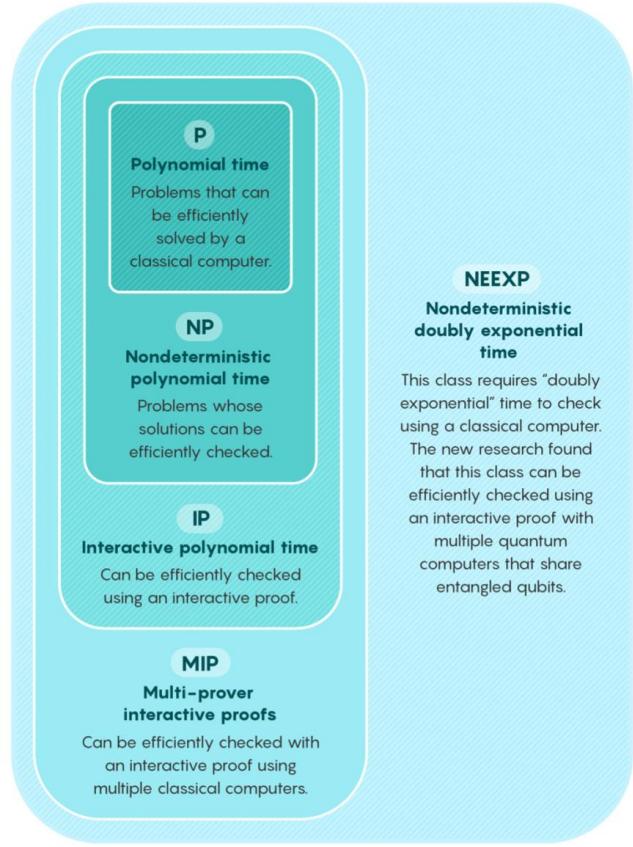
**QCMA** is a hybrid problems class situated between QMA and NP. The proof is provided in classical polynomial time but the resolution is at the QMA level and is performed in a quantum way.

<sup>1089</sup> See [Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation](#) by Dorit Aharonov, Wim van Dam and Julia Kempe (from CNRS), 2008 (30 pages).

<sup>1090</sup> See [QMA-complete problems](#) by Adam Bookatz, 2013 (18 pages).

Many publications point out the limitations of quantum algorithms and computers. A BQP problem that is not in PH gives the advantage to quantum computing. But exponential intractable problems for which the improvement brought by quantum computing is only a square root of classical time do not change their exponential nature. This is what Scott Aaronson points out<sup>1091</sup>. Complete NP problems and beyond remain inaccessible to quantum computers. Brute force has limits that even quantum computing cannot overcome in theory! This partly explains the difficulty of creating efficient quantum algorithms.

Finally, **NEEXP** is a class of problems that requires a double exponential computation time for its verification. Recent work shows that a result can be verified with several quantum computers with entangled qubits. This does not however enable us to solve this type of problems<sup>1092</sup>!



Some problems are undecidable, i.e. they cannot be solved by an algorithm, no matter how much time you have. This is the case for the determination of the end of a Turing machine program.

In other words, there is no program that is able to know whether any program written in a common programming language will stop or loop for an infinite amount of time.

However, in 2020, there was some progress with a demonstration that the classes MIP\* and RE were identical<sup>1093</sup>.

In the same order, **Rice's theorem** demonstrates that no non-trivial property of a program can be decided algorithmically. All this is to say that there is no automatic method to detect bugs in a program or to certify that it runs well. There are, however, formal methods of proof that can be used to certify the execution of specific programs. This involves the use of formal program specifications that serve as a reference for assessing how well a program is running. This is already widely used, without quantum, in industrial information technology and in critical systems such as aerospace.

## Quantum speedups

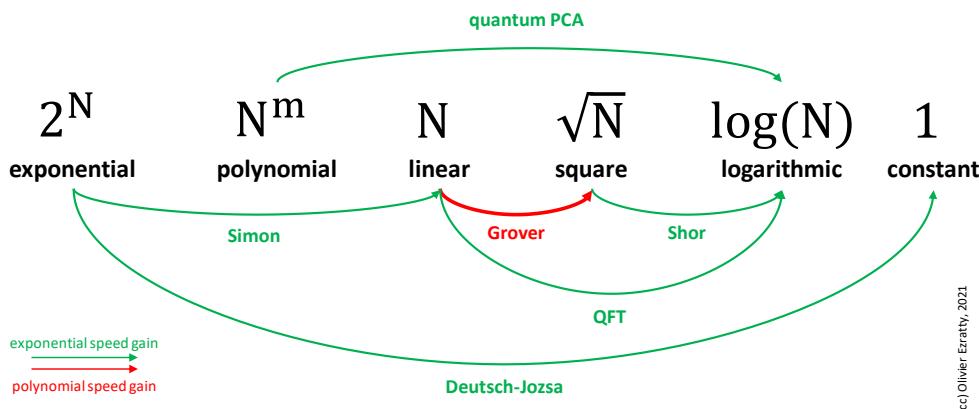
The chart *below* summarizes the theoretical performance gains of some of the deterministic algorithms we have just seen. Complexity levels (exponential, polynomial, linear, ...) are generic.

<sup>1091</sup> See [The Limits of Quantum Computers](#) (16 pages) and [NP-complete Problems and Physical Reality](#) (23 pages).

<sup>1092</sup> See [NEEXP in MIP\\*](#) by Anand Natarajan and John Wright, 2019 (122 pages) and [Computer Scientists Expand the Frontier of Verifiable Knowledge](#), 2019.

<sup>1093</sup> The MIP\* class of problems that can be verified by quantum entanglement is equal to the RE class of problems that are no more difficult than the problems of program termination. See [A quantum strategy could verify the solutions to unsolvable problems - in theory](#) by Emily Conover, 2020 which refers to [MIP\\*=RE](#) by Zhengfeng Ji et al, January 2020 (165 pages) and seen in [Mathematicians Are Studying Planet-Sized Computers With God-Like Powers](#) by Mordechai Rorvig, 2020. See [Landmark Computer Science Proof Cascades Through Physics and Math](#) by Kevin Hartnett, March 2020.

The precise levels of complexity of each algorithm are roughly associated with these classes.  $N \log(N)$  is the complexity of a classical Fourier transform and is nearly linear since  $N$  grows much faster than  $\log(N)$  and  $\log(N)^3$  is a log level complexity for the Shor algorithm and a QFT.



An exponential gain is also obtained when we move from  $N$  or  $\sqrt{N}$  to  $\log(N)$ . A QFT thus generates a theoretical exponential gain. The time scales are more meaningful in the table [next<sup>1094</sup>](#).

Complexité	$n$	$n \log_2 n$	$n^2$	$n^3$	$1.5^n$	$2^n$	$n!$
$n = 10$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	4 s
$n = 30$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	18 min	$10^{25}$ ans
$n = 50$	< 1 s	< 1 s	< 1 s	< 1 s	11 min	36 ans	$\infty$
$n = 100$	< 1 s	< 1 s	< 1 s	1s	12, 9 ans	$10^{17}$ ans	$\infty$
$n = 1000$	< 1 s	< 1 s	1s	18 min	$\infty$	$\infty$	$\infty$
$n = 10000$	< 1 s	< 1 s	2 min	12 jours	$\infty$	$\infty$	$\infty$
$n = 100000$	< 1 s	2 s	3 heures	32 ans	$\infty$	$\infty$	$\infty$
$n = 1000000$	1s	20s	12 jours	31, 710 ans	$\infty$	$\infty$	$\infty$

The ideal performance gains is to traverse several complexity scales, and particularly for an exponential problem. In practice, the main algorithms skip one or two complexity classes, but not necessarily from the exponential problem class. But my scheme is misleading.  $N$  can also grow exponentially depending on the size of a problem. The classic example is Shor's algorithm.

The starting point is an  $N$  which is actually an RSA key size which itself is evaluated in power of 2. A 1024-bit key is  $2^{1024}$ . If we move from  $2^{256}$  to  $2^{1024}$ , the growth of the key size is exponential. With Shor's algorithm, we get an exponential performance gain by going from a square root of  $2^{1024}$  to  $\log(2^{1024})$ , that is to say 1024 (in log base 2)! So the time scale move from  $2^{512}$  to 1024, which is a perfectly exponential gain.

Deutsch-Jozsa's algorithm has the particularity of traversing all levels of this scale, from an exponential time to a fixed time. We have unfortunately seen that it has no known practical application.

The speedup gain from an algorithm depends on the gates it's using. Shor's algorithm and any QFT based algorithm provide an exponential gain since it uses phase-controlled R gates. Grover's algorithm is providing a polynomial gain since it uses only Hadamard gates. But Deutsch-Jozsa's algorithm has an exponential gain although it is using only Clifford's group gates like the Hadamard gate. Why so? Because it uses an Oracle function that may use non-Clifford's group gates<sup>1095</sup>.

<sup>1094</sup> Table source: [Complexity in time](#), Ecole Polytechnique (25 pages).

<sup>1095</sup> See [Focus beyond quadratic speedups for error-corrected quantum advantage](#), by Hartmut Neven et al , 2021 (11 pages) that also explain why quadratic speedups are not efficient due to the error correction overhead.

Other exponential speedups have been found for various algebraic algorithms like **estimating Gauss sums**<sup>1096</sup>, **approximating Jones polynomial** that is not based on a QFT and still brings some exponential speedup, with some applications in topological quantum computing<sup>1097</sup> or counting solutions of **finite field equations**<sup>1098</sup>. But don't count on me to explain what it's all about!

It is also necessary to boil in the fact that the complexity of some problems can be addressed on conventional computers with probabilistic or heuristic approaches that also allow a significant reduction of the computing time of exponential problems. Practically, when moving from this kind of solution to a quantum algorithm, we replace one probabilistic approach with another since quantum computing is also highly probabilistic and prone to many computing errors.

All in all, quantum algorithms are attractive but they are not always the only solution to cleverly solve a complex problem.

This is amplified by the emulation going on between algorithms designers. Each and every new quantum performance challenges the classical supercomputers algorithms designers to improve the performance of their own tools. This is what Toshiba did in 2019 with a classic optimization algorithm that was 10 times more powerful than the state of the art. That was fine even though a linear x10 gain is still not an exponential progress<sup>1099</sup>.

This being said, even if a polynomial gain is considered as a minor gain in complexity theories, it can still have a non-negligible practical value and make quantum computing attractive, without going through the Holy Grail of some fancy exponential acceleration.

But the devils in the details have to be cared about<sup>1100</sup>:

- First, the quantum speedup will be affected by the number of times the algorithm must be run. It's taken into account in some of the speedups like with Grover's algorithms but not always. These repetitions are also named shot count or shots. It depends on the problem, the number of qubits and the algorithm output (integers, real numbers). With Google's supremacy and its 53 qubits, it was 3 million shots. With IBM Q System One using from 5 to 28 qubits, the typical proposed shots number ranges from 1000 to 8000 shots.
- The quantum advantage is also depending on the number of qubits in your register that are put in superposition using Hadamard gates. Other qubits might be used elsewhere in the algorithm such as ancillas.
- Data preparation must also be taken into account, which is of particular importance for quantum machine learning algorithms<sup>1101</sup>.
- The same should be said of oracle based algorithms, particularly when they rely on some classical data access.
- Then, with large scale quantum computing, quantum error correction will add some additional burden. Using concatenation codes, you may lose polynomially on your speedup. Meaning that an initial polynomial speedup may be lost at this stage.

---

<sup>1096</sup> See [Efficient Quantum Algorithms for Estimating Gauss Sums](#) by Wim van Dam and Gadiel Seroussi, 2008 (11 pages).

<sup>1097</sup> See [A Polynomial Quantum Algorithm for Approximating the Jones Polynomial](#) by Dorit Aharonov, Vaughan Jones and Zeph Landau, 2006 (19 pages).

<sup>1098</sup> See [Quantum computing and polynomial equations over the finite field](#) by Christopher M. Dawson et al, 2004 (7 pages).

<sup>1099</sup> See [Toshiba Promises Quantum-Like Advantage on Standard Hardware](#) by Tiffany Trader, 2020, which references [Combinatorial optimization by simulating adiabatic bifurcations in nonlinear Hamiltonian systems](#) by Hayato Goto et al, April 2019 (9 pages).

<sup>1100</sup> This is well explained in [What Is the Quantum Advantage of Your Quantum Algorithm?](#) by Jack Krupansky, February 2020.

<sup>1101</sup> See [Information-theoretic bounds on quantum advantage in machine learning](#) by Hsin-Yuan Huang, Richard Kueng and John Preskill, April 2021 (34 pages) which describes the conditions when QML algorithms provide a real speedup.

So, as mentioned before, appreciating the real speedup of any quantum algorithm requires adopting an end-to-end approach taking into account all the parameters of the quantum algorithm execution time.

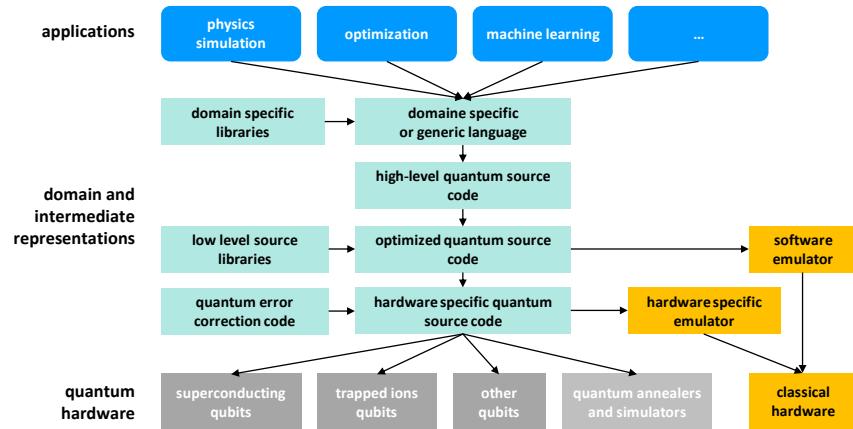
### Quantum algorithms key takeaways

- Quantum algorithms have been created since the early 1990s, over ten years before any quantum computer was working out of a research laboratory.
- Quantum algorithms use very different concepts than classical programming, even including artificial intelligence development tools or object oriented programming. It's based on the manipulation of large matrices and using interferences.
- The main algorithms classes are oracle based and search algorithms, optimization algorithms, quantum physics simulation algorithms and quantum machine learning algorithms.
- A quantum algorithm is interesting if it provides some quantum speedup compared to their equivalent best-in-class classical version, including those that are heuristics based. These problems are said to be intractable on classical hardware. Most of the time, quantum speedups are theoretical and do not incorporate the costs of quantum error corrections and of creating non-Clifford quantum gates. These gates are implementing small phase changes and are used in quantum Fourier transforms and implemented in many other algorithms. A quantum speedup that is not exponential is highly questionable. All of this requires some understanding of complexity classes like P, NP and BQP.
- Another key aspect of quantum algorithms is data loading and/or preparation. It is often overlooked and can have a significant time cost, on top of frequently requiring some form of not-yet-available quantum memory hardware. As a consequence, quantum computing is not adequate for big-data computations.
- Gate-based computers and quantum annealers can exploit hybrid algorithms, combining a classical (preparation) part and a quantum part interacting with each other.
- Quantum inspired algorithms are running on classical computers and using some form of quantum mathematical models like interferences and signals decomposition (Fourier series/transforms).

# Quantum software development tools

We now need to explore quantum computing software to implement the various algorithms we've just uncovered. It is a completely new world with very different paradigms.

Quantum algorithms still require programming, programming languages and development environments. As shown in the diagram<sup>1102</sup>, quantum software is organized in layers with, starting from the bottom, the physical qubits followed by low-level machine language to drive them at the physical level (microwaves length and frequencies, readouts, etc).



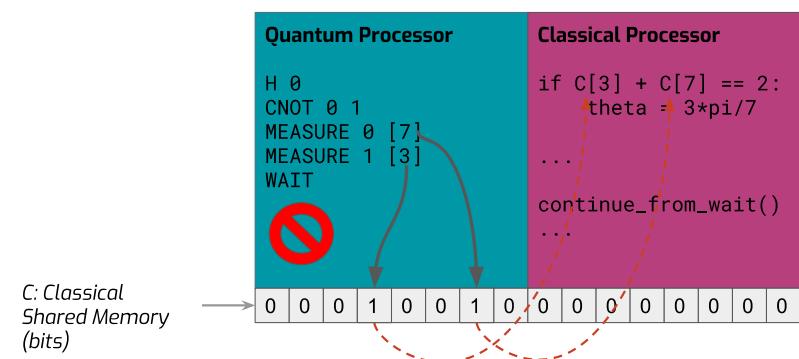
Next comes high level quantum source code which is in fact a kind of macro-assembler, able to take advantage of function libraries with ready-to-use algorithms (quantum Fourier transforms, phase estimates, etc.) and finally, high-level languages or libraries tailored to specific business needs.

In the lower layers between machine language and macro-assembler are functions for converting quantum gates into a set of universal quantum gates supported by the quantum hardware as well as error correction code systems that may require the execution of a large number of quantum gates.

A quantum compiler also implements many optimizations by for example removing quantum gate sequences that do not change the state of a qubit, such as two consecutive Hadamard or X (NOT) gates. It also arranges them to minimize the number of quantum gate steps in the solution. Quantum software architectures are generally hybrid. They manage side by side the execution of classical and quantum code, as shown in this diagram from Rigetti<sup>1103</sup>.

## Interacting with a Classical Computer

- > The Quantum Abstract Machine has a **shared classical state**.
- > The QAM becomes a practical device with this shared state.
- > Classical computers can take over with classical/quantum synchronization.



At the very least, the classical computer is used to control the execution of quantum algorithms, if only to trigger the quantum gates at the right time, sequentially.

<sup>1102</sup> I created this chart based on an equivalent chart I discovered back in 2018, but I lost its source in the meantime.

<sup>1103</sup> Source: [Quantum Cloud Computing](#) by Johannes Otterbach, January 2018 (105 slides).

# Development tool classes

We can identify some major classes of tools for creating quantum software: graphic programming tools, scripting languages, intermediate languages, machine languages, compilers and application libraries.

## Graphical programming tools

They allow to visually define the sequence of quantum gates to create algorithms and execute it on quantum accelerators.

These tools can also emulate, run and visualize the status of qubits when their number is reasonable with various methods: Bloch sphere, register state and density matrix.

One example of such tools is the [IBM Q Experience](#) IBM Composer that is available online since 2016. Code can be executed on an IBM emulator or on one of the many IBM quantum systems available in the cloud, and for free up to 15 operational qubits.

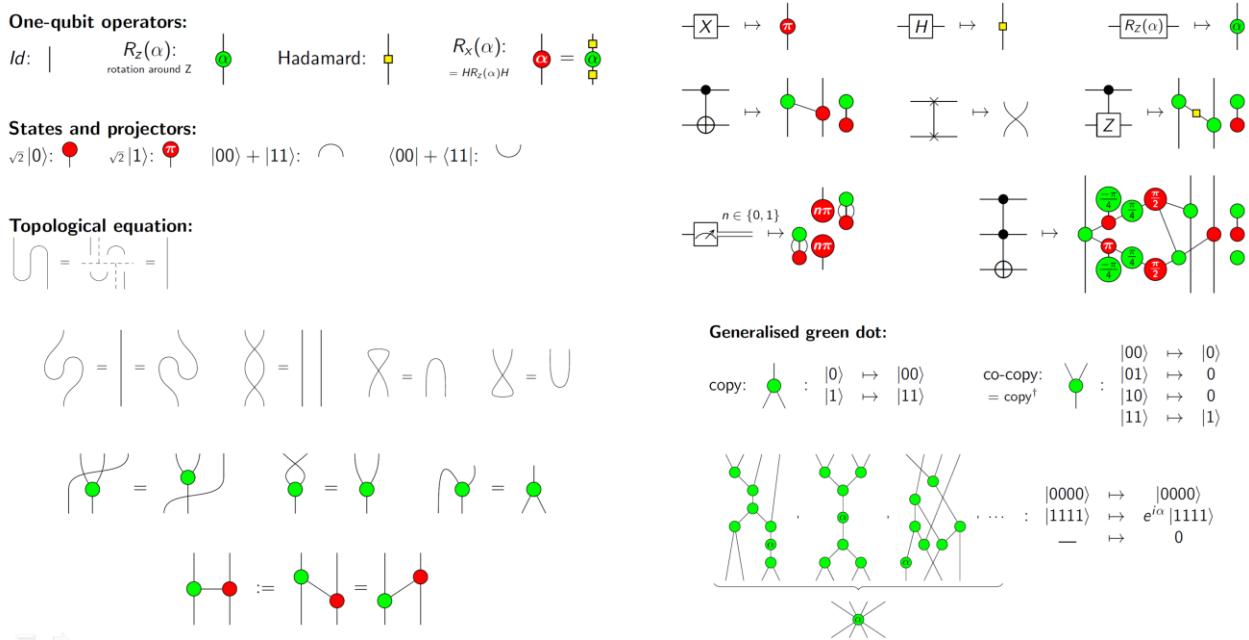
There are also graphical simulators of qubits that can be used to understand how to chain quantum gates on a few qubits and visualize the result visually. The most open one is the open-source tool [Quirk](#) which can simulate up to 16 qubits. It works online and can be downloaded to run on your own computer locally. Below is an [example](#) of a quantum Fourier transform performed in Quirk. It was developed by [Craig Gidney](#), a Google engineer.



Finally, let's pay some attention to **ZX-calculus**, a graphical programming language that uses topological composition rules. It was created in 2008 by Bob Coecke and Ross Duncan<sup>1104</sup>. It visualizes the modifications made to a set of qubits and is based on transformations applicable to the geometric representation of quantum gates that simplify models.

<sup>1104</sup> See [Interacting Quantum Observables: Categorical Algebra and Diagrammatics](#) by Bob Coecke and Ross Duncan, 2009 (80 pages).

It is particularly useful for programming a quantum computer in MBQC (measurement base quantum computing) and for visually model error correction codes. It can also help optimize quantum code compiling<sup>1105</sup>.



ZX has its own zoo of extensions:

- **PyZX** is a Python tool created in 2019 that implements ZX-Calculus principles for the creation, visualization, and automated rewriting of large-scale quantum circuits.
- **SZC-calculus** (Scalable ZX-calculus) is a high-level extension of ZX-calculus for the design and verification of quantum computations with qubits registers. Among other things, it can be used to describe graph states used in MBQC and error correcting codes<sup>1106</sup>.
- **ZXH-calculus** is a graphical language based on ZX-calculus helps modelize many-body states<sup>1107</sup>.
- **ZW-calculus** is a variant that allows better entanglement modeling and **ZH-calculus** is used for the generalization of MBQC programming models thanks to the addition of a box implementing the Hadamard gate and an easier integration of Toffoli gates in its diagrams. It is associated with a development tool, **Quantomatic**, created by Aleks Kissinger and Vladimir Zamazhiev of Oxford University<sup>1108</sup>. Contributors to the ZX-Calculus work include researchers from Loria under the responsibility of Simon Perdrix, a research laboratory located in Nancy and Dominic Horsman from the UGA LIG in Grenoble<sup>1109</sup>. They organize their own international conference, the **QPL** (Quantum Physics and Logic) but it covers broader topics than ZX calculus.

<sup>1105</sup> See [Effective Compression of Quantum Braided Circuits Aided by ZX-Calculus](#) by Michael Hank et al, November 2020 (13 pages).

<sup>1106</sup> See [SZX-calculus: Scalable Graphical Quantum Reasoning](#) by Titouan Carette, Dominic Horsman and Simon Perdrix, April 2019 (29 pages).

<sup>1107</sup> See [AKLT-states as ZX-diagrams: diagrammatic reasoning for quantum states](#) by Richard D. P. East et al, December 2020 (22 pages).

<sup>1108</sup> See [Quantomatic: A Proof Assistant for Diagrammatic Reasoning](#), 2015 (11 pages).

<sup>1109</sup> See [Completeness of the ZX-Calculus](#) by Renaud Vilmart, 2018 (123 slides) which is the source of the illustrations and [Completeness of the ZX-Calculus](#) by Emmanuel Jeandel, Simon Perdrix and Renaud Vilmart (73 pages) which explains them.

## Scripting languages

They are used to program a quantum algorithm in text mode. These tools allow to associate classical programming with the chaining of quantum functions conditioned by the state of variables in classical memory.

There are two main types of quantum scripting languages: imperative and functional languages:

- **Imperative languages** are procedural programming languages where step-by-step algorithms are described. They include the usual languages such as C, C++, PHP or Java.
- **Functional languages** are used by defining various functions that are called on an ad-hoc basis by the program. The loops (for, while) are replaced by recursive functions and there are no modifiable variables. It uses high-level abstract data types that are manipulated by functions. It creates more concise code.

Table 1: A selection of some quantum programming languages.

Name	Style	Notes
QCL	Imperative	Has classical sublanguage, multiple high-level programming features.
qGCL	Imperative	Emphasis on algorithm derivation and verification.
LanQ	Imperative	Full operational semantics, proven type soundness.
Quipper	Functional	Focus on scalability, plans to include linear types for static checks (currently done at run-time).
QPL	Functional	Statically typed, denotational semantics in terms of CPOs of superoperators.
QML	Functional	Linearly typed, focused on weakening - not contraction. Quantum control and quantum data.
Qumin	Functional	Two sublanguages (untyped and linearly typed). Focus on ease of use and clean, functional style of programming.

table source: [Qumin, a minimalist quantum programming language](#), 2017 (34 pages).

Many traditional programming languages can be used for imperative or functional programming, especially if they use function pointers or support event-driven logic. To some extent, JavaScript and jQuery can be used as functional languages via their call-back functions. This is also the case with C++.

With quantum computer vendors such as IBM or Rigetti, two types of languages are sometimes offered: an intermediate language (Quil at Rigetti, openQASM with IBM) and a higher-level language in the form of extensions to the Python programming language (pyQuil at Rigetti, IBM Qiskit). A conversion tool converts the second one into the first one.

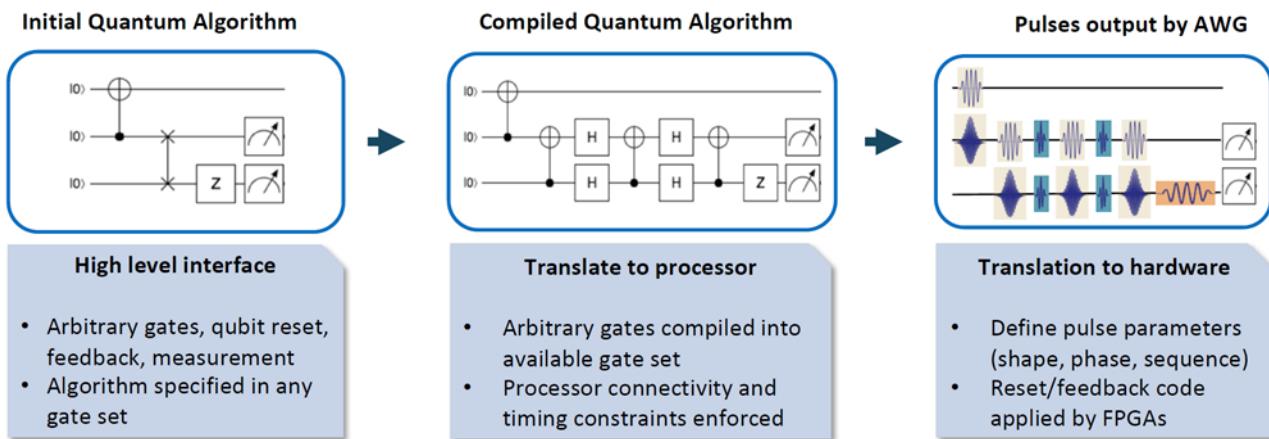
The most common programming language used with quantum libraries is Python. It provides language constructs, data types, for-loops code branching, modularity and classes. It can help build repetitive code structures, which would be harder than with graphical circuit design. It can also be used to create automatic testing tools.

## Machine languages

These are the lowest level programming languages of the quantum computer, which program the initialization of qubits and drive the physical signals sent to the qubits to implement universal gates and qubit readouts. They are generally specific to each type of quantum computer, or even to each quantum computer. Most quantum algorithms developers never use this type of low-level language.

## Compilers

Compilers quantum translate your code into the low-level sequences of qubit electronic controls for the target quantum accelerator expressed in a sort of machine language. It can also integrate quantum error correction codes (QEC). These compilers transform the program gates into universal physical gates operated by the quantum computer and then into control pulses of the qubits<sup>1110</sup>.



It will also compute the gates activation times and verify that the accumulation of these activation times is within the range of the target accelerator's qubits coherence time. Compilers can also carry out optimizations specific to certain types of algorithms<sup>1111</sup>.

Like Atos' aQASM, these compilation tools can be cross-platform and support different gate-based quantum computer architectures. Quantum programming languages are generally able to combine classical procedural programming with quantum registers and gates programming. They allow parallel management of classical memory with quantum registers.

All these programming tools come from either research labs or from quantum computer vendors such as IBM, Rigetti and D-Wave<sup>1112</sup>.

## Emulators

Emulators, usually wrongly labelled simulators which is confusing them with quantum simulators which are quantum systems, are software and/or hardware tools that emulate the execution of quantum algorithms on classical computers. Their qubit emulation capacity is closely related to the amount of memory available and the emulation mode that is implemented<sup>1113</sup>.

Let's look first at software emulation. On a laptop with 16 GB of memory, one can simulate about 20 qubits. Specialized appliances such as Atos' QLM are designed to manage a very large amount of memory, allowing the emulation of up to 40 qubits. These machines and the related software are also able to emulate specific physical characteristics of qubits (noise, T<sub>1</sub>, T<sub>2</sub>, ...). More than 40 qubits can be emulated on massively parallel architectures.

<sup>1110</sup> Source of the diagram: [How about quantum computing?](#) by Bert de Jong, June 2019 (47 slides).

<sup>1111</sup> This is the case of [Partial Compilation of Variational Algorithms for Noisy Intermediate-Scale Quantum Machines](#) by Pranav Gokhale et al, 2019 (13 pages) which deals with a two-pass compiler optimized for Variational Algorithms (VQE). See also [Spacetime tradeoffs when optimizing large quantum computations](#) by Craig Gidney (Google AI Quantum, USA), IQFA 2020, December 2020 (60mn) and [slides](#). He is turning serialized circuits into parallelized ones. With T state distillation, he gains three orders of magnitude in fidelities.

<sup>1112</sup> See this presentation which describes some of the tasks performed by quantum compilers: [Opportunities and Challenges in Intermediate-Scale Quantum Computing](#) by Fred Chong, 2018 (34 slides).

<sup>1113</sup> See the list of quantum algorithm simulation tools at <https://quantiki.org/wiki/list-qc-simulators>.

On the software side, many emulation tools are available<sup>1114</sup> such as **Quirk** running in your browser and **Quantum Circuit Simulator** running under Android. **SimulaQron** from QuTech can run on their **Quantum Inspire** platform running two quantum processors using 2 and 5 superconducting qubits and two simulators supporting 26 and 31 qubits. **Intel** also created its own emulator, qHiPSTER, in 2016<sup>1115</sup>.

**Qode** is a free online tool used to edit a quantum circuit and to generate the associated code for Q#, Qiskit, QASM and Cirq environments. It integrates advanced features such as predefined codes and expression entry ([site](#)). The simulated code can then feed the cloud quantum services.

## JÜLICH QUANTUM COMPUTER SIMULATOR (JUQCS)



JUQUEEN, Jülich, Germany



K, Kobe, Japan

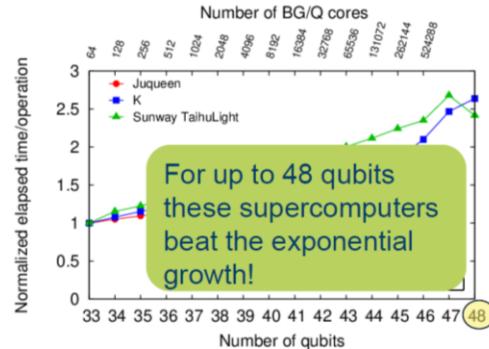


Sunway TaihuLight, Wuxi, China

- $N$  qubits  $\rightarrow |\psi\rangle$  is a superposition of  $2^N$  basis states
- Represent a quantum state with 2 bytes  $\rightarrow N$  qubits requires at least  $2^{N+1}$  bytes of memory  $\rightarrow$  new world record in 2018

N	Memory
27	256 MB
39	1 TB
48	0.5 PB
49*	1 PB

\* Could be run on Trinity, Los Alamos



For up to 48 qubits  
these supercomputers  
beat the exponential  
growth!

Member of the Helmholtz Association

29 March 2018

Page 11

Kristel Michielsen



The main limitations of supercomputers for emulating quantum algorithms are more related to their memory (RAM) than to their processing capacity. It would take 16 Po of memory to fully simulate 50 qubits. How about 96 qubits? The memory requirement would be multiplied by  $2^{46}*2$ . Moore's law of memory cannot therefore keep pace with a linear increase in the number of aligned qubits in a quantum computer.

Nevertheless, the number of emulated qubits on supercomputers is still constantly increasing. The Chinese have been the most active in this emulation race, particularly at Alibaba and Huawei, with several records set in 2018.

There are three main methods for simulating a circuit of  $N$  qubits and a certain level of depth of quantum gate sequences which will resonate with what we've learned about register computational basis and density matrices<sup>1116</sup>:

<sup>1114</sup> See this long [list of emulators](#).

<sup>1115</sup> qHiPSTER stands for quantum High Performance Software Testing Environment. See [qHiPSTER: The Quantum High Performance Software Testing Environment](#) by Mikhail Smelyanskiy et al, 2016 (9 pages).

<sup>1116</sup> See [Classical Simulation of Intermediate-Size Quantum Circuits](#), Alibaba, 2018 (12 pages). See also [What limits the simulation of quantum computers?](#) by Yiqing Zhou, Miles Stoudenmire and Xavier Waintal, March 2020 (14 pages) which provides a theoretical and practical framework for the optimization of quantum code emulation. Noteworthy is the work on the emulation of superconducting qubit modules with ... superconducting qubits. See [Quantum computer-aided design: digital quantum simulation of quantum processors](#) by Thi Ha Kyaw et al, 2020 (23 pages).

- Managing the complete **quantum state vector** Hilbert space in memory with  $2^N$  complex numbers representing  $2^{N+1}$  floating point numbers and  $2^{N+5}$  since double precision floating point numbers occupy 16 bytes. The action of quantum gates on this large vector consists in applying to it the quantum gates unitary matrices to one, two or three qubits which are respectively made of  $2 \times 2$ ,  $4 \times 4$  or  $8 \times 8$  complex numbers. This method is implemented on supercomputers with huge memory capacities of the order of several Petabytes. The method is currently limited to about 50 qubits. It can be optimized since these vectors are generally filled with many zeros.
- Managing these quantum state vector amplitudes without the phase, with  $2^N$  real numbers and thus  $2^{N+4}$  bytes. The method is easier to distribute over several servers<sup>1117</sup>. Alibaba used a cluster of 10,000 servers with 96 CPUs. In September 2019, they simulated 70 qubits over a depth of 34 quantum gates with 1449 instances of their Cloud Elastic Computing Service (ECS), each comprising 88 Intel Xeon chipsets with 160 GB of memory. So, a total of 127,512 processors!<sup>1118</sup>
- The third and more demanding one consists in managing the whole **density matrix** of the qubits register containing  $2^{2N}$  real numbers. It is the most memory-hungry method and is not frequently used with a large numbers of qubits. It can be necessary if you need to emulate imperfect qubits with their noise and decoherence and their impact on quantum algorithm's execution.

On top of this exist many compression methods with a lower accuracy<sup>1119</sup>.

**Google**'s emulator qsim can simulate 30 qubits on a laptop and up to 40 qubits in Google Cloud.

**Origin Quantum**, a Chinese multi-role (hardware, software) startup in partnership with the Guang-Can Guo team from the **University of Science and Technology of China**, simulated 64 qubits with a 22-depth algorithm on a cluster of 128 nodes<sup>1120</sup>. They used a method to transform combinations of CZ gates (conditional Pauli Z gates) and single-qubit gates into simpler sub-circuits that do not need to be interleaved. They also thought they could simulate 72 qubits over a depth of 23 gates on a supercomputer running for 16 hours.

This work shows that two key parameters condition the emulation capabilities in classical computers: not only the number of qubits but also the number of quantum gate sequences. The larger the number of qubits emulated, the fewer quantum gate sequences we can simulate.

A second record coming from **Alibaba** was achieved with 81 qubits and 40 quantum gate sequences<sup>1121</sup>. Their Taizhang simulation exploited a method created by Igor Markov and Shi Yaoyun in 2005 that allows a quantum algorithm to be distributed over a farm of thousands of servers<sup>1122</sup>. The Alibaba Quantum Laboratory is managed by the same Shi Yaoyun, a professor at the University of Michigan. Their simulations included 100 qubits over 35 layers ( $10 \times 10 \times 35$ ), 121 qubits over 31 layers ( $11 \times 11 \times 31$ ) and 144 qubits over 27 layers ( $12 \times 12 \times 27$ ). The chosen architectures are those of qubit density matrices, hence the square numbers of qubits.

<sup>1117</sup> Partitioning methods for quantum simulation are well described in [Distributed Memory Techniques for Classical Simulation of Quantum Circuits](#), Ryan LaRose of the University of Michigan, June 2018 (11 pages).

<sup>1118</sup> See [Alibaba Cloud Quantum Development Platform: Large-Scale Classical Simulation of Quantum Circuits](#), September 2019 (5 pages).

<sup>1119</sup> See [Full-State Quantum Circuit Simulation by Using Data Compression](#) by Xin-Chuan Wu et al, 2020 (29 slides).

<sup>1120</sup> See [Researchers successfully simulate a 64-qubit circuit](#), Science China Press, June 2018.

<sup>1121</sup> See [Alibaba Says Its New "Tai Zhang" Is the World's Most Powerful Quantum Circuit Simulator](#), May 2018 et [Alibaba announced that it has developed the world's strongest quantum circuit simulator "Taizhang"](#), May 2018.

<sup>1122</sup> See [Simulating quantum computation by contracting tensor networks](#) by Igor Markov et Shi Yaoyun, 2005 (21 pages).

Reference	General Technique	Qubits	Depth	# of Amplitudes
Intel [6]	Full amplitude-vector update	42	High	All
ETH [5]	Optimized full amplitude-vector update	$5 \times 9$	25	All
IBM [7]	Tensor-slicing with minimized communication	$7 \times 7$ $7 \times 8$	27 23	All $2^{37}$ out of $2^{56}$
Google [8]	Preprocessing using undirected graphical model	$7 \times 8$	30	1
USTC [9]	Qubit partition with partial vector update	$8 \times 9$	22	1
Sunway [10]	Dynamic programming qubit partition	$7 \times 7$ $7 \times 7$	39 55	All 1
Alibaba	Undirected graphical model with parallelization	$9 \times 9$	40	1

TABLE I: A very broad overview of existing simulators. The final column reports the number of amplitudes that are computed by that simulator.

The third record in 2018 came from **Huawei** and its "HiQ Cloud" service, capable of emulating 42 to 169 qubits<sup>1123</sup>. The method was similar to the one used by **Alibaba**. The 42 qubits were simulated in "full amplitude" mode. 81 qubits were simulated with "a single amplitude" and 169 qubits with a single amplitude and a small number of quantum gates.

Other records have been broken in the USA, such as **Google's** record with NASA, the University of Illinois and the Oak Ridge laboratory with 49 to 121 qubits on the IBM Summit<sup>1124</sup>.

IBM broke a record of 56 qubits emulation in 2017 on a classic supercomputer of their own, the Vulcan BlueGene installed at the Lawrence Livermore National Laboratory in California. The same Oak Ridge laboratory is at the origin of **XAAC** (eXtreme-scale ACCelerator programming framework), a framework for Eclipse that manages hybrid calculations combining quantum computers and supercomputers such as the Titan equipped with Nvidia GPUs installed in Oak Ridge<sup>1125</sup>. It can transform quantum code for computers with quantum gates or adiabatic models into executable code on any quantum architecture.

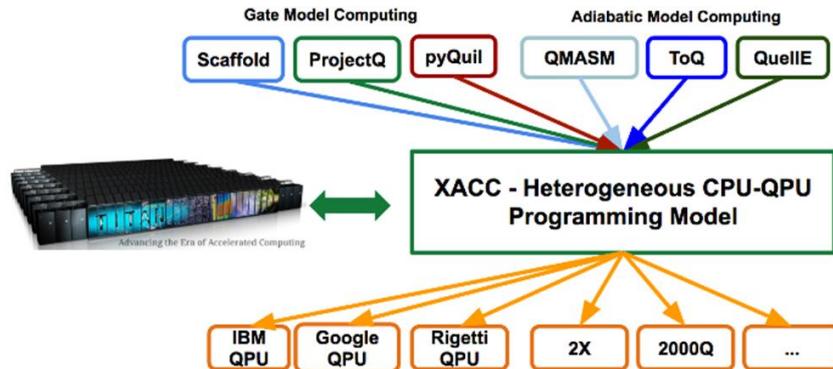


Figure 1: The XACC CPU-QPU programming model enables quantum acceleration in classical HPC applications in a quantum language and hardware agnostic manner.



**Atos** (France) developed a quantum emulator on Intel-based servers, the [Atos Quantum Learning Machine](#) (QLM). Launched in September 2017, the QLM quantum emulator is a classic computer.

It's been adopted by the US DoE's Oak Ridge research center, by the CEA, at the University of Reims, at the cybersecurity research department of the University of Applied Sciences of Upper

<sup>1123</sup> See [Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform](#), October 2018.

<sup>1124</sup> See [Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation](#), May 2019 (11 pages). This Summit must have consumed a good part of the production of Nvidia V100! Here is also the list of qubit and qubit simulation records in <https://quantumcomputingreport.com/scorecards/qubit-count/>.

<sup>1125</sup> The diagram comes from [Eclipse Science and Open Source Software for Quantum Computing](#), 2017. See the article describing XAAC: [A Language and Hardware Independent Approach to Quantum-Classical Computing](#), July 2018 (15 pages).

Austria in Hagenberg, by the Hartree Science and Technology Facility Centre (STFC) in the UK, at the C-DAC (Centre for Development of Advanced Computing) in India, in its Quantum Computing Experience Center<sup>1126</sup>, in Japan, in Finland to the CSC IT Center for Science Kvasi in collaboration with the startup IQM, and in the new Quantum Integration Centre (QIC) from LRZ (Leibniz Supercomputing Centre) of the Bavarian Academy of Sciences and in Spain (CESGA).

Atos is also working with Total to develop quantum solutions to identify new materials and molecules in the energy transition. They rely on Atos' [Center of Excellence in Parallel Programming](#) (CEPP), which is located at the GENCI computing center in Orsay, France.

In June 2020, Atos launched the QLM E, a new version of this emulator integrating from 2 to 32 Nvidia V100 GPUs, and multiplying computing power by 12 compared to the initial version which was equipped only with Intel CPUs. This system was first delivered in December 2020 to the Irish HPC center (ICHEC). This was completed in early July 2020 with the support of a limited form of quantum annealing emulation.

### Some Atos QLM customers



6

In May 2019, Atos launched myQLM, a quantum programming tools for researchers, students and developers. It is a Python-based development environment that allows users to simulate quantum programs on their own computer. Programming is carried out in AQASM (Atos Quantum Assembly Language) and pyAQSM. To access a number of qubits that exceeds the current capacity of PCs, i.e. more than 20 qubits, developers can run their code on an Atos Quantum Learning Machine simulator in the cloud, but at a charge. Atos plans to enable the sharing of quantum practices, libraries and application codes. Atos also offers one of the open-source translators of myQLM code to other quantum programming environments. In September 2020, this software offer became free of charge<sup>1127</sup>.

In July 2020, Atos launched the **Scaler** Acceleration Program, aimed at start-ups and SMEs to enable them to adopt high-power computing and quantum code emulation technologies. This also covers security and decarbonation solutions.

Atos also announced in 2020 that they would launch a NISQ quantum accelerator by 2023. They are looking at several tracks such as superconductors (with IQM), trapped ions (with the University of Innsbruck), cold atoms (with Pasqal) and in the longer-term silicon qubits (with CEA-Leti). They participate in the European Flagship projects **AQTION** (quantum accelerator) and **PASQuanS** (analog quantum simulator).

Atos is also heavily involved in the EuroHPC project, which includes the **European Processor Initiative**, an initiative to develop a processor adapted to the needs of supercomputers and on-board as well as autonomous vehicles<sup>1128</sup>.

<sup>1126</sup> See [Atos and C-DAC sign a cooperation agreement to accelerate the development of quantum and exascale computing and Artificial Intelligence in India](#), August 2019.

<sup>1127</sup> See [Atos roadmap in The Atos Quantum Program - Paving the way to quantum-accelerated HPC](#) by Jean-Pierre Panziera, June 2021 (10 slides).

<sup>1128</sup> In July 2018, Atos also acquired Syntel for \$3.4B in the USA, a \$923M service provider specializing in the development and deployment of applications in the cloud with 22,500 employees, created in 1980 by Indo-Americans. This does not seem to have anything to do with quantum.



**Nvidia** (USA) announced in April 2021 the future release of the cuQuantum SDK running on top of their GPGPU A100 and V100. It implements gates-based programming emulation at the density matrix level.

Thanks to the GPGPU tensors implementing matrix multiplications and fast HBM2E memory, the acceleration provided is clear, making it possible to emulate Google Sycamore processor with a depth of 20 gates in less than 10 minutes<sup>1129</sup>. It is to be supported by various cloud offerings from JUQCS-G (Julich), Qgate (NVAITC), Qiskit-AER (IBM), QuEST (Oxford), SV1 (Amazon Web Services) and Vulcan (QC Ware). As of May 2021, it however was not yet available. One question will be whether this SDK allows some processing parallelization across multiple GPGPU and DGX servers and support large memory capacities in the multi-TB range like Atos QLMs.

Many other IT players want to jump on the quantum emulation bandwagon. It was the case with **Dell** which announced its hybrid solution combining classical computing and quantum emulation using its Dell EMC PowerEdge R740xd server appliance and IBM's Qiskit Runtime.

## Research-originated quantum development tools

Here is an overview of the main quantum languages created to date, starting with languages that are independent of hardware architectures and that often originate from research laboratories.

They have the disadvantage that they are not generally linked to cloud quantum computer offerings. The related researchers are the equivalents of the Kernighan and Richie (creators of the C language) and Bjarne Stroustrup (creator of C++) in the quantum realm! A good number of these languages come from Europe.

- **QCL** or Quantum Computation Language has a syntax and data types close to those of the C language. This language is one of the first for quantum programming, created in 1998 by the Austrian researcher **Bernhard Ömer** from the Austrian Institute of Technology in Vienna. It is described in [Structured Quantum Programming](#), 2009 (130 pages) which positions very well the conceptual differences between classical and quantum programming languages.

Classical concept	Quantum analogue
classical machine model variables variable assignments classical input	hybrid quantum architecture quantum registers elementary gates quantum measurement
subroutines argument and return types local variables dynamic memory	operators quantum data types scratch registers scratch space management
boolean expressions conditional execution selection conditional loops	quantum conditions conditional operators quantum if-statement quantum forking

Table 2.1: *Classical and quantum programming concepts*

- **Q Language** is an extension of the C++ language that provides classes for programming quantum gates (Hadamard, CNOT, SWAP, QFT for quantum Fourier transform)<sup>1130</sup>.
- **QFC** and **QPL** are two functional languages defined by Peter Selinger, from Canada, the first one using a graphical syntax and the second one using a textual syntax<sup>1131</sup>.
- **QML** is a functional programming language created by Thorsten Altenkirch and Jonathan Grattage (UK)<sup>1132</sup>.

<sup>1129</sup> See [What Is Quantum Computing?](#) by Dion Harris, April 2021 and [Nvidia entangled in quantum simulators](#) by Nicole Hemsoth, April 2021.

<sup>1130</sup> It is documented in [Toward an architecture for quantum programming](#), 2003 (23 pages), with as co-author, Stefano Bettelli from the Laboratory of Quantum Physics of the Paul Sabatier University of Toulouse.

<sup>1131</sup> They are described in [Towards a Quantum Programming Language](#), 2003 (56 pages).

<sup>1132</sup> See [A functional quantum programming language](#), 2004 (15 pages). The principles are well described in the presentation [Functional Quantum Programming](#), (151 slides).

- **qGCL** or Quantum Guarded Command Language was created by Paolo Zuliani of the University of Newcastle<sup>1133</sup>.
- **ProjectQ** is a scripting language from ETH Zurich that takes the form of an open-source Python framework, released on GitHub since 2016. It includes a compiler that converts quantum code into C++ language for execution in a quantum simulator with a traditional processor<sup>1134</sup>. Launched in early 2017, it supports IBM's quantum computers via their OpenQASM language, which is normal since ETH Zurich is a partner of the latter, as well as simulation on a traditional computer via a C++ implementation that supports up to 28 qubits. ProjectQ is compatible with OpenFermion from Rigetti and Google.

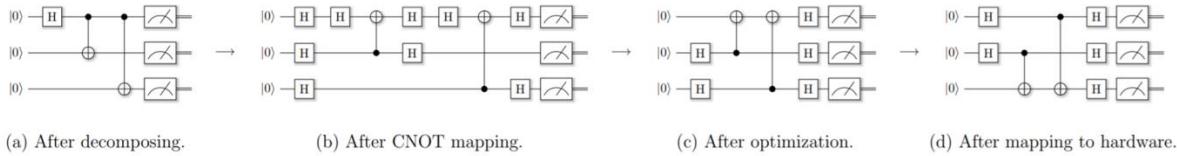
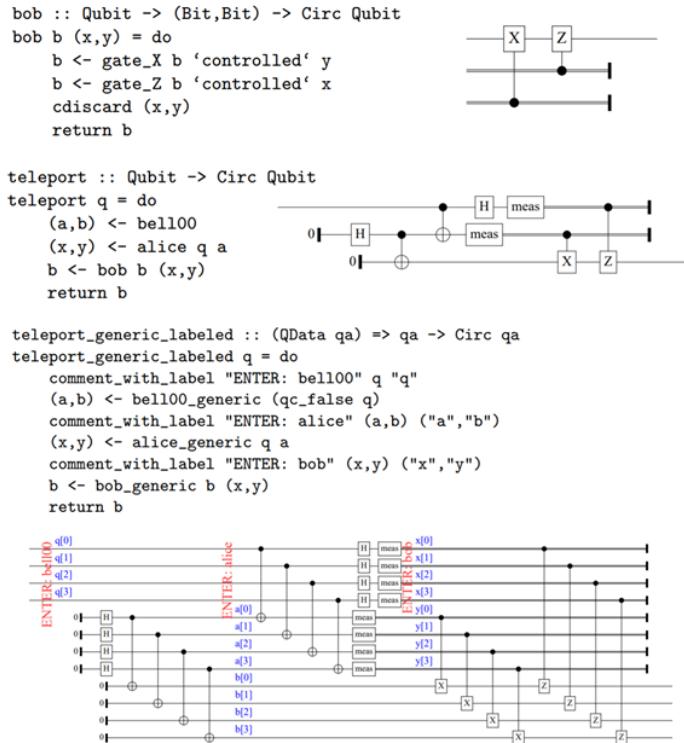


Figure 5: Individual stages of compiling an entangling operation for the IBM back-end. The high-level Entangle-gate is decomposed into its definition (Hadamard gate on the first qubit, followed by a sequence of controlled NOT gates on all other qubits). Then, the CNOT gates are remapped to satisfy the logical constraint that controlled NOT gates are allowed to act on one qubit only, followed by optimizing and mapping the circuit to the actual hardware.

- **Quipper** is a language created in 2013 that builds on the classic **Haskell** language, created in 1990, to which it provides extensions in the form of data types and function libraries<sup>1135</sup>. It manipulates a software version of qRAM, an addressable quantum memory register, that is essential for the execution of algorithms such as Grover and QMLs. The language does not seem to have evolved since 2016. One of its creators is Benoît Valiron who teaches quantum programming at Centrale-Supelec in France<sup>1136</sup>.
- **QWire** is another quantum programming language close to Quipper, launched in 2018, from the University of Pennsylvania<sup>1137</sup>. It is associated with a formal proof solution.



<sup>1133</sup> See [Compiling quantum programs](#), 2005 (39 pages).

<sup>1134</sup> See [ProjectQ: An Open Source Software Framework for Quantum Computing](#) by Damian Steiger, Thomas Häner and Matthias Troyer, 2018 (13 pages) which explains how the compiler optimizes the code according to the gates available in the quantum computer.

<sup>1135</sup> It is documented in [An Introduction to Quantum Programming in Quipper](#), 2013 (15 pages). Its creation was funded by IARPA.

<sup>1136</sup> See his presentation [Programming a Quantum Computer](#), 2017 (38 slides) and [Quantum Computation Model and Programming Paradigm](#), 2018 (67 slides).

<sup>1137</sup> See [QWIRE: A Core Language for Quantum Circuits](#) (13 pages) and [A core language for quantum circuits](#) by Jennifer Paykin et al, 2017 (97 slides).

- **Qubiter** is an open-source language developed in Python that can be used on top of IBM's OpenQASM and Google's OpenFermion. It was created in 2017.
- **Scaffold** is a language developed at Princeton University<sup>1138</sup>. It is used to program traditional code which is then automatically transformed into quantum gates via its C2QG (Classical code to Quantum Gates) function. In particular, Scaffold can generate QASM. It can be interesting to develop oracles for search algorithms.

Here is a sample code, almost easy to understand! Its development was also funded by IARPA.

```
// Pauli X, Pauli Y, Pauli Z, Hadamard, S, and T gates
gate X(qreg input[1]);
gate Y(qreg input[1]);
gate Z(qreg input[1]);
gate H(qreg input[1]);
gate S(qreg input[1]);
gate T(qreg input[1]);

// Daggered gates
gate Tdag(qreg input[1]);
gate Sdag(qreg input[1]);

// CNOT gate defined on two 1-qubit registers
gate CNOT(qreg target[1], qreg control[1]);

// Toffoli (CCNOT) gate
gate Toffoli(qreg target[1], qreg control1[1], qreg control2[1]);

// Rotation gates
gate Rz(qreg target[1], float angle);           //Arbitrary Rotation

// Controlled rotation
gate controlledRz(qreg target[1], qubit control[1], float angle);

// One-qubit measurement gates
gate measZ(qreg input[1], bit data);
gate measX(qreg input[1], bit data);

//One-qubit prepare gates: initializes to 0
gate prepZ(qreg input[1]);
gate prepX(qreg input[1]);

//Fredkin (controlled swap) gate
gate fredkin(qreg targ[1], qreg control1[1], qreg control2[1])
```

- **Qumin** is a minimalist quantum language designed in Greece in 2017. It is available in open-source<sup>1139</sup>.
- **QuEST (Quantum Exact Simulation Toolkit)** is a quantum emulator developed in C language and supporting QUDA APIs (not CUDA) and Nvidia's GPUs, created by Oxford University researchers and distributed in open-source. The system can simulate 26 to 45 qubits depending on the available memory, respectively 2 GB and 256 GB. It also dates from 2017.
- **Q.js** is a graphical quantum emulator launched in 2019, running in JavaScript and thus running in a browser<sup>1140</sup>.
- **QuTiP (Quantum Toolbox in Python)** is another open-source quantum code simulation tool developed by Paul Nation of IBM, Robert Johansson of Rakuten and Franco Nori of RIKEN (Japan) and the University of Michigan. The project started in 2011. It targets superconducting qubits.
- **QNET** is a language from Stanford University created in 2012, which allows to simulate the operation of quantum networks.
- Quantum implementation languages of **lambda calculus**, conceptualized by Alonzo Church and Stephen Cole Kleene during the 1930s, followed. This type of computation makes it possible to solve very complex and NP-complete problems, the class of problems that can be verified in polynomial time and whose resolution requires exponential time on classical computers and potentially polynomial time on quantum computers<sup>1141</sup>!

---

<sup>1138</sup> See [Scaffold: Quantum Programming Language](#), 2012 (43 pages).

<sup>1139</sup> See [Qumin, a minimalist quantum programming language](#), 2017 (34 pages).

<sup>1140</sup> See [Quantum Programming: JavaScript \(Q.js\) - a drag and drop circuit editor](#) by Stewart, 2020. And <https://quantumjavascript.app/>.

<sup>1141</sup> See [A lambda calculus for quantum computation with classical control](#) by Peter Selinger and Benoît Valiron, 2004 (15 pages).

- **OpenQL** is an open-source quantum programming language created by TU Delft in 2020. It includes a high-level quantum programming language, its associated quantum compiler and a low-level assembly language, cQASM<sup>1142</sup>.
- **eQASM** is an intermediate quantum machine language from Delft University and its subsidiary QuTech. It sits in between high-level programming tools (QASM) and the quantum accelerator. It is a compiled language, hence the "e" for executable. The compiler manages the dependencies with hardware implementation specifics. Tests have been carried out with a 7-qubit superconducting chipset<sup>1143</sup>.

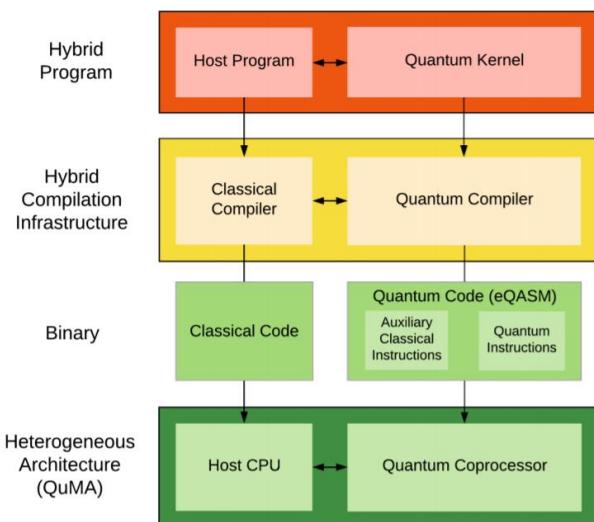


Fig. 1. Heterogeneous quantum programming and compilation model.

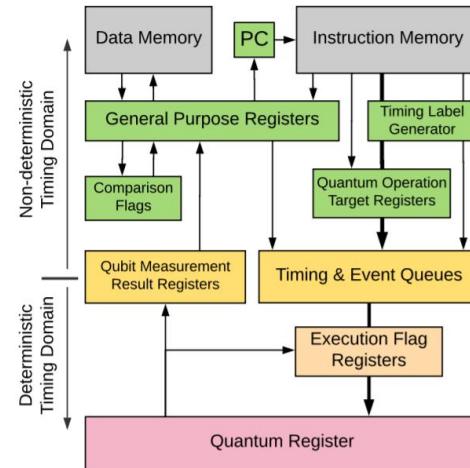


Fig. 2. Architectural state of eQASM. Arrows indicates the possible information flow. The thick arrows represent quantum operations, which read information from the modules passed through.

- Researchers at the University of Chicago's Enabling Practical-scale Quantum Computation (**EPiQC**) laboratory proposed a compiler that can improve the speed and reliability of quantum computers by a factor of 10. Here again, the compiler has to adapt to the underlying hardware architecture<sup>1144</sup>. Their [video](#) explains the process. The team used Google's TensorFlow library to optimize the physical control parameters of the qubits.
- **Silq** is a concise and static quantum programming language proposed by a team from ETH Zurich<sup>1145</sup>.
- **Yao.jl** is a package for the Julia language used for creating quantum circuits.

As already mentioned, a good majority of software tools for quantum programming are open-source. [Open-source software in quantum computing](#), by Mark Fingerhuth, Thomas Babej and Peter Wittek, December 2018 (28 pages), makes a detailed inventory of these different tools and gauges them against classical open-source software features like source code documentation. It shows that differentiation is mainly concentrated on documentation and tutorials. In practice, few commercial application developers use the languages discussed in this section. Instead, they are hooked to the languages and toolkits provided by commercial quantum computer vendors listed afterwards. They are easily locked into "full stack" approaches that are proprietary in practice.

<sup>1142</sup> See [OpenQL : A Portable Quantum Programming Framework for Quantum Accelerators](#) by N. Khammassi et al, 2020 (13 pages).

<sup>1143</sup> See [eQASM: An Executable Quantum Instruction Set Architecture](#), March 2019 (14 pages).

<sup>1144</sup> See [Research provides speed boost to quantum computers](#), April 2019.

<sup>1145</sup> See [Swiss scientists launch high-level quantum computing language](#) by ETH Zurich, June 2020.

The most interesting thing about all this is that many development tools allow us to get our hands on small-scale quantum algorithms before "big" quantum computers are available. It's up to you if you feel like it! And most of them are open-source<sup>1146</sup>.

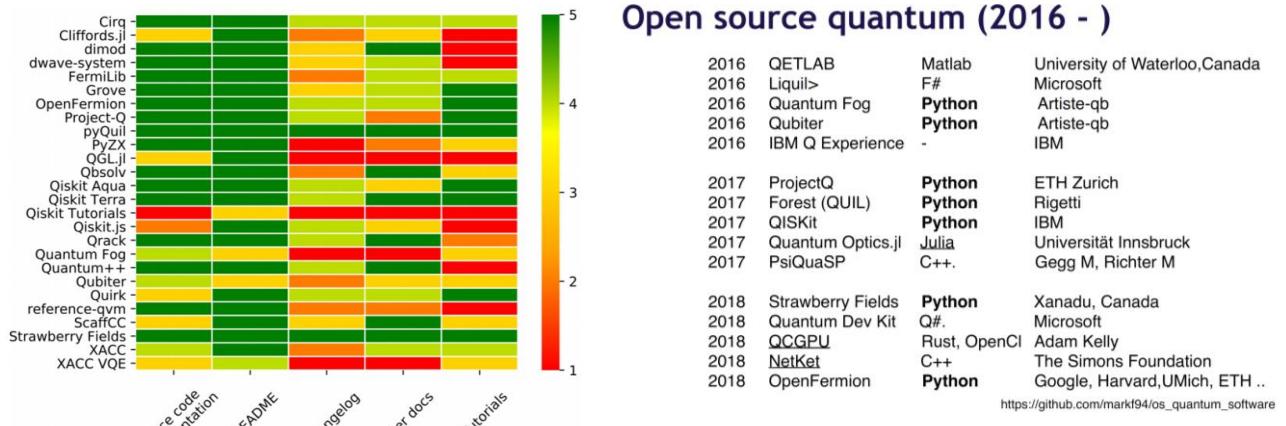


Fig 4. Heatmap of documentation analysis results. The heatmap shows the evaluation results for source code documentation, README files, changelogs, user documentation and tutorials on a scale from 1 (bad) to 5 (good). The evaluation rubrik used for scoring can be found in [S1 Table](#). Data was obtained in August 2018.

Year	Language	Reference(s)	Semantics	Host Language	Paradigm
1996	Quantum Lambda Calculi	[181]	Denotational	lambda Calculus	Functional
1998	QCL	[206–209]		C	Imperative
2000	qGCL	[241, 312–314]	Operational	Pascal	Imperative
2003	$\lambda_q$	[282, 283]	Operational	Lambda Calculus	Functional
2003	Q language	[32, 33]		C++	Imperative
2004	QFC (QPL)	[245–247]	Denotational	Flowchart syntax (Textual syntax)	Functional
2005	QPAlg	[141, 160]		Process calculus	Other
2005	QML	[10, 11, 113]	Denotational	Syntax similar to Haskell	Functional
2004	CQP	[102–104]	Operational	Process calculus	Other
2005	cQPL	[180]	Denotational		Functional
2006	LanQ	[188–191]	Operational	C	Imperative
2008	NDQJava	[298]		Java	Imperative
2009	Cove	[227]		C#	Imperative
2011	QuECT	[48]		Java	Circuit
2012	Scaffold	[1, 138]		C (C++)	Imperative
2013	QuaFL	[162]		Haskell	Functional
2013	Quipper	[114, 115]	Operational	Haskell	Functional
2013	Chisel-Q	[175]		Scala	Imperative, functional
2014	LIQUI >	[292]	Denotational	F#	Functional
2015	Proto-Quipper	[234, 237]		Haskell	Functional
2016	QASM	[212]		Assembly language	Imperative
2016	FJQuantum	[82]		Feather-weight Java	Imperative
2016	ProjectQ	[122, 266, 272]		Python	Imperative, functional
2016	pyQuil (Quil)	[259]		Python	Imperative
2017	Forest	[61, 259]		Python	Declarative
2017	OpenQASM	[66]		Assembly language	Imperative
2017	qPCF	[213, 215]		Lambda calculus	Functional
2017	QWIRE	[217]		Coq proof assistant	Circuit
2017	cQASM	[146]		Assembly language	Imperative
2017	Qiskit	[4, 232]		Python	Imperative, functional
2018	IQu	[214]		Idealized Algol	Imperative
2018	Strawberry Fields	[147, 148]		Python	Imperative, functional
2018	Blackbird	[147, 148]		Python	Imperative, functional
2018	QuantumOptics.jl	[157]		Julia	Imperative
2018	Cirq	[271]		Python	Imperative, functional
2018	Q#	[269]		C#	Imperative
2018	Q SI>	[174]		.Net language	Imperative
2020	Silq	[35]		Python	Imperative, functional

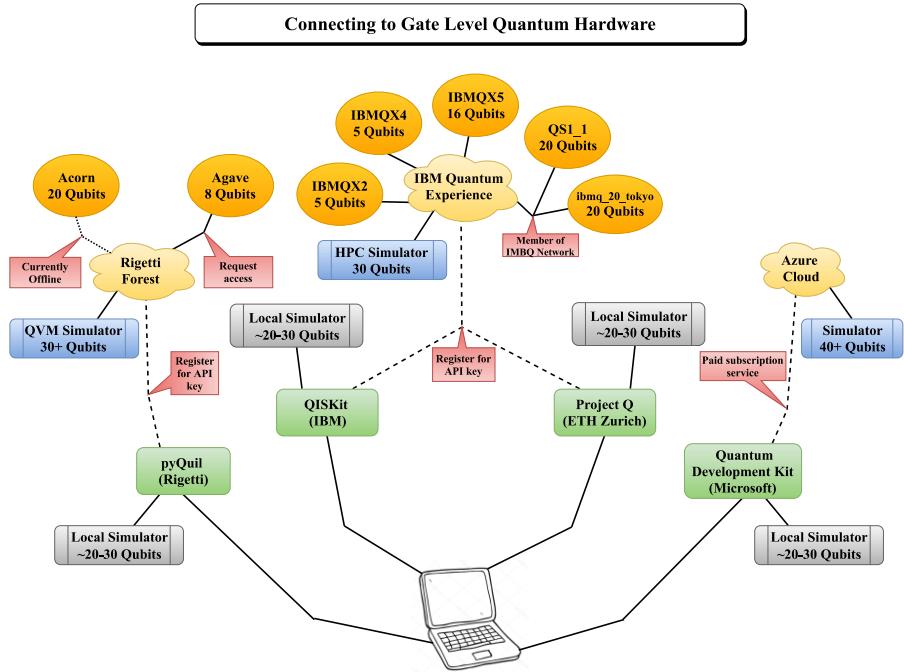
<sup>1146</sup> See on this subject the [presentations](#) of FOSDEM 2019 conference.

<sup>1147</sup> Source: [Quantum Software Engineering Landscapes and Horizons](#) by Jianjun Zhao, 2020 (31 pages) which provides an excellent overview of development tools covering the entire quantum software creation cycle, including the thorny issues of debugging and testing.

# Quantum vendors development tools

Even before general-purpose quantum computers are operational on an exploitable scale, the software platforms battle has already begun. The major quantum computing players have almost all adopted an end-to-end vertical integration approach from quantum processors to development tools. This is particularly the case at IBM, Microsoft, Rigetti and D-Wave. This is well illustrated in the chart *below*, which also describes the main development environments for quantum applications from Rigetti and IBM<sup>1148</sup>.

The vertical offering of the above-mentioned vendors often integrates a low-level quantum language, then a higher-level language similar to the macro-assembler of traditional computers, then an open-sourced framework that can be most often used in Python with ready-to-use functions, a development environment, possibly a quantum gates graphical coding tool, and often some access to their cloud based quantum accelerators and simulators.



One remaining tool to invent would be a higher level of abstraction tool to free developers from understanding the intricacies of quantum gates and interferences. Most recent supposed “higher level” languages are classical gate-based programming tools.

Here is another consolidation of these proprietary - although also open-sourced - quantum software development platforms<sup>1149</sup>.

When all software tools are open-source, it's not anymore a differentiating factor, or it is when you look at the fine prints. Is the open-source software controlled by the vendor or by an independent third party?

Are all software tools really open-sourced or just the lower layers with additional proprietary layers? Who are the main contributors to the open-source tool? What is the exact open-source license used?

<sup>1148</sup> Schematic discovered in [Overview and Comparison of Gate Level Quantum Software Platforms](#) by Ryan LaRose, March 2019 (24 pages).

<sup>1149</sup> I was notably inspired by the schema integrated in the article [Quantum Computing languages landscape](#) by Alba Cervera-Lierta of the Quantum World Association, September 2018. I completed it and added a column with Atos.

Q Experience	Forest			Quantum Playground	Visual Studio		
visual programming and integrated development environments							
thematic quantum libraries (chemistry, finance, machine learning, ...)	QisKit Aqua	OpenFermion	Quadrant, Qsage, ToQ	PENNY LANE	OpenFermion	Quantum Chemistry PNNL	PENNY LANE
generic quantum libraries / full-stack	QisKit	Grove QAOA	QUBO qbsolv	STRAWBERRY FIELDS	Cirq	Quantum Developer Kit	Braket SDK
high level machine language (quantum circuits)	QisKit Terra	pyquil	QMASM			Q#	
low level machine language	Open QASM	quil	QMI	Blackbird	many machine languages		D-Wave rigetti
qubits and quantum gates	super-conducting	super-conducting	quantum annealing	photons	super-conducting	topologic, IonQ, Quantinuum	IONQ OQC
							any

schema inspired from Alba Cervera-Lierta for the QWA 2018, updated in 2021  
[https://medium.com/@quantum\\_wa/quantum-computing-languages-landscape-1bc6dedb2a35](https://medium.com/@quantum_wa/quantum-computing-languages-landscape-1bc6dedb2a35)

## D-Wave

D-Wave proposes a complete range of software tools that have evolved a lot since its creation<sup>1150</sup>. The latest iteration of D-Wave's software platform is called Ocean. It includes low- and high-level building blocks for the development of quantum applications<sup>1151</sup>.

The lowest level language is **QMI**, a kind of machine language for defining the links between the qubits to prepare the related Hamiltonian for an Ising model. QMI is usable from C, C++ Python and even Matlab, via the SAPI (Solver API) interface.

Above QMI is a higher level of abstraction tool, **qbsolv**, an open-source library launched in 2017. It allows you to solve optimization problems by converting a QUBO (Quadratic Unconstrained Binary Optimization) problem into an Ising model ready to be processed by a D-Wave or even a classical computer.

Developers can also use the open-source **QMASM** (Quantum Macro Assembler) language, which is a low-level language suitable for programming on a D-Wave annealer. It is a third-party tool coming from a D-Wave partner. Like qbsolv, QMASM is used to describe a Hamiltonian made of coupler-based qubit relationships. This method has a drawback: it is preferable to initialize the system in a state close to the search solution and this state can only be determined by classical calculations.

It is in any case a very different programming model from the universal quantum gate model, even if there is a theoretical equivalence between quantum annealing and gate-based models as we saw in the [previous section](#).

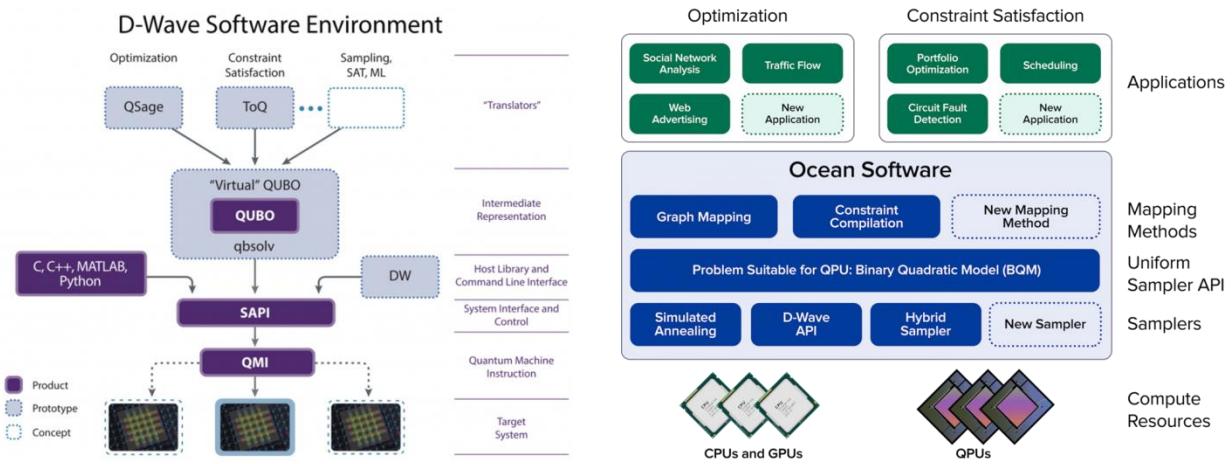
QMASM is also part of **Quadrant**, a comprehensive platform for the development of D-Wave's cloud-based solutions for machine learning launched by D-Wave in 2018<sup>1152</sup>.

The D-Wave Ocean SDK also includes **Hybrid**, an open-source framework for creating hybrid algorithms.

<sup>1150</sup> The source for the diagram on the left is [D-Wave Initiates Open Quantum Software Environment](#), January 2017. And the one on the right is from: <https://www.dwavesys.com/software>.

<sup>1151</sup> D-Wave provides a very good document describing the problems that can be solved with their computers: [D-Wave Problem - Solving Handbook](#), October 2018 (114 pages).

<sup>1152</sup> See [D-Wave Announces Quadrant Machine Learning Business Unit](#), May 2018.



We can add third party tools such as **Qsage**, an optimization problems framework and **ToQ**, another framework for solving constraint satisfaction problems, as well as the SDK from **1Qbit**.

As of spring 2021, D-Wave, its partners and customers had prototyped over 250 algorithms and solutions. They have not necessarily generated any definite quantum advantage, but they do allow customers to learn quantum programming.

D-Wave's offering is mainly offered as a cloud-based resource, under the name **Leap**.

Leap V2 was launched in February 2020<sup>1153</sup>.

It includes a new hybrid solver service that can handle - optimization problems with up to 10,000 variables and a new interactive development environment using Python.

Prices range from \$335 to \$3000 per month for access to 10 to 90 minutes of quantum computing time.

Tier 1	Tier 2	Tier 3
<b>\$335</b> US / MONTH + TAXES (US AND CANADIAN PRICING)	<b>\$1000</b> US / MONTH + TAXES (US AND CANADIAN PRICING)	<b>\$3000</b> US / MONTH + TAXES (US AND CANADIAN PRICING)
QPU and hybrid solvers use your subscription at different rates. <ul style="list-style-type: none"> <li>Up to 10 minutes of direct access to D-Wave QPUs</li> <li>Up to 200 minutes of access to hybrid solvers</li> <li>Community and email support</li> <li>No obligation to open source</li> </ul>	QPU and hybrid solvers use your subscription at different rates. <ul style="list-style-type: none"> <li>Up to 30 minutes of direct access to D-Wave QPUs</li> <li>Up to 600 minutes of access to hybrid solvers</li> <li>Community and email support</li> <li>No obligation to open source</li> </ul>	QPU and hybrid solvers use your subscription at different rates. <ul style="list-style-type: none"> <li>Up to 90 minutes of direct access to D-Wave QPUs</li> <li>Up to 1800 minutes of access to hybrid solvers</li> <li>Community and email support</li> <li>No obligation to open source</li> </ul>
<a href="#">ADD TO CART</a> <ul style="list-style-type: none"> <li>• QPU usage at \$2000/hour</li> <li>• Hybrid solver usage at \$100/hour</li> <li>• 4-month commitment*</li> </ul>	<a href="#">ADD TO CART</a> <ul style="list-style-type: none"> <li>• QPU usage at \$2000/hour</li> <li>• Hybrid solver usage at \$100/hour</li> <li>• 4-month commitment*</li> </ul>	<a href="#">ADD TO CART</a> <ul style="list-style-type: none"> <li>• QPU usage at \$2000/hour</li> <li>• Hybrid solver usage at \$100/hour</li> <li>• 4-month commitment*</li> </ul>

## IBM

IBM's quantum software development platform includes **OpenQASM**, a programming language that complements its online graphical programming tool Q Experience, currently in its third version (V3). OpenQASM includes a dozen commands<sup>1154</sup>.

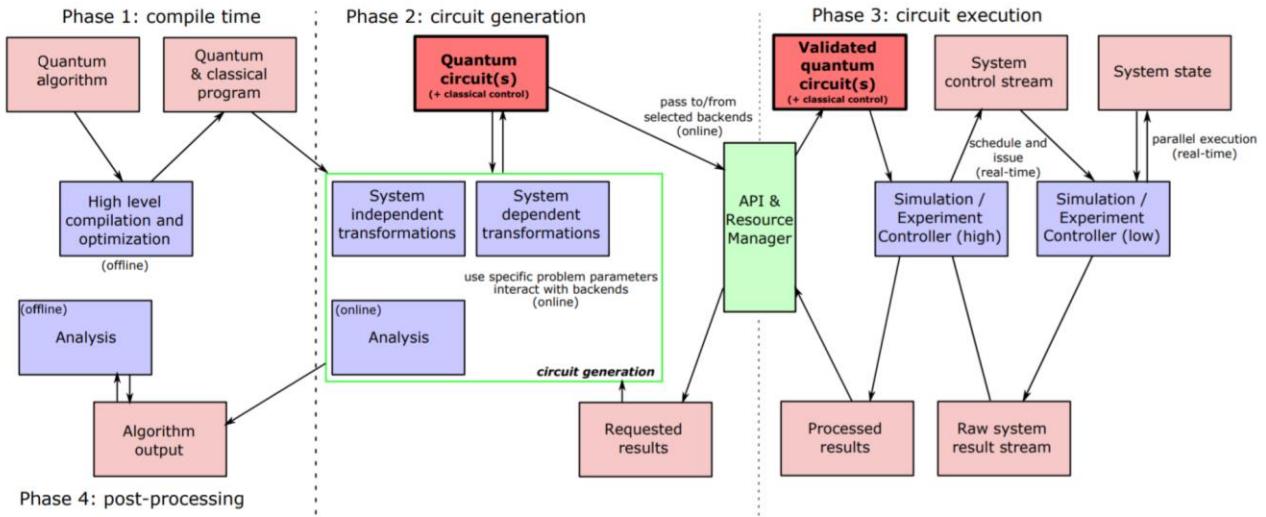
**Qiskit** is a high-level scripting library associated with OpenQASM. It can be used in Python, JavaScript and Swift (a general-purpose language from Apple) and on Windows, Linux and MacOS. It was launched in early 2017 and is published in open-source<sup>1155</sup>.

<sup>1153</sup> See [D-Wave announces Leap2, its cloud service for quantum computing applications](#) by Emil Protalinski, February 2020.

<sup>1154</sup> It is specified in [Open Quantum Assembly Language](#), 2017 (24 pages), this document describing the many tasks performed by the associated compiler.

<sup>1155</sup> The slide above that describes Qiskit comes from the presentation [Quantum Computing is Here Powered by Open Source](#), 2018 (41 slides, [video](#)).

Qiskit comes with numerous templates and sample codes to exploit a wide range of known quantum algorithms. It includes a graphical circuit-drawer function that generates a graphical visualization of programmed quantum circuits using the open-source document composition language LaTeX. Qiskit is supported or will be supported by other quantum computers vendors such as **IonQ** (USA) and **AQT** (Austria), both with trapped ions qubits, and **ColdQuanta** (USA) with cold-atoms.



**Figure 1:** Block diagrams of processes (blue) and abstractions (red) to transform and execute a quantum algorithm. The emphasized quantum circuit abstraction is the main focus of this document. The API and Resource Manager (green) represents the gateway to backend processes for circuit execution. Dashed vertical lines separate offline, online, and real-time processes.

Four software building blocks are provided in Qiskit, the first and fourth being the most common ones:

- **Qiskit Terra** provides the main compositional elements of its quantum algorithm. It also contains quantum algorithms for various applications such as chemical simulation, machine learning and finance which previously belonged to Qiskit Aqua, a library whose support was formally deprecated in April 2021 but with most of its components merged into Terra. One example of the available features is a library function to launch the Grover with one line of code, given you also need to code your oracle separately:

```
CLASSGrover(oracle, good_state=None, state_preparation=None, iterations=1,
sample_from_iterations=False, post_processing=None, grover_operator=None,
quantum_instance=None, init_state=None, incremental=False,
num_iterations=None, lam=None, rotation_counts=None, mct_mode=None)
```

- **Qiskit Aer** provides a C++ simulator to simulate qubits on classical hardware.
- **Qiskit Ignis** is a framework to analyze noise in quantum circuits and to better manage it.
- **Qiskit Aqua** which contains vertical use cases libraries, like for finance and chemical simulation.

The compilation of the quantum code then takes place to run the simulation either on IBM's classic cloud-based HPC simulator or on a single-virtual-quantum computer such as those from IBM that are also available in the cloud such as Tenerife and Yorktown (5 qubits) and Melbourne (14 qubits), followed by 28 and 65 qubit versions launched in 2020.

**IBM Quantum Composer** allows you to program your code graphically online and run it on a quantum simulator or on the many IBM quantum systems available online. The tool allows to interact indifferently with the text code on the left or with its graphical representation on the right. It can show registers vectors after running the code.

**QISKit—programming real quantum computers**

- In addition to using a visual Composer on the site, there are open dev kits available for the IBM Quantum Experience Chip
- QISKit <https://github.com/QISKit> Python SDK allows:
  - Building of quantum circuits that represent a problem
  - Compiling to run on different backends (simulators/real chips of different quantum volumes)
  - Running the jobs
- ProjectQ lets users also simulate quantum programs on classical computers, emulating at a higher level of abstraction

BT RSAConference2018

**IBM Q Experience**

New Save Clear Help Untitled Experiment Result 5d3c33c... Unsaved changes Run →

Circuit editor

```
1 OPENQASM 2.0;
2 include "qelib1.inc";
3 gate n60 ( param ) q {
4   h q;
5 }
6
7 qreg q[5];
8 creg c[5];
9
10 x q[0];
11 h q[0];
12 h q[1];
13 h q[2];
14 h q[3];
15 h q[4];
16 measure q[0] -> c[0];
17 measure q[1] -> c[1];
18 measure q[2] -> c[2];
19 measure q[3] -> c[3];
20 measure q[4] -> c[4];
```

Circuit composer

Gates

Operations Subroutines

Gates overview Barrier

The simulator emulates up to 32 qubits and responds much faster than quantum computers, at least with a few qubits. You can execute your code once or 1024, 4096 and 8192 times to get an average of the results.

Since the batches are submitted one after the other, one can wait up a long long time, more than one hour for your code to be executed. The creation of an account is free and you can use up to 15 physical qubits for free<sup>1156</sup>.

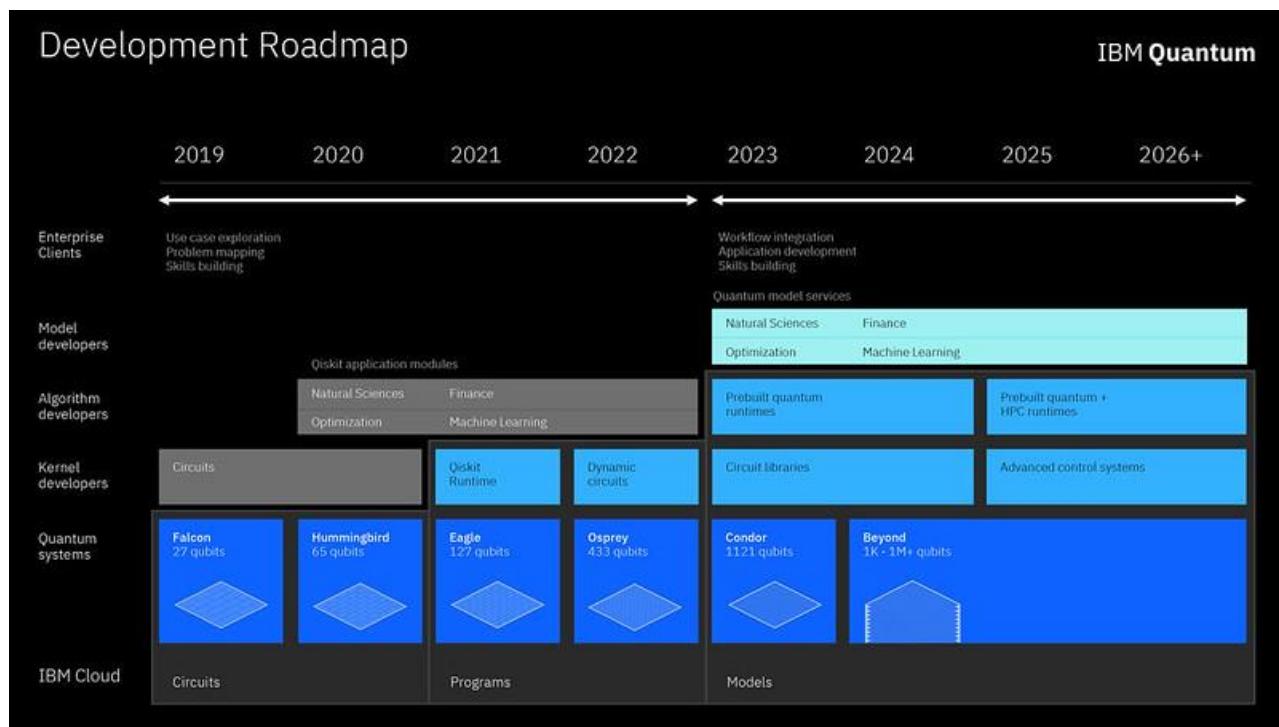
IBM also offers the **Hello Quantum** mobile application for programming code with a few qubits.

In February 2021, IBM complemented its hardware roadmap announced in September 2020 with a five years software roadmap<sup>1157</sup>. Its main item was Qiskit runtime, a quantum software execution environment that is supposed to increase by 100x the workloads speed working in batch mode in the cloud when they run circuits execution iteratively (in the end, it was a 120x improvement). It's optimizing the way workloads are loaded in the classical computers driving quantum processors.

<sup>1156</sup> There's a legal caveat in the tool terms of use: "*You may not use IBM Q in any application or situation where failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage, such as aircraft, motor vehicles or mass transport, nuclear or chemical facilities, life support or medical equipment, or weaponry systems*". Given that with the few qubits offered, you can wonder how you could risk doing any of these nasty things.

<sup>1157</sup> See [IBM's roadmap for building an open quantum software ecosystem](#) by Karl Wehden, Ismael Faro and Jay Gambetta, February 2021.

The rest of the announcement covered the willingness to address vertical markets with partners. They plan to package off-the-shelf libraries for natural science, optimization, machine learning, and finance with partners like **Strangeworks**.



At last, IBM launched in March 2021 a certification program and test for Qiskit developers based on 60-question exam working on the Pearson VUE electronic testing solution<sup>1158</sup>. This is a typical tactic used when building developer communities and practiced for a long time by the likes of Novell (CNEs) and Microsoft (MCPs).

## Rigetti

Rigetti proposes an integrated software development platform with the low-level language **Quil** that supports a mixed classical and quantum memory model<sup>1159</sup>. It runs on Windows, Linux and MacOS. The language uses the gates class to describe operations to be performed on qubits, indexed from 0 to n-1, for n qubits and with quantum gates.

The language allows you to create conditional programming based on the qubits state. It is completed by the open-source library **pyQuil** launched in 2017 which includes the Grove library of basic quantum algorithms ([documentation](#)).

It can be used with the Python programming language. The high level pyQuil (assembler) generates the low-level Quil language (machine code).

## pyQuil generates Quil

```
from pyquil.gates import X, CNOT, H, Z, RX
from pyquil.api import QVMConnection
from pyquil.quil import Program
import numpy as np

qvm = QVMConnection()

alice_register = 0
ancilla_register = 1

flip_correction_branch = Program(X(1))
phase_correction_branch = Program(Z(1))

prog = (Program()
        .inst(H[0])
        .inst(CNOT[0, 1])
        .inst(RX(.2 * np.pi, 2))
        .inst(CNOT[2, 0])
        .inst(H[2])
        .measure[0, alice_register]
        .measure[2, ancilla_register]
        .if_then(alice_register, flip_correction_branch)
        .if_then(ancilla_register, phase_correction_branch))

qvm.run_and_measure(prog, list(prog.get_qubits()), trials=10)

H 0
CNOT 0 1
RX(pi/5) 2
CNOT 2 0
H 2
MEASURE 0 [0]
MEASURE 2 [1]
JUMP-WHEN @THEN1 [0]
JUMP @END2
LABEL @THEN1
X 1
LABEL @END2
JUMP-WHEN @THEN2 [1]
JUMP @END6
LABEL @THEN5
Z 1
LABEL @END6
```

<sup>1158</sup> See [IBM offers quantum industry's first developer certification](#) by Abe Asfaw, Kallie Ferguson, and James Weaver, IBM, March 2021.

<sup>1159</sup> It is documented in [A Practical Quantum Instruction Set Architecture](#), 2017 (15 pages).

Here is a simple example with a single qubit activated by a Hadamard gate that creates an overlay of state 0 and 1 to create a truly random number generator. Used iteratively in a classical loop, the program can generate a random series of 0 and 1 with a 50% chance of having either one allowing to create a completely random single binary code.

```

1 # random number generator circuit in pyQuil
2 from pyquil.quil import Program
3 import pyquil.gates as gates
4 from pyquil import api
5
6 qprog = Program()
7 qprog += [gates.H(0),          • Hadamard gate on qubit 1
8           gates.MEASURE(0, 0)] • qubit readout on superposed state
9
10 qvm = api.QVMConnection()   • readout output
11 print(qvm.run(qprog))

```



**Listing 2:** pyQuil code for a random number generator.

Rigetti offers the execution of quantum programs in its cloud systems and on conventional simulators via its QVMs, for **Quantum Virtual Machines**<sup>1160</sup>. Since 2020, it's also available on Amazon Braket cloud services. It is usable from the **Forest** development environment proposed by Rigetti. These tools are open-source, but not cross-platform.

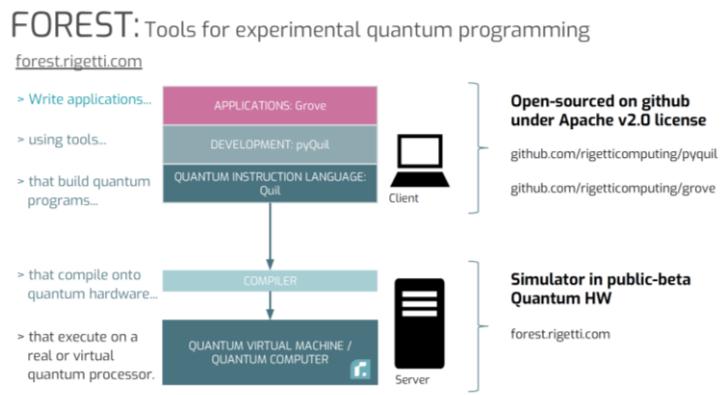
At the end of 2017, Google and Rigetti launched the open-source initiative **OpenFermion**.

This framework developed in Python exploits research work from the Universities of Delft and Leiden in the Netherlands. It is a software solution for the creation of quantum algorithms for the simulation of chemical functions supporting any quantum computer, from Universal Quantum Computers to D-Wave annealers.

It complements Atos<sup>1161</sup>. In 2018, Rigetti finally launched a Quantum Algorithm Contest with a \$1M prize, but with an interesting bias, comparing the creators of quantum algorithms with others seeking to create equivalents running on conventional computers.

The process could last 3 to 5 years and looks like the XPrize process<sup>1162</sup>.

At last, Rigetti is also promoting **Quantum Programming Studio**, a web based interactive programming tool that can run your code on a Rigetti quantum computer in the cloud.



<sup>1160</sup> This is documented in [pyQuil Documentation](#), June 2018 (120 pages) which contains many code examples like the one *above*.

<sup>1161</sup> See the [announcement](#) in October 2017, [OpenFermion: The Electronic Structure Package for Quantum Computers](#), 2018 (19 pages) and [Openfermion documentation](#).

<sup>1162</sup> See [Can You Make A Quantum Computer Live Up To The Hype? Then Rigetti Computing Has \\$1 Million For You](#) by Alex Knapp, Forbes, October 2018.

## Google

In addition to OpenFermion which is a high-level framework, Google launched on July 19, 2018 its own quantum framework **Cirq**, of course also in open-source. It is a Python framework.

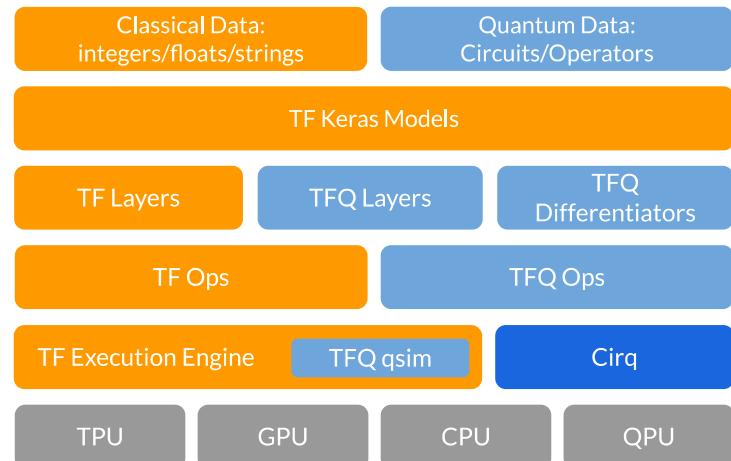
Since Google's superconducting Sycamore systems are not available on the cloud, Cirq is mainly used on a cloud simulator provided by Google<sup>1163</sup>. A tool for compiling OpenFermion code in Cirq is also proposed. It also supports IonQ trapped-ions qubits that are supported in Google Cloud since 2021. It supports also Pasqal cold-atoms systems and Rigetti superconducting qubits.

In March 2020, Google launched **TensorFlow Quantum**, an extension of the famous open-source machine and deep learning framework. It provides hybrid classical/quantum computing functions for machine learning<sup>1164</sup>. Of course, the library supports Cirq.

The screenshot shows the Google Quantum AI Software page. The navigation bar includes 'Google' and 'Quantum AI' followed by dropdown menus for 'Software', 'Hardware', 'Research', 'Education', and 'Team'. A search bar is on the right. Below the navigation, the word 'Cirq' is highlighted. The main content area has tabs for 'Overview', 'Guide', 'Tutorials' (which is underlined), 'Experiments', and 'Reference'. On the left, there's a sidebar with sections for 'IonQ hardware', 'Pasqal hardware' (with 'Getting started with Pasqal hardware' selected), 'Rigetti hardware', 'Educators workshop', and several other topics like 'Cirq intro workshop' and 'Textbook algorithms in Cirq'. The central content area displays the 'Quantum circuits on Pasqal devices' tutorial. It features a code editor with Python code for installing Cirq, and buttons to 'Run in Google Colab', 'View source on GitHub', and 'Download notebook'. There are also icons for settings and sharing.

It is adapted to quantum simulators running on classical computers based on CPUs, GPUs and TPUs (Tensor Processing Unit, the specialized AI processors running in Google's data centers).

Eventually, QPUs (Quantum Processing Units) will be supported. Why doesn't Google use its 53-qubit quantum computer? Because it is a research object and not a production tool that could be integrated at this stage in a cloud offer.



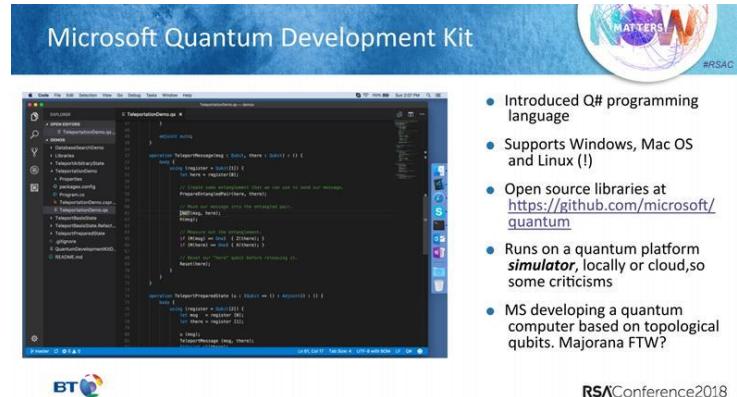
<sup>1163</sup> See explanations in [Google Cirq and the New World of Quantum Programming](#) by Jesus Rodriguez, July 2018.

<sup>1164</sup> See [TensorFlow Quantum: A Software Framework for Quantum Machine Learning](#) by M Broughton et al, 2020 (39 pages, and [associated video](#)). It is the source of the illustration.

## Microsoft

They first proposed three developers tools with the **LIQUI|>** extension of the **F#** scripting language which allows to simulate quantum programs. In December 2017 was launched **Q#**, a language particularly suitable for programming topological quantum computers, which do not yet exist, but can be simulated on conventional computers in the cloud with up to 30 qubits. Q# uses a syntax derived from Microsoft's C# language<sup>1165</sup>.

It is provided as an extension to the Visual Studio development environment and in the QDK (Quantum Development Kit). An intermediate language is generated by the compiler, QIL. It is supposed to be cross-platform. Microsoft certainly has an interest in making its development tools cross-platform to capture the attention and time of developers and for its Azure quantum cloud service.



In July 2018, Microsoft launched **Quantum Katas**, an open-source project containing examples of quantum Q# code integrated into interactive tutorials<sup>1166</sup>. They then introduced in December 2018 a chemical simulation library co-developed with Pacific Northwest National Labs, a kind of equivalent of OpenFermion, which is co-developed by Rigetti and Google<sup>1167</sup>. The library complements PNNL's NWChem quantum chemistry simulation software package. And in May 2019, Microsoft announced that it was going to make its quantum development tools open-source, so at least Q# and the Quantum Development Kit.

In September 2020, Microsoft launched **QIR** (Quantum Intermediate Representation), an intermediate representation for quantum programs, serving as a layer between gate-based quantum programming languages like Q# and target quantum computers. It's based on **LLVM** open-sourced intermediate language that was created in 2000 at the University of Illinois and now handled by the LLVM Foundation run by Tanya Lattner. It can also be used to run code on an emulator. The support is done with a compiler extension supporting that QIR with Q#. It is used by Azure Quantum to support the various hardware platforms it serves (IonQ, Honeywell, QCI). But it seems, not yet by any other vendor.

At last, let's mention a joint quantum research partnership program between Microsoft and **Inria** in France, launched in May 2021 and built upon their joint research lab created in 2005. This will lead to a couple researchers to jointly work on quantum error corrections and quantum walks algorithms<sup>1168</sup>.

<sup>1165</sup> See [Q#: Enabling scalable quantum computing and development with a high-level domain-specific language](#), 2018 (11 pages). It involves Alain Sarlette, Anthony Leverrier, Eric Fleury, Hélène Robak and Laurent Massoulié from Inria and Nicolas Delfosse from Microsoft Research.

<sup>1166</sup> See [Learn at your own pace with Microsoft Quantum Katas](#), July 2018.

<sup>1167</sup> See [Simulating nature with the new Microsoft Quantum Development Kit chemistry library](#), December 2018. PNNL is a research laboratory co-funded by the US Department of Energy and operated by the non-profit foundation Batelle Memorial Institute. Batelle operates numerous US laboratories such as Lawrence Livermore National Laboratory, Los Alamos National Laboratory and Oak Ridge National Laboratory.

<sup>1168</sup> See [Kickoff of the Quantum computing projects of the Microsoft Research-Inria joint center](#), May 2021.

## Amazon

Amazon's quantum software offering is organized in their Braket platform. It contains both a custom hardware independent development framework as well as the PennyLane framework from Xanadu, and all the tools to submit quantum code to the various AWS supported systems (IonQ, D-Wave, Rigetti and soon OQC) as well as their own classical computing emulators for testing and learning purpose.

## IonQ

Like Rigetti, IonQ also has its own "full stack" software offering adapted to their trapped ions quantum computer architecture and proposed in the cloud. It's also offered in Amazon and Microsoft's quantum cloud services.

## Intel

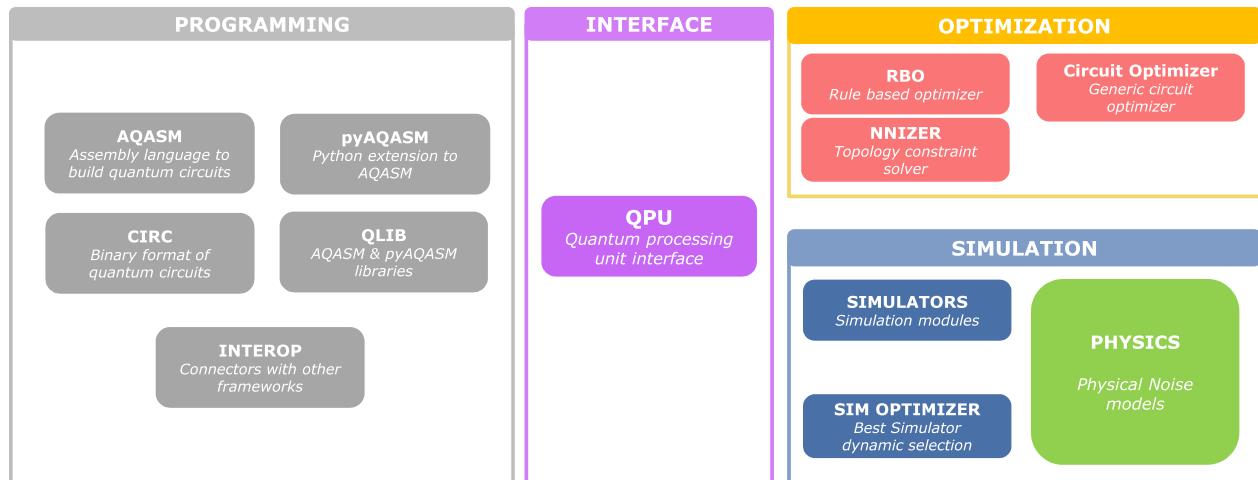
At this stage, Intel is not very advanced in the development of quantum software. They have created a quantum emulation software for classical computers<sup>1169</sup>, the first two authors working at Intel and the last one at Harvard. It can simulate up to forty qubits.

## Huawei

At the end of 2018, Huawei launched its own quantum application development framework, compatible with ProjectQ, and including a graphical interface for algorithm creation. All this is integrated into their HiQ cloud-based quantum emulation service<sup>1170</sup>. It is provided free of charge for simulating up to 38 qubits. It can also simulate up to 81 qubits with a processing depth of 30 and 169 qubits with a computing depth of 20.

## Atos

Atos is not yet a manufacturer of quantum computers. Their partnerships with various players such as Finland's IQM and France's Pasqal suggest that at some point, they will integrate hybrid solutions mixing their classical server nodes and quantum accelerators.



For the time being, they are offering a quantum software emulation solution running on Intel processor machines and with their own optimized memory architecture, QLM.

<sup>1169</sup> Documented in [qHiPSTER: The Quantum High Performance Software Testing Environment](#) by Mikhail Smelyanskiy, Nicolas Sawaya, and Alan Aspuru-Guzik, 2016 (9 pages)

<sup>1170</sup> See [Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform](#), October 2018.

They simulate 30 to 40 qubits depending on the QLM configuration and are agnostic regarding the physical qubit that are emulated. Since July 2020, they sell QLMe, a faster version of this emulator that runs Nvidia V100s GPUs.

aQASM (Atos Quantum Assembly Programming Language) is a programming language that complements Python to create quantum algorithms executable on QLM emulator or on any physical quantum computer architecture with universal gates.

The language allows to define quantum gates using other quantum gates, equivalents of objects, functions or macros in traditional programming<sup>1171</sup>.

aQASM is based on the OpenQASM standard language. It is completed by the PyAQASM Python library used to generate aQUASM files. The language helps programing the repetitive execution of looped gates and create reusable functions.

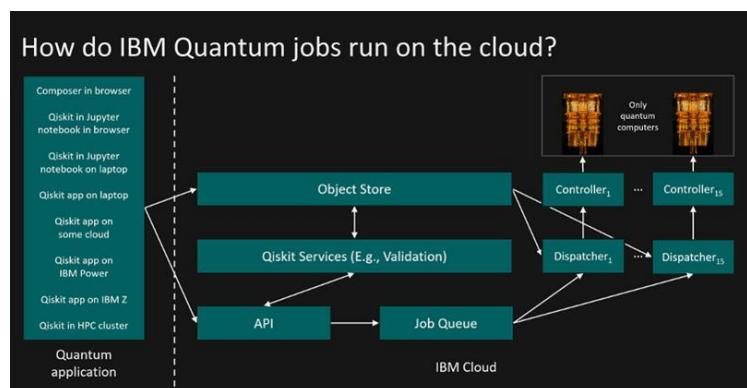
The aQASM code compiler generates CIRC binary code that is the low-level pivot language, which is then converted into the control language for specific universal quantum computers or for simulation supercomputers via the Quantum Processing Unit Interface (QPU). It is complemented by various optimization plugins that eliminates useless gates and tunes the generated low-level code for the targeted quantum accelerator hardware architecture.

## Cloud quantum computing

A large share of quantum computers is intended to be offered through cloud services. It's even got a specific name: **QCaaS** (Quantum Computing as a Service). There are various estimates for the cloud quantum computing market including an optimistic one of \$26B by 2030 by The Quantum Daily<sup>1172</sup>.

This is already the case for **D-Wave** with its Leap offer, **Rigetti** which launched its Cloud Services offer in 2019 and since July 2020, **Honeywell** with its System Model H0 which offers 6 ion-trapped qubits in the cloud and for a fee, upgraded in October 2020 to 10 qubits with their Model H1.

**IBM** proposes cloud access to over 30 quantum computers with 1 to 65 superconducting qubits as of September 2021. **Alibaba** has a similar offer in China, with fewer qubits. We are here in the context of vertically integrated offers, the operator of the cloud service being the designer of the quantum computers. A second type of offer relates to quantum emulation resources in the cloud.



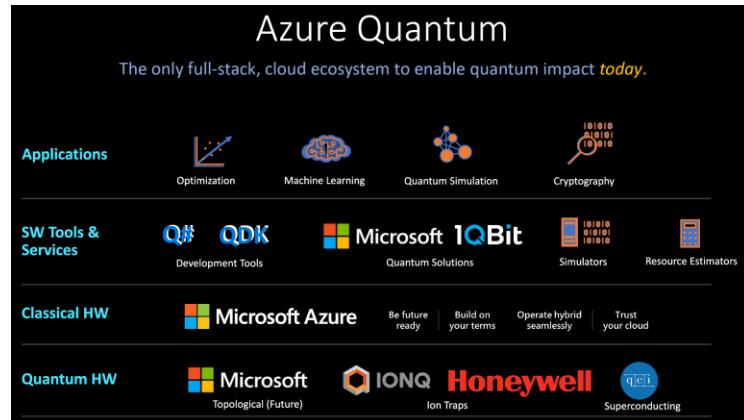
They enable quantum algorithms to be executed on conventional supercomputers or data centers with a reduced number of supported qubits. Such solutions can be found at IBM, Microsoft, Google, Alibaba, Huawei and also Atos.

<sup>1171</sup> Source of the diagram: [Atos QLM, a future-proof approach to quantum computing](#) by Christelle Piechurski, Atos, March 2018 (26 slides).

<sup>1172</sup> See [Report: Quantum Computing as a Service Market to Hit \\$26 Billion by End of Decade](#) by The Quantum Daily, August 2021 and [Quantum Computing as a Service Market Sizing - How We Did It](#) by The Quantum Daily, August 2021. These forecasts are fairly inconsistent with other [quantum computing forecasts](#) mentioned in this document, page 526, planning a total \$2B in 2030.

A final approach, launched at the end of 2019, consists of cloud operators offering access to quantum computers that they have not designed, possibly mixed with quantum emulation resources on conventional servers. This is what Amazon and Microsoft announced almost simultaneously at the end of 2019 and made available in 2020.

It is unclear whether this is related to the slow development of Majorana's fermions, but in November 2019, **Microsoft** announced that it was integrating a quantum computing offering into the Azure cloud, and relying on third-party suppliers: **IonQ**, **Honeywell** (trapped ions) and **QCI** (superconductors). As of spring 2021, only IonQ and Honeywell quantum accelerators seemed to be available online<sup>1173</sup>.



They are also associated with **1QBit** (Canada) to propose quantum software application layers<sup>1174</sup>. In particular, they promote quantum inspired algorithms that rely on traditional cloud resources, as in this case study of MRI scanner optimization at Case Western Reserve University<sup>1175</sup>. Microsoft Azure Quantum also supports Qiskit and Cirq Python-based quantum code since October 2021.

**Amazon** was appeared in the quantum cloud market at the end of 2019 with the announcement of three components: Amazon Braket cloud services, AWS Center for Quantum Computing at Caltech University<sup>1176</sup>, and Amazon Quantum Solutions Lab, a customer evangelization program reminiscent of IBM's Q initiative<sup>1177</sup>. Amazon also uses the brand Quantum Compute Cloud (QC2) for its offering. Braket provides access to quantum computers from D-Wave (the 2000Q and Advantage annealers with respectively 2048 qubits and 5000 qubits), IonQ (configuration not specified but probably their 11 qubits version), Rigetti (16Q Aspen-4 with 16 superconducting qubits and their 31 qubits Aspen-9 version) and OQC (with 8 coaxmon qubits, planned for 2022). IonQ is thus proposed by both Microsoft and Amazon. It is also adapted to the execution of hybrid algorithms associating classical and quantum computation<sup>1178</sup> as well as to the emulation of quantum algorithms on classical servers without specifying the hardware configurations used or the associated prices.

---

<sup>1173</sup> Microsoft Azure Quantum was introduced step by step: announced in December 2019, released in limited preview in May 2020 and then in public preview in February 2021.

<sup>1174</sup> See [Experience quantum impact with Azure Quantum](#), November 2019 and [Microsoft Announces Azure Quantum with Partners IonQ, Honeywell, QCI, and 1QBit](#) by Doug Finke, 2019. At the same time, Microsoft also announced that it has brought together many other quantum software partners: ProteinQure, Entropica Labs, Jij, Multiverse Computing, Qu&Co, QC Ware, OTI, Qubit Engineering, Qulab, QunaSys, Rahko, Riverlane, SolidStateAI, StrangeWorks, Xanadu, Zapata. See the list here : [Quantum Network-A community of pioneers](#) by Microsoft, 2019.

<sup>1175</sup> See [How the quest for a scalable quantum computer is helping fight cancer](#) by Jennifer Langston, July 2019.

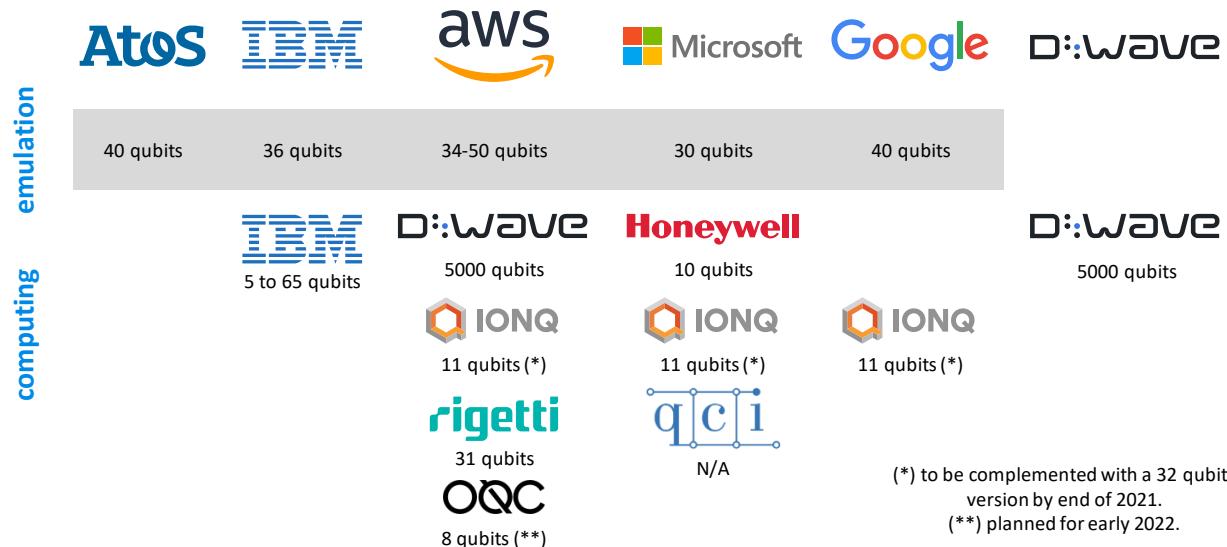
<sup>1176</sup> The AWS Center for Quantum Computing is headed by Brazilian Fernando Brandao (1983), who is both a professor at Caltech and director of this Amazon AWS laboratory. He was previously a researcher at Microsoft Research. He is a good generalist, initially a physicist and now a specialist in quantum algorithms. In June 2020, John Preskill, also a professor at Caltech, announced that he would spend one day a week at the research center.

<sup>1177</sup> See [Amazon Braket-Get Started with Quantum Computing](#) by Jeff Barr, December 2019 and the presentation of the announcement Introducing Quantum Computing with AWS by Fernando Brandao and Eric Kessler ([video](#) and [slides](#)), featuring the Eiffel Tower of Rydberg atoms from French startup Pasqal in slide 15). I discovered in the [hundreds of presentations](#) at the Amazon Reinvent conference in December 2019 where this Braket announcement took place that Amazon was also presenting the [QLDB](#), or Quantum Ledger Database, a blockchain management software brick. But that doesn't seem to have anything quantum at all.

<sup>1178</sup> See [PennyLane on Braket + Progress Toward Fault-Tolerant Quantum Computing + Tensor Network Simulator](#) by Jeff Barr, December 2020.

Amazon Braket is associated with an in-house SDK based on the classic Python language. Development is supported in the integrated open-source environment Jupyter. It also includes support for the OCL (Object Constraint Language) constraint programming language. Like Microsoft, Amazon is also a partner of quantum software publishers.

We find almost the same players with Xanadu, Zapata, Rahko, QC Ware, 1Qbit and Qsimulate. The service was operational in August 2020 for the US market.



(cc) Olivier Ezratty, December 2021

Surprisingly, Google didn't offer any access to its quantum computers in its cloud offering. It had only an emulation offering with 40 qubits. In June 2021, Google announced the integration of IonQ's 11 qubits processor in its Cloud Marketplace. IonQ becomes de-facto the most distributed solution in the cloud with Amazon, Google and Microsoft, on top of supporting IBM's Qiskit.

Above is a summary of these cloud-based quantum computing offerings, distinguishing between emulating quantum code on classical computers and executing quantum code on quantum computers.

In China, we can add **Baidu** and its Quantum Leaf cloud offering. It's provided with **Paddle Quantum**, a quantum machine learning development toolkit based on the PaddlePaddle programming language, **QCompute**, a Python-based open-source SDK and **Quanlse**, a machine-level programming tools controlling the pulse sent to emulated superconducting qubits.

## Certification and verification

The verification and certification of quantum algorithms and the results of their use is an important new topic. The factorization of integer numbers is obviously easy to verify. But when a quantum algorithm is used to simulate physical interactions such as those of atoms in molecules, it is less obvious.

Theoretical work shows that it is possible to prove polynomially that a result of a quantum algorithm is accurate<sup>1179</sup>. But, unfortunately, we cannot explain in detail the origin of the result by breaking it down.

<sup>1179</sup> See [How to Verify a Quantum Computation](#) by Anne Broadbent, 2016 (37 pages) which demonstrates that all quantum algorithm results can be verified with classical polynomial algorithms by performing several tests and encrypting the input data. See also [Verification of quantum computation: An overview of existing approaches](#) by Alexandru Gheorghiu, Theodoros Kapourniotis and Elham Kashefi, 2018 (65 pages).

Nor can we prove that the result found, however valid it may be, is the best of all if there are several good ones<sup>1180</sup>. On top of that, we must make a distinction between error corrected hardware (LSQ) and noisy systems (NISQ). Surprisingly, while LSQ regimes will be inaccessible to classical hardware emulation and make verification difficult, verification is also complicated for noisy systems, particularly when they repeat some sequence of code iteratively.

The other key point is to make sure, in the case of the use of a remote quantum computer, that the recovered result corresponds to the submitted calculation and that an intruder did not interfere in the history nor was able to alter the calculation on the quantum computer side.

One of the methods consists in relying on the concept of **blind computing** devised in 2009 by Anne Broadbent, Joseph. Fitzsimons and Elham Kashefi<sup>1181</sup>.

The **CEA LIST** announced in June 2020 that it had created **QBRICKS**, an environment for the specification, programming and formal verification of quantum algorithms. They used to do this for critical embedded systems where certification by formal proof is particularly important. They are now entering the field of quantum programming and have experimented their model with QPE, the quantum phase algorithm that fits into Shor's model for integer factorization and the full Shor algorithm. This work involves the joint LRI laboratory at the University of Paris-Saclay and Centrale-Supelec<sup>1182</sup>.

One of the major advances in the explicability of quantum algorithms comes from researcher **Urmila Mahadev**, whose work between 2012 and 2018 has led to the creation of a method for verifying quantum computer processing. She was postdoc at Berkeley and supported by Scott Aaronson and Umesh Vazirani, two eminent researchers in quantum algorithmic research.

Her work aims at proving that a quantum computer has indeed performed the treatments it has been asked to do. She shows that a classical computer coupled to a simple quantum computer can verify in a polynomial way the results of a quantum computer<sup>1183</sup>. The method exploits a technique of post-quantum cryptography that the verifier cannot break (LWE: Learning With Errors). LWEs are part of the Lattice-based cryptography (EN) or Euclidean networks (FR) class<sup>1184</sup>.

Other quantum programs verifiers<sup>1185</sup> from research laboratories include the **Path-sum** framework from the University of Waterloo<sup>1186</sup>, **VOQC** (Verified Optimizer for Quantum Circuits) from the University of Maryland, itself based on **SQIR** (Small Quantum Intermediate Representation) supporting verification<sup>1187</sup> and QHL from Tsinghua University<sup>1188</sup>.

---

<sup>1180</sup> See also [Quantum cloud computing with self-check](#) by Rainer Blatt et al, May 2019, which discusses quantum simulation calculations on 20 qubits of trapped ions with results controlled on the quantum computer as fast as on the PC.

<sup>1181</sup> See [Universal blind quantum computation](#) by Anne Broadbent, Joseph Fitzsimons and Elham Kashefi, 2008 (20 pages) and the [associated presentation](#) (25 slides).

<sup>1182</sup> See [Toward certified quantum programming](#) by Sébastien Bardin, François Bobot, Valentin Perelle, Christophe Chareton and Benoît Valiron, 2018 (4 pages) and [An Automated Deductive Verification Framework for Circuit-building Quantum Programs](#) by Christophe Chareton, Sébastien Bardin, François Bobot, Valentin Perelle and Benoît Valiron, 2021 (30 pages).

<sup>1183</sup> See a description of the method in near-natural language in [Graduate Student Solves Quantum Verification Problem](#), October 2018 and two reference publications: [Classical Verification of Quantum Computations](#), September 2018 (53 pages) and [Interactive Proofs For Quantum Computations](#), April 2017 (75 pages).

<sup>1184</sup> See this presentation describing the LWE protocol: [An Introduction to the Learning with Errors Problem in 3 Hours](#) (76 slides).

<sup>1185</sup> See the review paper [Formal Methods for Quantum Programs: A Survey](#) by Christophe Chareton, Sébastien Bardin, Dongho Lee, Benoit Valiron, Renaud Vilmar and Zhaowei Xu, September 2021 (66 pages).

<sup>1186</sup> See [Towards Large-scale Functional Verification of Universal Quantum Circuits](#) by Matthew Amy, University of Waterloo, 2018 (21 pages).

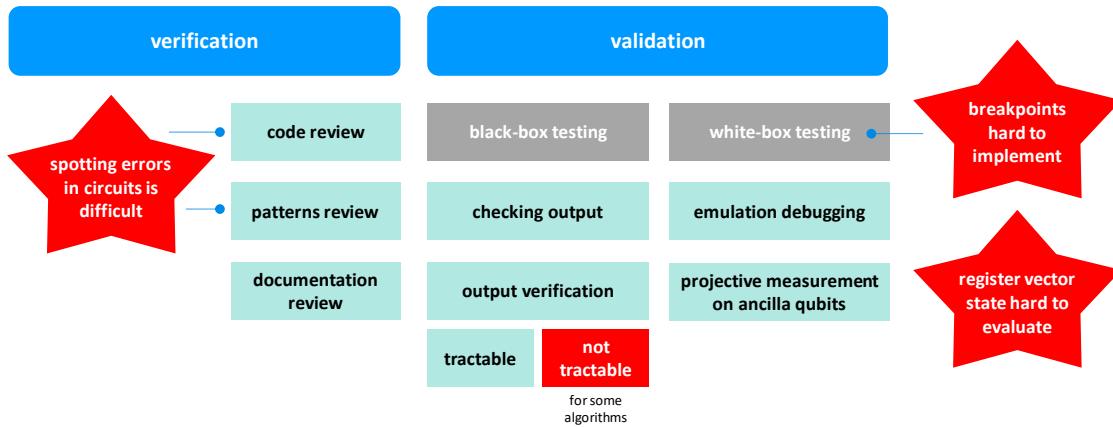
<sup>1187</sup> See [A Verified Optimizer for Quantum Circuits](#) by Kesha Hietala et al, University of Maryland (36 pages).

<sup>1188</sup> See [Quantum Hoare logic with classical variables](#) by Yuan Feng et al, University of Technology Sydney, Australia, Chinese Academy of Sciences and Tsinghua University, China, April 2021 (44 pages).

# Debugging

Like any computer software, quantum software requires a set of quality control processes. Like most human-originated creations, they are prone to bugs and errors. Some classical computing methods can be reused for this respect but many require some adaptation to the specifics of quantum computing, whether done on gate-based systems or on analog quantum simulators.

A quantum circuit is not easy to debug! It will certainly require new debugging tools and approaches. For the moment, simple circuits can be analyzed and debugged with a quantum emulator running on a classical computer, to understand how the qubit register vector state evolves step-by-step. But when quantum circuits in the advantage regime, beyond any classical emulation capacity, other means will have to be used.



Software quality control usually goes through two main steps: verification and validation.

**Verification** deals with verifying that the code will run as expected. It includes checking code documentation, designs, circuits and the various software components or patterns that are used. Verification also deals with making sure that the specifications are correctly implemented by the system. It responds to the question: are we building the product right?

In classical programming, good programmers and code reviewers can spot an error with just looking at the code. Code inspection tools can also detect undeclared variables or variables used in the wrong context. These errors are way more difficult to detect visually on a quantum circuit, particularly with large ones. It may require the use of code decomposition in modules or patterns, like in object-oriented programming.

**Validation** concerns the program output and making sure it works as planned. It includes testing and validating the code against the user's needs. It responds to the question: are we building the right product? Quantum computing results validation is usually fast like with integer factoring (it requires a simple classical multiplication) or a Grover search (it requires checking the Oracle once in a classical way).

But some circuit validations may need to be done on a quantum computer, like with a boson sampling or with a QMA prover (Quantum-Merlin-Arthur). On top of that, contrarily to classical computers, quantum computations errors can also come from hardware imperfections and the fateful quantum noise<sup>1189</sup>. Compiler, code optimizers and even error correction codes can also generate software bugs and amplify some errors.

<sup>1189</sup> See [Formal Verification vs. Quantum Uncertainty](#) by Robert Rand et al, University of Maryland, 2019 (12 pages) that pinpoints the role of hardware errors in quantum programs.

Quantum software bugs can have various sources: errors in the data preparation (which is itself based on quantum gates), incorrect operations and transformations, incorrect compositions and iterations and also incorrect qubits deallocations (or “uncomputations”)<sup>1190</sup>.

During validation, testing use the white-box and black-box approaches. **White-box** testing tests internal data structures and program flow, and may include some interactive debugging.

**Black-box** testing looks at the functionality, ignoring the inner workings of the software, making sure the expected output is obtained with a given input?

How about using interactive debugging in the white-box approach? Right now, it can be done on quantum emulators but is limited by their computing/memory capacity. It can't exceed 40 qubits and practically 16 qubits. A state vector representation is quite difficult to visualize beyond 8 qubits.

On a real machine, implementing interactive breaking points in a quantum circuit is difficult due to the impact of measurement on the qubits register vector state and on the probabilistic nature of quantum computing. Let's say we'd like to implement a breaking point and line by line code execution. We'd need to run the quantum algorithm and stop it at the breaking point then make some measurement.

But good measurement, just to get a state in the computational basis would require running the code many times. And even way more times if we'd need to reconstitute the full vector state. Then, to move to the next series of gates, the circuit would have to be re-run the same number of times. And again and again and again. It would be worse if we were to check the entanglement within the register. Deciding if a register is separable is in itself an NP-hard problem. One way to proceed is to implement unit testing with splitting the code in trusted blocks and patterns. Other debugging tools can involve projective measurements on ancilla qubits or even gentle measurement techniques<sup>1191</sup>. And this deals just with classic gate-based quantum computing. Analog quantum computing and special techniques like MBQC or FBQC (from PsiQuantum) will mandate specific debugging techniques and tools.

At last, let's mention that many quantum algorithms are hybrid and aggregate classical and quantum algorithms, which requires another set of discipline and tools.

Research is going on in all these dimensions around the world. These are strategic components for quantum computing<sup>1192</sup>.

## Benchmarking

### Quantum Volume

IBM has been communicating since 2017 on the notion of **quantum volume** to evaluate the power of its quantum computers. This notion was then adopted by **Honeywell** in March 2020 and afterwards by **IonQ** in October 2020. Its use is also recommended by the **Gartner Group**.

Quantum volume is an integer that is supposed to associate the quantity of qubits and the number of quantum gates that can be executed consecutively with a reasonable error rate.

---

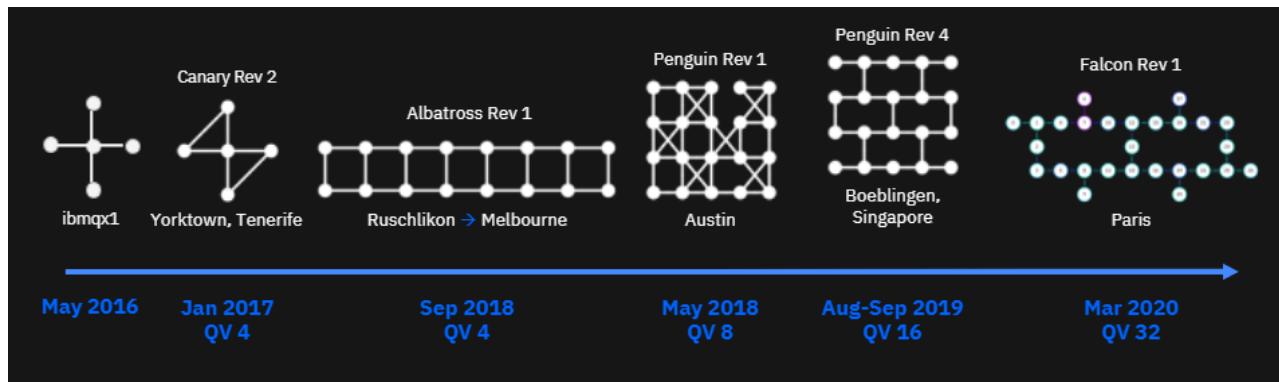
<sup>1190</sup> See [Quantum Computing Made Easier Through New Debugging Tools](#) by Lornajane Altura, 2019. Referring to [QDB: From Quantum Algorithms Towards Correct Quantum Programs](#) by Yipeng Huang and Margaret Martonosi, 2018 (13 pages).

<sup>1191</sup> See [Debugging Quantum Processes Using Monitoring Measurements](#) by Yangjia Li and Mingsheng Ying, 2014 (7 pages) describes the process of interim measurement process within code and [Projection-Based Runtime Assertions for Testing and Debugging Quantum Programs](#) by Gushu Li et al, 2020 (29 pages) proposes to use some ancilla qubits to indirectly detect vector state characteristics. It uses projective measurements on a different basis than the computational basis of each qubit.

<sup>1192</sup> It includes the study [Program Verification, Debugging, and QC Simulation — EPiQC](#), a IARPA funded project on quantum program verification and debugging.

Indeed, having N qubits but being limited by the number of quantum gates that can be used can be detrimental to the execution of many quantum algorithms. Some are greedy for quantum gates, others are not<sup>1193</sup>.

IBM thus indicated the qubit configurations that allowed them to go from a quantum volume of 4 with 5 qubits in 2017 to 32 in March 2020 and then to 64 in August 2020, with 27 qubits and 128 in July 2021 also with 27 qubits (both on the Montreal system)<sup>1194</sup>.



It's apparently very simple. But as soon as you try to understand where this magic number comes from, things get complicated. First, this number is supposed to aggregate four performance factors:

- The **number of physical qubits** of the processor.
- The **number of quantum gates** that can be chained consecutively without the error rate being detrimental to the results.
- The **connectivity between these qubits**, which will impact the length of execution of an algorithm and potentially improve quantum volume for qubits with high connectivity such as with trapped ions.
- The **number of quantum gates** that can be executed in parallel.

This quantum volume is evaluated using a random calculation benchmark consisting of chaining random quantum gates and which must give a correct result in two thirds of the cases. Why two thirds? Because quantum computing provides a probabilistic result. To obtain a deterministic result, the calculation is executed several times and the average of the results is evaluated, up to thousands of times as proposed by IBM in its cloud system. With an average of two-thirds good results, one can therefore statistically converge to a good result after a few measurements. The accuracy of the result will depend on this number, which is usually a few thousand.

In the first version in 2017, the quantum volume was the square of the maximum number of qubits on which the processor could perform this calculation<sup>1195</sup>. The definition then was changed in 2019 to become 2 to the power of this number of qubits<sup>1196</sup>.

The following illustration explains how the 2017 and 2019 quantum volumes are evaluated.

<sup>1193</sup> Some algorithms can thus be satisfied with a limited number of quantum gates, such as Deutsch-Jozsa's and is satisfied with only four series of quantum gates. Peter Shor's integer factoring algorithm requires a depth of quantum gates equal to the cube of the number of qubits used.

<sup>1194</sup> See [IBM Delivers Its Highest Quantum Volume to Date, Expanding the Computational Power of its IBM Cloud-Accessible Quantum Computers](#), August 2020. To obtain a volume of 64, IBM must align 8 qubits to a computational depth of 8 sets of quantum gates.

<sup>1195</sup> See [Quantum Volume](#) by Lev Bishop, Sergey Bravyi, Andrew Cross, Jay Gambetta and John Smolin, 2017 (5 pages).

<sup>1196</sup> See [Validating quantum computers using randomized model circuits](#) by Andrew W. Cross et al, 2019 (12 pages).

The diagram below from a paper by Robin Blume-Kohout and Kevin Young specifies how the m (number of qubits) and the d (computational depth) are evaluated<sup>1197</sup>.

$d \simeq 1/(n\epsilon_{eff})$ $V_Q = dn = 1/\epsilon_{eff}$ $V_Q = \min(n, d)^2$ $V_Q = \max_{n' \leq n} \min \left[ n', \frac{1}{n'\epsilon_{eff}(n')} \right]^2$ $\log_2 V_Q = \operatorname{argmax}_m \min[m, d(m)]$	<b>d = maximum computing depth</b> <b>n = number of qubits</b> <b><math>\epsilon_{eff}</math> = % error rate of 2 qubits gates</b> <b>base quantum volume = qubits # * computing depth</b> <b>quantum volume becomes <math>\min(n, \text{depth})^2</math> to avoid tweaking the system with a low n=2 and a very high fidelity</b> <b>2017 QV : scans all combinaisons of n' qubits below the available number of qubits, to run a random algorithm generating 2/3 good results.</b> <b>2019 QV : QV is a power of 2 of the number of qubits</b>
--	--

The number of qubits obtained to evaluate the quantum volume is much lower than the total number of qubits available: 8 for 16 in this case. The benchmark allows only 8 series of quantum gates in a row over 8 qubits, for 38 with only two qubits. In its 2017 version, the quantum volume was the grey square area containing the red lined squares.

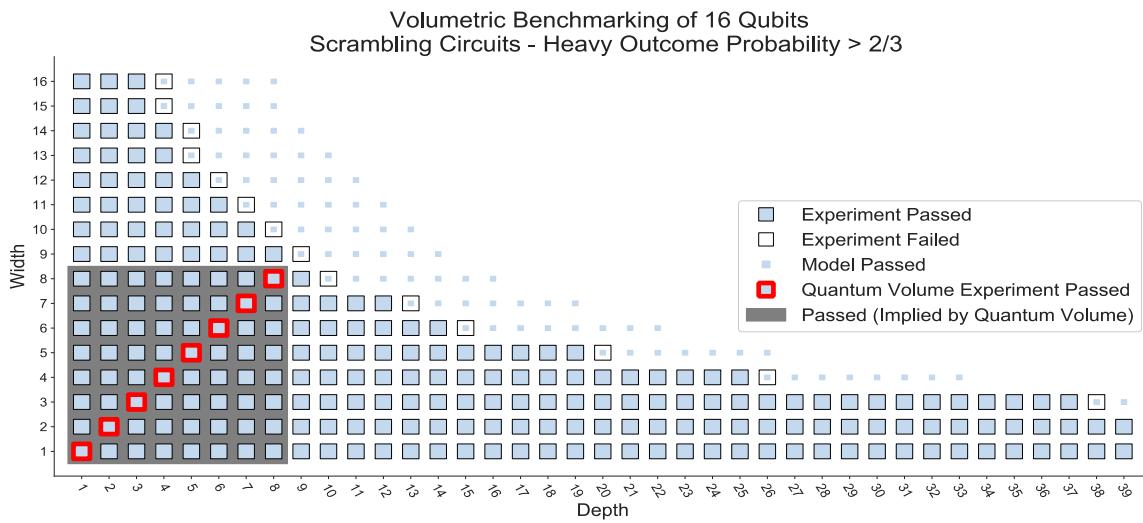


Figure 8(a). Volumetric benchmarking of a 16 qubit device using scrambling circuits. If at least 2/3 of the measurement results are heavy for a given width/depth pair, then the pair passes the test and is marked with a large, solid blue box. Using linear axes, the quantum volume experiments appear along the diagonal and are outlined with heavy, red lines. For this example,  $\log_2(V_Q) = 8$ . It is expected that scrambling circuits with both width and depth less than or equal to the quantum volume should succeed, and we highlight these with a gray background.

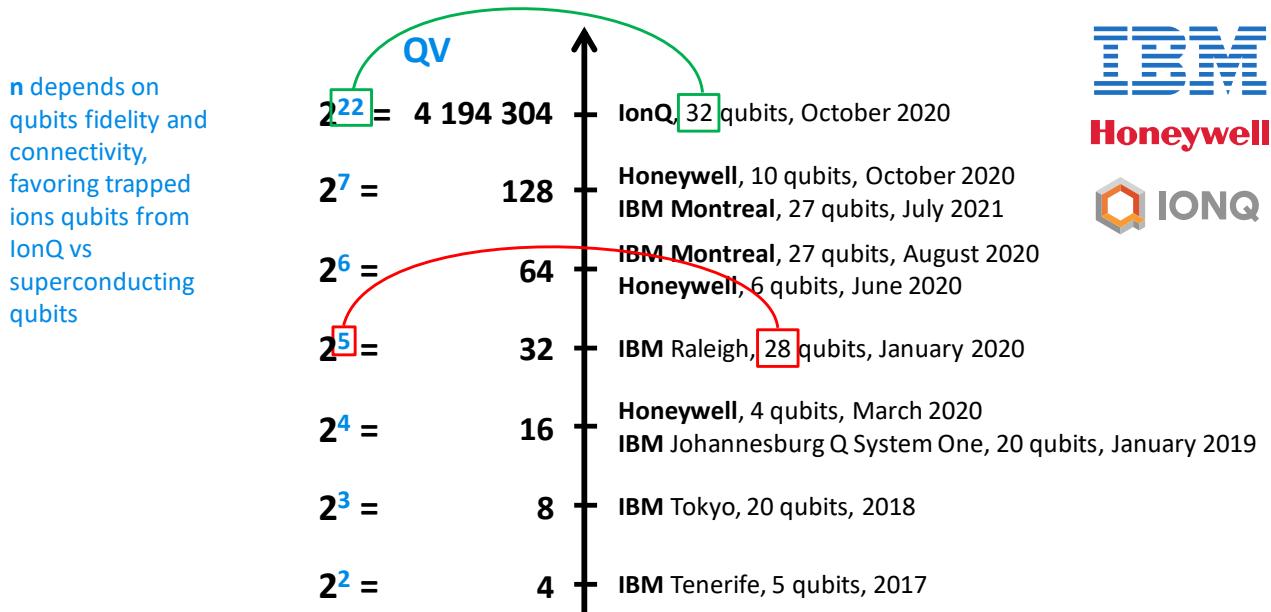
In its 2019 version, it became  $2^8$ , or 256 instead of 64 ( $8^2$ ). In the end, it is the dimension of Hilbert's vector space, i.e. the number of different superposed states that it is able to manage from a practical point of view with a depth of computation equal to the number of corresponding qubits.

When IBM states that their 27-qubit processor has a quantum volume equal to 127, it means that they only managed to validate their benchmark with 7 qubits among these 27 qubits.

---

<sup>1197</sup> In [A volumetric framework for quantum computer benchmarks](#), February 2019 (24 pages), Robin Blume-Kohout and Kevin Young propose volumetric benchmarks to evaluate the performance of quantum computers based on IBM's quantum volume. The latter also proposes its [own quantum volume evaluation code](#).

The announcement of IonQ of a quantum volume greater than four million corresponded precisely to a QV of 4,194,304, representing  $2^{22}$ .



So, with the ability to run 22 sets of quantum gates on 22 of these 32 qubits, with two-thirds correct results on the used random benchmark. This record seems to be related to the good connectivity of trapped ion qubits. These can all be directly entangled with each other, unlike superconducting qubits, which are at best entangled with their immediate neighbors. This allows the benchmark to be achieved in fewer series of quantum gates than on superconducting qubits, which require a lot of SWAP gates generating rapidly accumulating errors.

By the way, **IonQ** now uses a quantum volume defined by “algorithmic qubits”, or the number of referenced qubits equal to  $\log_2(\text{IBM's QV})$ , 22 in our case.

The quantum volume is also limited to about 50 operational qubits. Indeed, it can only be evaluated with a benchmark comparing the qubits with their simulation on a conventional computer. This emulation is constrained by memory size, which reaches its limits between 50 and 55 qubits<sup>1198</sup>.

Quantum computing scientists are circumspect about the interest of this indicator which is too simplistic<sup>1199</sup>. This use is contested by Scott Aaronson, a specialist in complexity theories and quantum algorithms<sup>1200</sup>.

He reminds readers that the quantum volume reached back then by Honeywell in mid-2020 was more than easily emulable in a simple classical computer, if not on an Apple Watch! This does not make it particularly powerful. And when the QV could make sense, we won't be able to measure it!

Scott Aaronson therefore believes that this quantum volume indicator, which is a marketing simplification tool from IBM, should be avoided. The solution? It consists in describing precisely the characteristics of the machine with its number of qubits, their connectivity, their coherence time (T1, T2), the error rate of the one and two-qubit quantum gates, the resulting depth of calculation and the resource requirements to emulate the whole on a conventional computer.

<sup>1198</sup> See [Why Is IBM's Notion of Quantum Volume Only Valid up to About 50 Qubits?](#) by Jack Krupansky, October 2020.

<sup>1199</sup> Imagine an indicator of the power of your laptop aggregating the processor clock frequency, its number of cores, the power of its CPU, the RAM memory, the storage capacity, its type (hard disk, SSD) etc? And there, to ask yourself if you will be able to efficiently use your video editing, photo derush or video game software on augmented reality headphones!

<sup>1200</sup> In [Turn down the quantum volume](#), Scott Aaronson, published just after Honeywell's February 2020 announcement.

With most vendors, these indicators are generally found in the scientific publications of researchers but not always in the marketing literature of manufacturers. However, IBM publishes most of these data on their quantum systems available on Q Experience.

In November 2021, IBM added a third item to measure quantum systems performance on top of the number of qubits (for scale), quantum volume (for quality): CLOPS, or Circuit Layers Operations per seconds (for speed), an equivalent to the clock of a classical CPU, given the numbers are different for resetting qubits, operating quantum gates and measuring qubits<sup>1201</sup>. As of 2021, IBM's systems CLOPS were between 1,5 and 2,4K, so about 2.000 layers of qubit gates per seconds.

## Atos Q-score

In December 2020, Atos announced its Q-score benchmark. Instead of comparing some computing power indicator like the Quantum Volume, it's based on getting the maximum size of a standardized problem that can be solved on a given hardware<sup>1202</sup>. The selected problem is the classical combinatorial **MaxCut**. Its variations are used to solve the traveling salesman problem or various graphs problems with applications in logistic, industry and finance. It can also be used to handle clustering in quantum machine learning. The Q-score benchmark is evaluated with using a hybrid classical+quantum with a QAOA (Quantum Approximate Optimization Algorithm).

This benchmark has some benefits : it's a simple metric (the number of variables that can be used in the optimization problem) and it's independent from the hardware architecture and it doesn't require a quantum computing emulation capacity like with the IBM Quantum Volume. And the algorithm solutions can be verified polynomially on a classical computer. The Q-Score software tools are also open-source and published on [Github](#).

Atos plans to publish the Q-scores of various QPU manufacturers. Right now, the record is at 15Q. It could soon reach 20Q. And 60Q is needed to showcase a real quantum supremacy.

This benchmark would need to be completed by other benchmarks such as one for quantum chemistry simulation (number of atoms in molecule) and another on the size of the maximum number that can be factorized (in power of 2).

### The Q-score procedure

For a given QPU. For increasing graph size  $N$ :

Get average quality (value of MAXCUT cost function)  $Q_R(N)$  of a random solver.

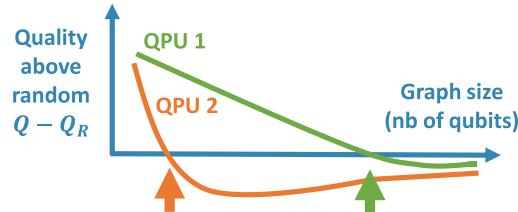
Repeat  $P = 500$  times:

- Pick a random (Erdős-Rényi) graph  $G_N$  of size  $N$
- Apply QAOA procedure with COBYLA optimization (random init.) and MAXCUT cost function  $H$ , get quality  $Q = \langle \psi | H | \psi \rangle$  of final state of optimized circuit
- Return quality  $Q(G_N)$

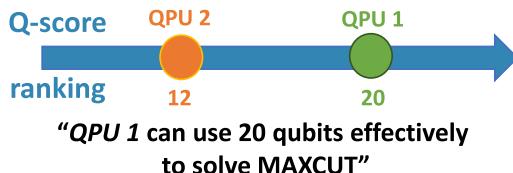
Average over the  $P$  qualities  $Q(G_N)$  to get average  $Q(N)$ .

As soon as the quality becomes lower than random ( $Q(N) \leq Q_R(N)$  with statistical confidence) and under a time limit, return  $N$ . This is the Q-score.

### Typical output



The quality above random usually decreases with the number of qubits because of decoherence in NISQ processors.



<sup>1201</sup> With their Falcon R5 processor, qubit reset takes 450ns while qubits readout takes 750 ns. It's much longer than gates.

<sup>1202</sup> See [Benchmarking quantum co-processors in an application-centric, hardware-agnostic and scalable way](#) by Simon Martiel, Thomas Ayral and Cyrille Allouche, February 2021 (11 pages).

## Other benchmarks

There are many other quantum computing benchmarks around.

The DoE **ORNL** (Oak Ridge National Laboratory) proposed its own benchmark for chemical simulation<sup>1203</sup>. It deals with the simulation of three 2-atoms molecules (NaH, KH et RbH) which can be simulated on existing IBM and Rigetti 20 and 16 qubits superconducting systems. It's not generic and can't go beyond these molecule sizes.

There is also the **cycle benchmarking** coming from a team involving Canada, Denmark and Austria which assesses the low-level quality of qubits entanglement<sup>1204</sup>. This is far from being a use-case centric benchmark.

In 2021, **DARPA** launched a research RFP for the creation of benchmarks in two categories: application-specific hardware-agnostic benchmarks (TA1, with \$1.45M for 18 months) for quantum computing and hardware resource estimates for quantum computers (TA2, with a funding of \$1.5M over 18 months).

In April 2021, another benchmark proposal was made by a team from QuSoft (The Netherlands), the University of Cambridge (UK) and Caltech (USA). It is bound to measure the performance of universal quantum computers in a hardware-agnostic way with six structured circuits tests (Bell test, Schrödinger's microscope, Mandelbrot, line drawing, matrix inversion and platonic fractals). It's quite complex to interpret and reading out the graphical results is not straightforward, nor connected to an application need<sup>1205</sup>.

In October 2021, a series of application oriented benchmarks was proposed by researchers from Princeton, HQS, QCI, IonQ, D-Wave and Sandia Labs as a collaboration driven by the Quantum Economic Development Consortium (QED-C) in the USA<sup>1206</sup>. It mixes the volumetric benchmarking method from IBM and a comparison of performance with various standard algorithms. They did some comparison on actual quantum hardware from IBM, Rigetti, HQS and IonQ.

Other kinds of benchmarks would be interesting, particularly comparing quantum computing technologies between gates-based, annealing and simulation computing variations.

At last, the **IEEE** has launched several benchmarking initiatives on its own with a standard to be submitted in 2024<sup>1207</sup>.

## Quantum supremacy and advantage

Quantum supremacy is a term widely used in the communication of certain vendors such as Google, at least in 2017 and with a peak in October 2019. The term was coined by John Preskill in a paper presented at the Solvay Congress in 2011<sup>1208</sup>.

Quantum supremacy is achieved when an algorithm, useful or not, is only executable on a quantum computer, since this problem cannot be solved on the most powerful supercomputer in a human scale time<sup>1209</sup>.

---

<sup>1203</sup> See [ORNL researchers advance performance benchmark for quantum computers](#), January 2020.

<sup>1204</sup> Presented in [Characterizing large-scale quantum computers via cycle benchmarking](#) par Alexander Erhard et al., 2019 (7 pages).

<sup>1205</sup> See [Scalable Benchmarks for Gate-Based Quantum Computers](#) by Arjan Cornelissen et al, April 2021 (54 pages).

<sup>1206</sup> See [Application-Oriented Performance Benchmarks for Quantum Computing](#) by Thomas Lubinski et al, October 2021 (33 pages).

<sup>1207</sup> See [P7131 - Standard for Quantum Computing Performance Metrics & Performance Benchmarking](#). It covers gate-based quantum computing. See also [Metrics & Benchmarks for Digital Quantum Computing](#) by Robin Blume-Kohout (18 slides) and [Summary of the IEEE Workshop on Benchmarking Quantum Computational Devices and Systems](#), 2019. Also, see [P2995 - Trial-Use Standard for a Quantum Algorithm Design and Development](#) and [P3120 - Standard for Quantum Computing Architecture](#).

<sup>1208</sup> It is described in [Quantum Computing and the Entanglement Frontier](#), 2011.

Many experts estimate that the threshold of 50-ish quality qubits, with a low error rate and a long coherence time, will be needed to achieve any quantum supremacy. These will probably be logical qubits, assembling physical qubits and some quantum error correction codes.

Quantum supremacy doesn't mean that a given quantum system is supremely more powerful than all its contemporary supercomputers. The term is associated with a trio consisting of one quantum algorithm, one quantum computer, and the best-in-class available algorithms adapted to the most powerful available supercomputers. The three criterias are moving targets.

Ariel Bleicher rightly points out that supercomputers and those who use them have not said their last word and are also looking to improve their own algorithms<sup>1210</sup>.

Robert König (Technical University of Munich), David Gosset (University of Waterloo, Canada) and Sergey Bravyi (IBM) demonstrated in October 2018 that quantum computers can actually perform operations inaccessible to conventional computers but based only on the case of a particular algorithm<sup>1211</sup>.

Some D-Wave and Google benchmarks carried out in 2015 and showing the superiority of the quantum solution were then contradicted by the creation of algorithms optimized for supercomputers under certain conditions. In a few years' time, it will certainly come into play for a few algorithms that cannot have optimized supercomputer equivalents.

Google's quantum supremacy announced in October 2019 was touted as serious back then. It was later downgraded. It was based on a sort of *random numbers sampling* algorithm using 53 qubits. But there was only a 0,2% chance to get a good result, thus the need to run the algorithm 3 million times to compute an average. When Sycamore is used for useful algorithms, fewer than 20 qubits are used and we're far off any quantum supremacy or advantage.

Cristian and Elena Calude of the University of Auckland in New Zealand then argued that a high-performance limit, that of a precise quantum computer, is compared to a low limit which is the best performance in solving the same problem in a supercomputer<sup>1212</sup>. Quantum supremacy is thus a comparable between the existence of a quantum performance and the assumption of the non-existence of an equivalent performance in classical computing. The authors also point out a criterion that is sometimes missing from the analysis: it would be better if the tested algorithm were useful for something! This is not always obvious with some quantum algorithms, as we will see later.

A 2020 paper from Yiqing Zhou (University of Illinois), Edwin Miles Stoudenmire (Flatiron Institute) and Xavier Waintal (CEA-IRIG) provided an interesting "reset" view on Google's quantum supremacy.

---

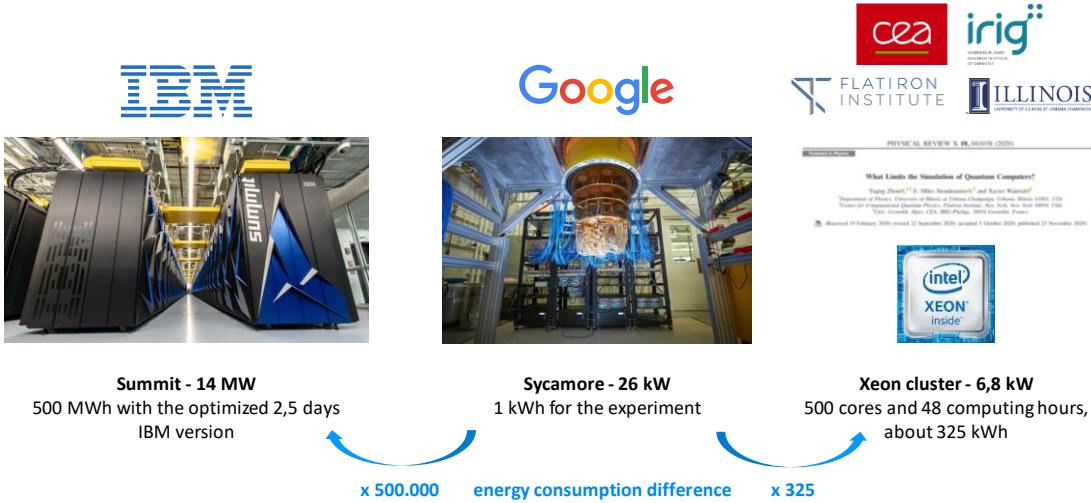
<sup>1209</sup> See [Quantum supremacy: Some fundamental concepts](#) by Man-Hong Yung, January 2019 (2 pages) according to which there are three ways to demonstrate quantum supremacy: boson sampling, PQI and chaotic quantum circuits.

<sup>1210</sup> See [Quantum Algorithms Struggle Against Old Foe: Clever Computers](#) by Ariel Bleicher, February 2018. This mentions the discovery of classical algorithms that are as powerful as their quantum equivalents, such as the one from Ewin Tang, already mentioned on page 61.

<sup>1211</sup> See [First proof of quantum computer advantage](#), October 2018 and [Quantum advantage with shallow circuits](#), April 2017 (23 pages).

<sup>1212</sup> In [The road to quantum computing supremacy](#), 2017.

It stated that emulating Sycamore's processes in a classical computing could use some compression technique to take into account the qubit's noise. With this compression, emulating Sycamore is much less costly and can be done on a simple microcomputer<sup>1213</sup>. But this was done with a 95% emulated gates fidelity. With a 99% fidelity matching Sycamore's system, it would still require a couple hundred cores and some TB of memory, probably fitting in a data-center rack. There would be an energy advantage for Sycamore but going down from x500.000 vs the IBM Summit to about only x325 for a 500 core cluster server.



Xavier Waintal use the scale *next*, with 5 difficulty levels, to build a quantum computing machine. It positions where we are right now and the challenges ahead. It goes beyond large scale computing given some quantum memory would be mandatory for some key algorithms like QML and HHL.

difficulty scale	technology	use cases	examples
1	quantum simulator (analog-no gates)	quantum simulations	D-Wave, Pasqal
2	gates-based analog systems, low fidelity	system validation NISQ algorithms	Google, IBM, Rigetti, ...
3	gates-based analog systems, low fidelity	variational calculations in quantum chemistry	Possibly PsiQuantum
4	ideal quasi-deterministic gates-based systems (FTQC/LSQ)	factoring large numbers, exact quantum chemistry	TBD
5	4 + quantum memory	quantum machine learning, linear algebra (HHL)	TBD

adapted from a Xavier Waintal presentation in 2020

In 2021, a Chinese team was even able to classically simulate the Google Sycamore cross-entropy benchmark with a single Nvidia A100 GPGPU running for 149 days with a fidelity of 73,9% while Sycamore's fidelity was only 0,2%<sup>1214</sup>. Another Chinese research team, from Alibaba, found a way to optimize Sycamore's emulation to reach only 20 days of computing on a system equivalent of the IBM Summit<sup>1215</sup>.

In February 2021, yet another quantum advantage was announced by a team of researchers from France and Edinburgh, including Eleni Diamanti and Iordanis Kerenidis<sup>1216</sup>.

<sup>1213</sup> See [What limits the simulation of quantum computers?](#) by Yiqing Zhou, Edwin Miles Stoudenmire and Xavier Waintal, PRX, November 2020 (14 pages).

<sup>1214</sup> See [Simulating the Sycamore quantum supremacy circuits](#) by Feng Pan and Pan Zhang, March 2021 (9 pages).

<sup>1215</sup> See [Efficient parallelization of tensor network contraction for simulating quantum computation](#) by Cupjin Huang et al, Alibaba, September 2021 (10 pages).

<sup>1216</sup> See [Experimental demonstration of quantum advantage for NP verification with limited information](#) by Federico Centrone, Niraj Kumar, Eleni Diamanti, and Iordanis Kerenidis, published in Nature Communications, February 2021 (13 pages). This was a follow-up of [Quantum superiority for verifying NP-complete problems with linear optics](#) by Juan Miguel Arrazola, Eleni Diamanti & Iordanis Kerenidis, Nature, 2018 (8 pages).

It involved a complicated photonics-based experiment that didn't do any real calculation. How can that be possible? It was about putting in place a QMA (Quantum Merlin Arthur) verification protocol.

The implemented protocol is an interactive test that requires, through a network, the verification of the solution of a complex NP-complete optimization problem without having to communicate the whole solution.

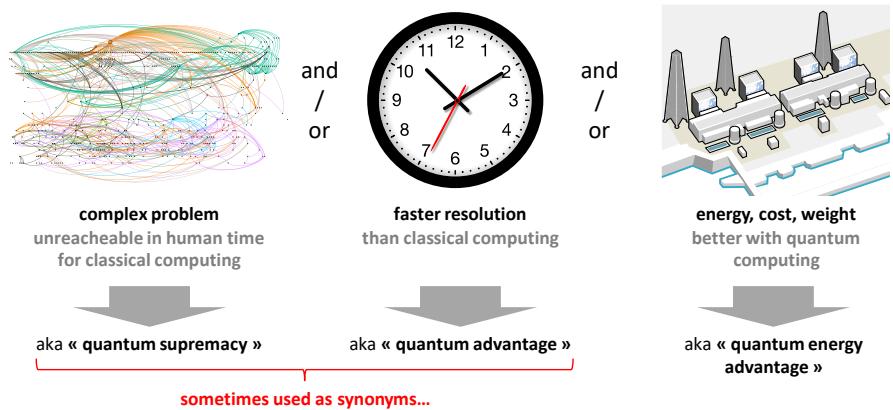
The breakthrough that made this possible was the creation of a system encoding the solution result with partial information about the solution to be verified from one network node to another. The protocol was able to compress a large vector state describing the partial information on the solution, involving some entanglement and multi-mode photons quantum communications.

This compression protocol would make it possible to verify the results in a much smaller time. No actual verification was done on the other end of the system.

So, we have here a quantum advantage coming from the way to connect a quantum computer solving an NP-complete SAT problem and another quantum computer verifying the solution with partial information. Both computers do not exist yet. Another view on this would be that it proposes an architecture to verify a solution to an NP-problem on an end-to-end solution.

Another comparison concept is now frequently used: **quantum advantage**. It corresponds to a situation where a quantum computer executes an algorithm faster than on the most powerful supercomputers. So, it's not as strong an argument as with quantum supremacy. But some are pushing various definitions for quantum advantage. Sometimes, it even has the same meaning than quantum supremacy but with a more politically correct terminology and for others, it's a stronger statement than quantum supremacy, meaning the same but for a useful algorithm. Who knows then?

We can also add the notion of **quantum energy advantage**, which may arise someday when on top of some computing time benefits, we could highlight the fact that quantum computers consume much less energy than supercomputers for solving similar problems. This remains to be proven and is still a subject of research.



In 2018, IBM researchers demonstrated that quantum supremacy was assured in the long run, even with quantum computers that can chain a finite and constrained number of quantum gates<sup>1217</sup>. In December 2020, they published a theoretical model that could prove some quantum advantage, solving binary function problems, and tested on a low scale on a 27 qubits superconducting system<sup>1218</sup>. These various, sometimes convoluted, performances are very hard to compare and evaluate.

<sup>1217</sup> See [Scientists Prove a Quantum Computing Advantage over Classical](#) by Bob Sutor, October 2018, [Quantum advantage with shallow circuits](#), Sergey Bravyi, David Gosset and Robert Koenig, 2017 (23 pages) and the video [Quantum advantage with shallow circuits](#), IBM Research, December 2017 (44 minutes).

<sup>1218</sup> See [Quantum advantage for computations with limited space](#) by Dmitri Maslov, Sarah Sheldon et al, IBM Research, December 2020 (12 pages). Also published in [Nature Physics](#) in June 2021.

Here's a tabulated consolidation of the various quantum supremacies and advantages announced since 2019<sup>1219</sup>. It shows that none of these achieved real useful computing with some application input data.

who and when	architecture	algorithm	input data	comment
Google, Oct 2019	Sycamore, 53 superconducting qubits	cross entropy benchmarking	none	running a random gates algorithm
China, December 2020	70 photons modes GBS (Gaussian Boson Sampling)	interferometer photons mixing	none	running a random physical process
IBM Research, December 2020	IBM 27 superconducting qubits	symmetric Boolean functions	SLSB3 function parameters	theoretical demonstration of quantum advantage
Kerenidis, Diamanti et al, March 2021	multi-mode photon dense encoding of verified solution	Quentin Merlin Arthur based verification	output from some quantum computation (not implemented)	no actual computing done in the experiment
China, April 2021	Quantum walk on 62 superconducting qubits	simple quantum walk	simulating a 2-photons Mach-Zehnder interferometer	no quantum advantage at all
University of Arizona, May 2021	supervised learning assisted by an entangled sensor network	variational algorithm, classical computing	data extracted from three entangled squeezed light photonic sensors	not a quantum « computing » advantage per se
China, June 2021	66 superconducting qubits and 110 couplers, Zuchongzhi 1, then 2.1	cross entropy benchmarking	none	56 used qubits
China, September 2021				60 used qubits
China, June 2021	144 photons modes GBS and up to 113 detected events	interferometer photons mixing	none	parametrizable photon phases could lead to a programmable system

## Quantum software development tools key takeaways

- Gate-based programming involves either graphical circuit design (mostly for training purpose) and (usually) Python based programming when qubit gates structures must be designed in an automated way.
- Python based programming is relying on libraries like IBM's Qiskit or Google's Cirq. There are however many development tools coming from universities and research labs like Quipper. Some tools like ZX Calculus are highly specialized and used to create quantum error correction codes or low-level systems.
- Quantum computing is based on running code multiple (thousands...) times and averaging the results. A single individual run yields a probabilistic outcome while many runs averages will converge into deterministic ones.
- Most quantum computers are used in the cloud, through offerings coming from the computer vendors themselves like IBM or D-Wave or from cloud providers like Amazon or Microsoft.
- Quantum emulators are very useful to learn programming, test it until the limits of classical emulation (about 40-50 qubits) and also help debug small-scale quantum algorithms. Quantum emulation is an indispensable part of any quantum cloud offering.
- Gate-based programs debugging is a significant challenge as it is difficult to implement equivalents of classical code breaking points. As a result, quantum code certification and verification is a new key discipline, particularly for distributed computing architectures such as the ones relying on the concept of blind quantum computing.
- Benchmarking quantum computers is an unsettled technique with many competing approaches. It includes the various techniques used to qualify so-called quantum supremacies and quantum advantages. Not a single of them, as of 2021, did show a real computing advantage compared to classical computing. The reasons were multiple, the main ones being that these experiments didn't implement any algorithm using some input data.

<sup>1219</sup> The Arizona performance is documented in [Researchers demonstrate a quantum advantage](#) by University of Arizona, June 2021, referring to [Quantum-Enhanced Data Classification with a Variational Entangled Sensor Network](#) by Yi Xia et al, June 2021 (17 pages). Their setting used variational quantum circuits for a classification of multidimensional radio-frequency signals using entangled sensors.

# **Quantum computing business applications**

Most algorithms mentioned before are generally very low-level. How about assembling them into business solutions, market by market? We are still far from having things settled for that respect. The quantum software industry is still very immature and for good reasons, since quantum computers are very limited at this stage. We are still in a stage equivalent where the computer industry was in the mid-1950s, when the software industry was in its infancy.

Still, you can discover here and there a lot of so-called case studies, mostly pushed by D-Wave and IBM and their customers or partners. These relate to proof-of-concepts and software prototypes. Most of these are not yet production grade nor bring any practical benefit compared to classical computing due to the limitations of existing hardware. Still, all this is very useful. This is an indispensable learning phase for research, startups and the industry. It's part of a readiness process that will speed things up when hardware will ramp-up. And this ramp-up will happen progressively.

## **Market forecasts**

Any new technology wave brings its market forecasts data born out of analysts and market survey companies. They have a very traditional closed-loop system in place: vendors want to get some ideas of customer demand or positive confirmation of their own biases, analysts poll large customers to get some understanding about their plans, and *voila*, you get your nice market predictions. It often looks like linear or simple non linear regressions. These predictions can become either self-fulfilling prophecies or total failures. The Gartner Group has turned its simplistic hype curve into a kind of Schrödinger's time and topic-independent wave equation of technology trends. But nobody really checked it, particularly when this curve was highly dependent on complicated scientific and technology challenges. It's more about probabilities than simplistic curves.

So, how could you predict the size and shape of the quantum software market, vertical per vertical, when you have no idea of when actual useful quantum accelerators will show up? Will it follow an exponential market growth rate worthy of those of the microcomputer and smartphones industries? Let's look at what we have in store.

BCG's quantum computing growth forecasts illustrate this strong uncertainty. They showcase predictions with an optimistic scenario, which starts seeing growth around 2030, and a very conservative one, which only takes off after 2040<sup>1220</sup>. In both cases, the quantum computing market grows linearly. They don't integrate a scenario of the emergence of the NISQ, or "Noisy Intermediate-Scale Quantum", or any advent of quantum simulators before NISQ become usable<sup>1221</sup>.

BCG has however created in 2018 a good inventory of the current potential qualitative use cases of quantum computing per vertical market<sup>1222</sup>. This covers both case studies coming from D-Wave and prospective applications devised by research labs and with large industry companies including the usual suspects from the aerospace, chemistry, energy, pharmaceuticals and financial sectors.

Most of these big names worked with either D-Wave or IBM, and sometimes with some independent software vendors or large IT services firms like Accenture.

---

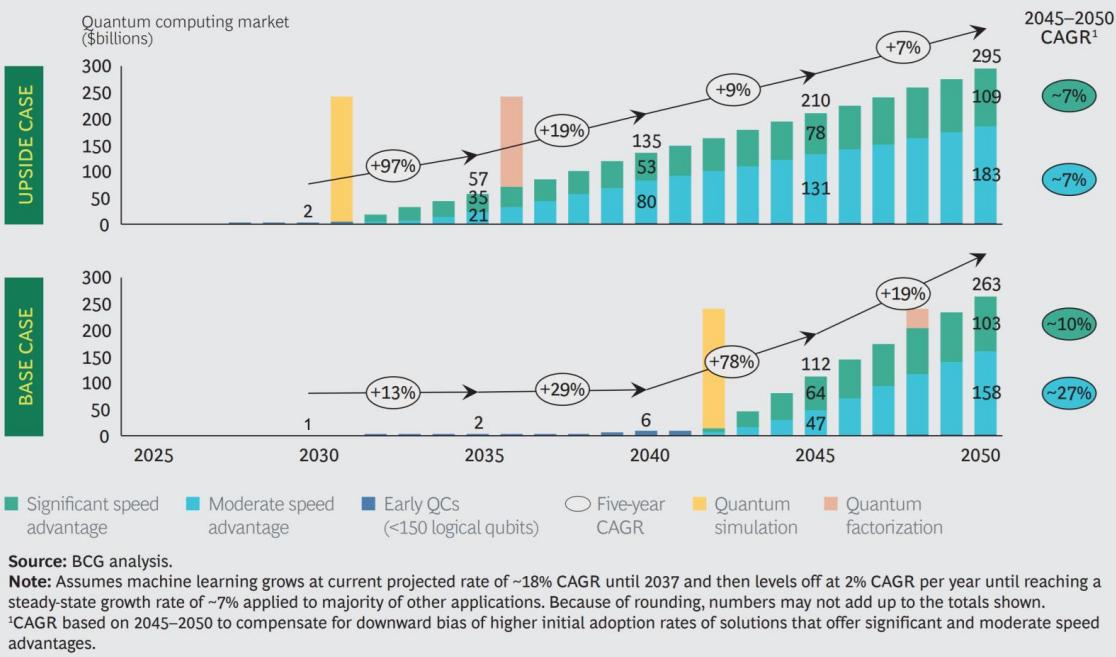
<sup>1220</sup> See [The coming quantum leap in computing](#), BCG, May 2018 (19 pages).

<sup>1221</sup> See [Quantum Computing in the NISQ era and beyond](#), 2018.

<sup>1222</sup> BCG illustration source: [The Next Decade in Quantum Computing and How to Play](#), BCG, 2018 (30 pages).

### EXHIBIT 3 | The Speed of Market Growth Depends on Technical Milestones

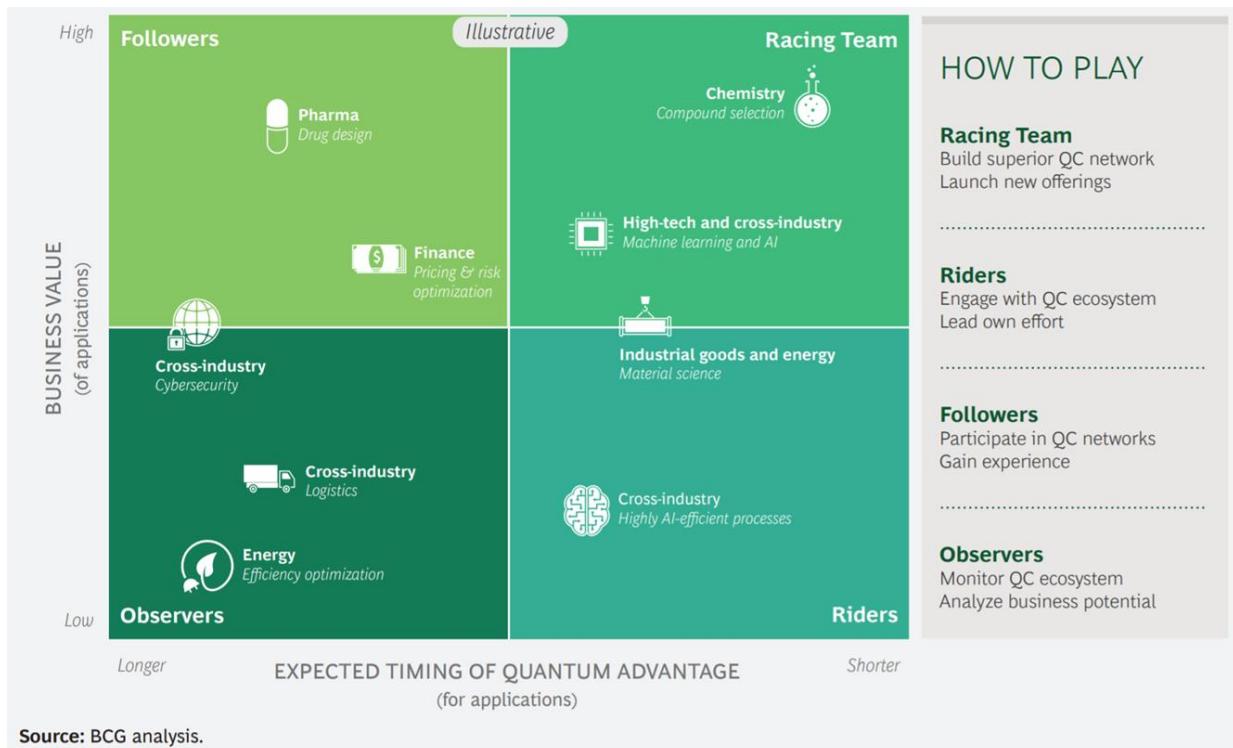
UPSIDE CASE (10:1 RATIO IN ERROR CORRECTION): MAJOR APPLICATIONS BY 2031  
BASE CASE (500:1): MAJOR APPLICATIONS BY 2042



### EXHIBIT 2 | Multiple Potential Use Cases for Quantum Computing Exist Across Sectors

INDUSTRIES	SELECTION OF USE-CASES	ENTERPRISES (EXAMPLES)
High-tech	<ul style="list-style-type: none"> <li>Machine learning and artificial intelligence, such as neural networks</li> <li>Search</li> <li>Bidding strategies for advertisements</li> <li>Cybersecurity</li> <li>Online and product marketing</li> <li>Software verification and validation</li> </ul>	 IBM      Telstra Alibaba      Baidu Google      Samsung Microsoft
Industrial goods	<ul style="list-style-type: none"> <li>Logistics: scheduling, planning, product distribution, routing</li> <li>Automotive: traffic simulation, e-charging station and parking search, autonomous driving</li> <li>Semiconductors: manufacturing, such as chip layout optimization</li> <li>Aerospace: R&amp;D and manufacturing, such as fault-analysis, stronger polymers for airplanes</li> <li>Material science: effective catalytic converters for cars, battery cell research, more-efficient materials for solar cells, and property engineering uses such as OLEDs</li> </ul>	Airbus      BMW NASA      Volkswagen Northrop Grumman      Lockheed Martin Daimler      Honeywell Raytheon      Bosch
Chemistry and Pharma	<ul style="list-style-type: none"> <li>Catalyst and enzyme design, such as nitrogenase</li> <li>Pharmaceuticals R&amp;D, such as faster drug discovery</li> <li>Bioinformatics, such as genomics</li> <li>Patient diagnostics for health care, such as improved diagnostic capability for MRI</li> </ul>	BASF      JSR Biogen      DuPont Dow Chemical      Amgen
Finance	<ul style="list-style-type: none"> <li>Trading strategies</li> <li>Portfolio optimization</li> <li>Asset pricing</li> <li>Risk analysis</li> <li>Fraud detection</li> <li>Market simulation</li> </ul>	J.P. Morgan      Barclays Commonwealth Bank      Goldman Sachs
Energy	<ul style="list-style-type: none"> <li>Network design</li> <li>Energy distribution</li> <li>Oil well optimization</li> </ul>	Dubai Electricity & Water Authority      BP

In another chart, BCG positions these vertical markets along two dimensions: business value and expected time of quantum advantage. This is more gut feeling than any real rationale thinking since there are too many variables to have any idea of where each of these industries sit in this fancy chart. We are at a too early stage of the quantum computing innovation cycle to make such predictions.



Predicting the size of the quantum computing market is indeed highly probabilistic. It's supposed to reach \$553M in 2023 according to **Markets and Markets** (in 2017), \$830M in 2024 for **Hyperion Research** (in 2021<sup>1223</sup>), \$1,9B in 2023 for CIR and \$2,64B in 2022 for **Market Research Future** (2018). Then we reached \$8,45B in 2024 for **Homeland Security** (in 2018), \$10B in 2028 for **Morgan Stanley** (as of 2017), \$15B by 2028 for **ABI Research** (2018) and \$64B by 2030 for **P&S Intelligence** (in 2020). At last, **ResearchAndMarkets** predicted in May 2021 that the global quantum technology market would even reach \$31.57B by 2026, including \$14.25B for quantum computing<sup>1224</sup>.

Some forecasts can reach other crazy heights. For **Bank of America**, quantum technologies will be as important as smartphones. The main reason? Its potential applications in healthcare.

The only problem: the analysis behind these predictions gets confused between big data and quantum computing<sup>1225</sup>.

As of early 2020, **McKinsey** even predicted that quantum computing would be worth \$1 trillion by 2035<sup>1226</sup>. It is easy to identify the forecast bias. It's based on a trick that was used a few years ago to evaluate the size of Internet of things and artificial intelligence markets.

<sup>1223</sup> See [Quantum Computer Market Headed to \\$830M in 2024](#) by John Russell, HPC Wire, September 2021.

<sup>1224</sup> See [The Worldwide Quantum Technology Industry will Reach \\$31.57 Billion by 2026 - North America to be the Biggest Region](#), May 2021.

<sup>1225</sup> See [Quantum computing will be the smartphone of the 2020s, says Bank of America strategist](#) by Chris Matthews, December 2019.

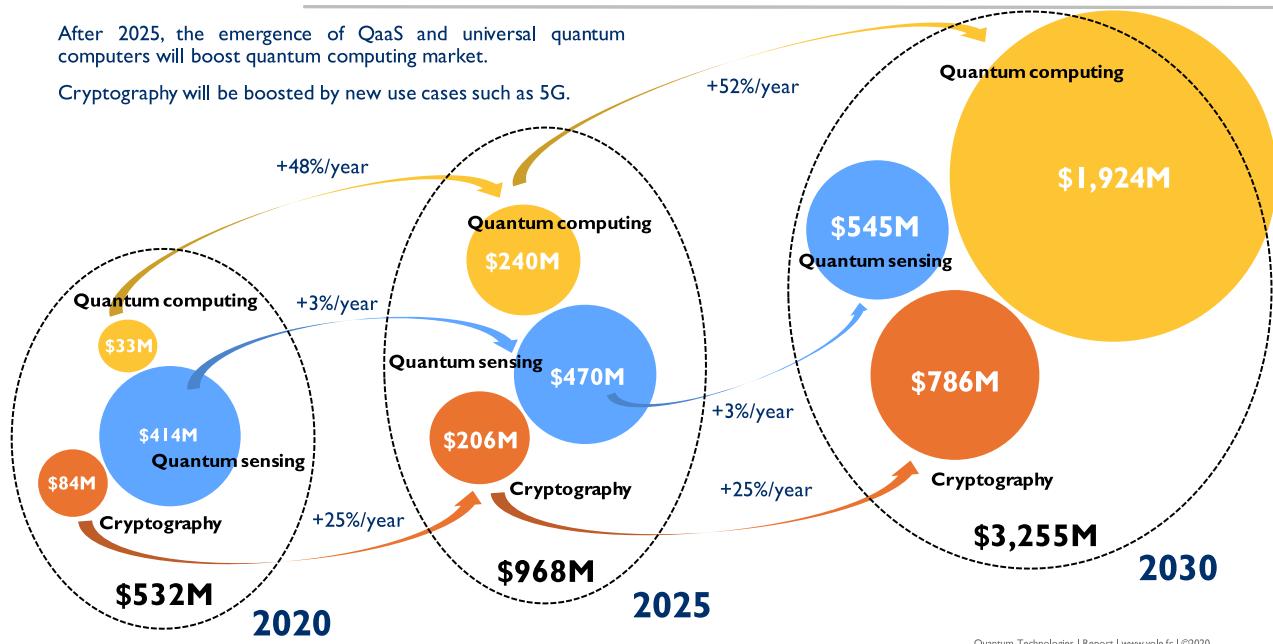
<sup>1226</sup> See [Quantum computing will be worth \\$1 trillion by 2035, according to McKinsey](#), March 2020.

It is not the market estimation for quantum technologies as such, but the incremental revenue it could generate for businesses, such as in health, finance or transportation. It is a bit like evaluating the software market (which could reach \$581B in 2021, including \$228B in enterprise software, source [Statista](#)) by summing up the total revenue of the companies who use some software! This would be quite a large number and a significant share of worldwide GDP<sup>1227</sup>. Market predictions should focus on IT products, software and services and should be compared with existing reference markets. For example, the 2020 worldwide servers market size was \$85.7B according to IDC<sup>1228</sup>.

In a 2021 publication<sup>1229</sup>, BCG estimated the size of the quantum computing market as 20% of its estimated generated value with customers, ending with a \$90B to \$170B market captured by technology providers, including software and services... some day after 2040, and a more reasonable \$1B to \$2B before 2030 and \$15B to \$30 after 2030. So, we have here an uncertainty based on an unknown estimated with some fuzzy technology capability predictions.

On its end, The Quantum Daily makes forecasts for the Quantum Cloud as a Service market of \$26B by 2030, tries to document its methodology and reminds us that it's based on vendors questionable roadmaps<sup>1230</sup>.

## 2020 – 2025 – 2030 QUANTUM TECHNOLOGIES FORECAST



Quantum Technologies | Report | www.yole.fr | ©2020

A more detailed market size assessment was made by **Yole Development** with seemingly more reasonable predictions for quantum technologies, with an increase to \$3.2B per year by 2030, with 17% average annual growth, including \$650M for hardware, \$1.37B for cloud-based software and \$785M for quantum cryptography (QKD)<sup>1231</sup>.

<sup>1227</sup> Analysis shared in [McKinsey Forecasts Quantum Computing Market Could Reach \\$1 trillion by 2035](#), April 2020.

<sup>1228</sup> IDC quarterly 2020 server market estimates: [Q1](#), [Q2](#), [Q3](#) and [Q4](#) with respectively \$18,6B, \$18,7B, \$22,6B and \$25,8B.

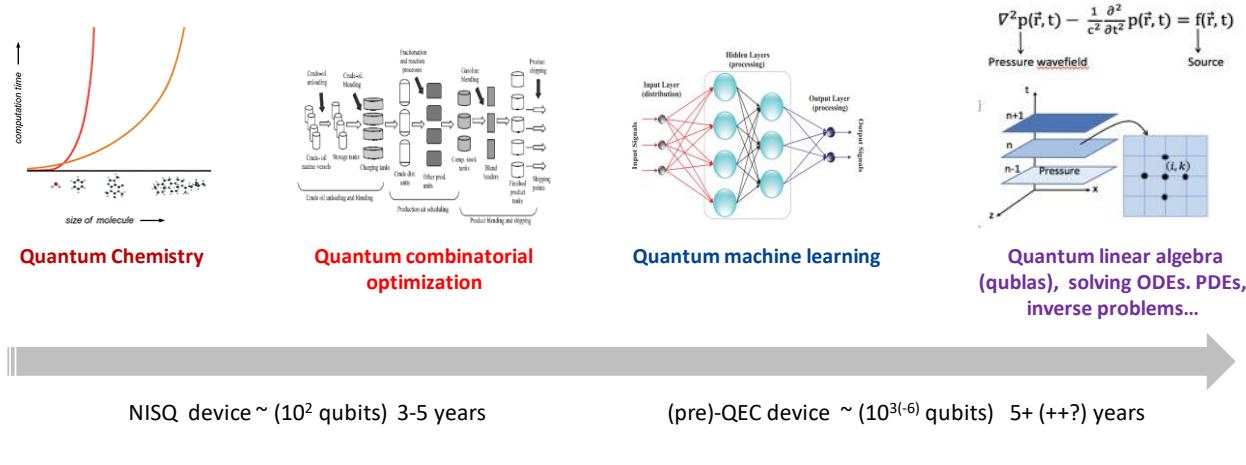
<sup>1229</sup> See [What Happens When ‘If’ Turns to ‘When’ in Quantum Computing](#), BCG, July 2021 (20 pages).

<sup>1230</sup> See [Quantum Computing as a Service Market Sizing - How we did it](#), The Quantum Daily, August 2021.

<sup>1231</sup> See [Quantum technologies: a jump to a commercial state](#), Yole Development, 2020 and their sample [Quantum Technologies Market and Technology Report 2020 -Sample](#), 2020 (22 slides).

The sensor market would grow from \$400M in 2019 to \$545M in 2030. This moderate growth seems a bit bearish since quantum sensors are the quantum objects with the lowest technological uncertainties and it is a market in its infancy.

The quantum team at **Total** constructed this interesting roadmap to provide an idea of the order in which practical quantum applications could emerge according to the number of available qubits.



Since we have no real idea of when scalable quantum computing will really work, let's try another exercise to determine the critical factors enabling some sort of technology commoditization for quantum computing:

**Technology.** The first factor is a mix of where and when we'll have first, useful quantum simulators, then useful NISQ, and then scalable **universal quantum computers** with more than a hundred logical qubits. Meanwhile, optimization solutions adapted to D-Wave's annealer will continue to be developed and may reach a point where they make a real difference with classical computing.

**Software Tools.** The second factor may be the consolidation of software development tools. These tools will continue to mature, raising their level of abstraction, and adapt to hardware evolutions. Libraries adapted to the needs of specific markets will undoubtedly consolidate, as in molecular simulation or finance. As the market matures, there will be some consolidation in this market.

**Skills.** One critical path to market growth as it's been the case for most previous major technology wave will be the availability of skilled workforce, particularly with developers. They will have, at least at the beginning, to handle abstractions levels that have nothing to do with the different forms of programming techniques that dominate today's computing, even in its event-driven programming variants that are common in the creation of websites and graphic applications. It's more an extension of the existing scientific computing community. A new generation of algorithm designers and developers will emerge. These will probably be young professionals who will have been able to digest new quantum computing concepts with a clean state mind.

**Startups.** The market will rely mostly on the fabric of startups, probably slightly ahead of traditional software publishers and IT services companies that may not necessarily venture first into this new world of quantum.

**Experience.** The first feedback from pilot projects, already underway, particularly with D-Wave, will be important. Most recent projects bring interesting learnings on the actual accelerations that quantum computing can provide. We will have to learn to make objective comparison between quantum algorithms, quantum hardware architectures and their equivalents running (or not) on supercomputers. It will also be necessary to sort out into "proof of concepts" and projects actually deployed.

**Mass impact.** At last, quantum computing commoditization will depend on the potential emergence of solutions that will have an impact on our daily lives. So, mostly consumer applications. It could come from healthcare and transportation. Who knows. Use cases will move gradually from the research community, to the corporate world, and then to consumer applications.

## Healthcare

The healthcare market, and particularly pharmaceutical industries, is one of the most sought after by quantum computing players. It is one of the vertical markets with the largest number of dedicated startups. Most major pharmaceutical companies have been exploring and evaluating the potential of quantum computing for a few years, starting by conducting a few pilot projects with D-Wave<sup>1232</sup>. The dream is to extend the capabilities of today's supercomputers to simulate living organisms molecules "in silico", mainly in order to create or discover new treatments. This is the field of "*in-silico drug discovery*".

This quest is linked to the pharmaceuticals industry worrisome situation, that is discovering fewer new treatments and seeing diminished portfolio of commercial patented drugs. The drugs development cycle from discovery to market is becoming increasingly expensive, particularly during clinical trials. It costs up to a \$1B, if not more, and failure rates are numerous. 45% of cancer therapies clinical trials fail in phase III in the USA, and 97% of the new therapies tested are not approved by the FDA in the USA! If we could better digitally simulate the effects of new treatments before clinical trials, we might be able to increase these success rates. Also, quantum computing could be a critical tool to create digital twins of molecular complexes, used to find the right combinations and optimize their efficiency.

On top of new drugs discovery, pharmaceutical companies are also trying to leverage their existing portfolio with drugs re-targeting. It can speed up clinical trials since their adverse effects are already known. Even though this has not prevented the long controversy surrounding hydroxychloroquine in 2020! In any case, pharmaceutical players need simulation tools and in particular molecular simulation tools: to create molecules, from the simplest (peptides) to the most complicated (proteins, antibodies, vaccines), to model them in 3D, to analyze their interactions between their active sites and targets like cell surface proteins (transmembrane glycoproteins)<sup>1233</sup>, and also to identify contraindications. Such treatments can be created ex-nihilo, but most often, they are derived from existing ones (known protein, enzyme, bio-inspiration, ...).

Molecular simulations are based on the broad field of computational chemistry. It originated with the description of the nature of chemical bonds by **Linus Pauling** in 1928, which launched the vast field of quantum chemistry. Chemical bonds describe the way electrons of covalent liaisons are shared between atoms and the shape of their related orbitals.

Pauling's work came just after the creation of the **Born-Oppenheimer** approximation in 1927<sup>1234</sup> which simplified Schrödinger's equation for a molecule by separating the nuclei of the atoms from their electrons. The same year, **Llewellyn Thomas** (1903-1992, English) and **Enrico Fermi** (1901-1954, Italian-American) created the later-called Thomas-Fermi model which describes the electronic structure of multi-atoms systems.

The field of computational chemistry began much later, in 1964, with the creation of the two Hohenberg-Kohn theorems by **Walter Kohn** (1923-2016, Austrian then American) and **Pierre Hohenberg** (1934-2017, French-American).

---

<sup>1232</sup> Like Abbvie, Amgen, AstraZeneca, Bayer, Biogen, Bristol-Myers Squibb, Johnson&Johnson, Merck, Roche, Sanofi and Taleda.

<sup>1233</sup> We could try to digitally simulate an entire cell with all its organelles. This would become quite complicated since a living cell comprises about 100 trillion atoms!

<sup>1234</sup> The Max Born from the probabilistic explanation of Schrödinger's equation and the Robert Oppenheimer from the atomic bomb.

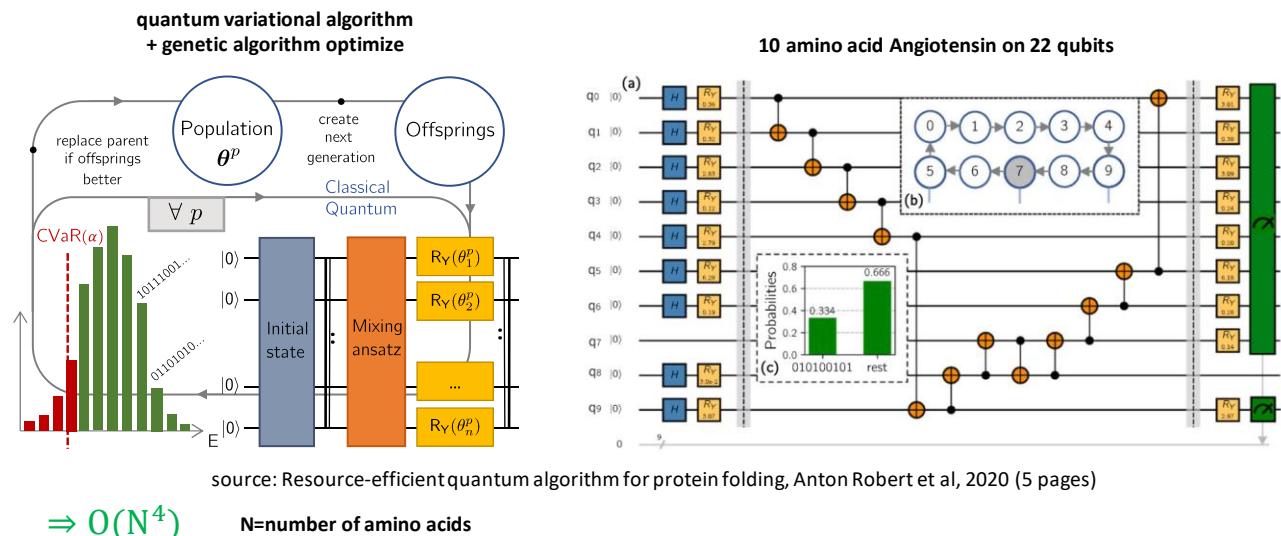
This was closely followed by **Kohn-Sham**'s equations from **Lu Jeu Sham** (1938, Chinese) in 1965. They are the basis of **DFT** (Density Functional Theory), a mathematical model that describes the structure of molecules at rest as a function of inter-atomic interactions and the structure of their electron clouds, and in a simpler way than with Schrödinger's equation which manipulates too many variables. Walter Kohn was awarded the Nobel Prize in Chemistry in 1998 for this work, along with **John Pople** (1925-2004, English) who had contributed to the modeling of electronic orbitals in molecules.

DFT was followed by the work of **Martin Karplus** (1930, American), **Michael Levitt** (1947, Israeli-American) and **Arieh Warshel** (1940, Israeli-American) who contributed to the digital modeling of chemical reactions in the 1970s. They were awarded the Nobel Prize in Chemistry in 2013 for their work. The DFT model was also simplified by **Axel Becke** (1953, Canadian) in 1993 with the hybrid DFT.

Molecular simulation faces quasi-quantum effects related to the continuous vibrations of molecules in their aqueous medium. Chemical bonds oscillate at a femto-second rate, atoms vibrate collectively at a one picosecond rate. On the other hand, more complex chemical processes such as the production and folding of proteins occur on scales ranging from micro-seconds to seconds.

The Holy Grail would be to understand how the assembly and then operations of ribosomes work. These molecular complexes are made of 73 proteins and 4 large RNA molecules. Ribosomes produce all proteins in our cells using messenger RNA code, which is itself synthesized from DNA through an also amazing biochemical process involving many complex molecules. Thousands of ribosomes operate in every living cell and each ribosome is made of about 250,000 atoms<sup>1235</sup>.

One of the most recent protein folding algorithm was able to simulate the folding of the 10 amino acid Angiotensin on 22 qubits. The same method was also applied to folding a 7 amino acid neuropeptide using 9 qubits, all on an IBM quantum computer<sup>1236</sup>.



Today, most molecular simulation calculations are carried out using algorithms running on classical supercomputers, increasingly using GPGPUs such as those from Nvidia or Google's TPUs.

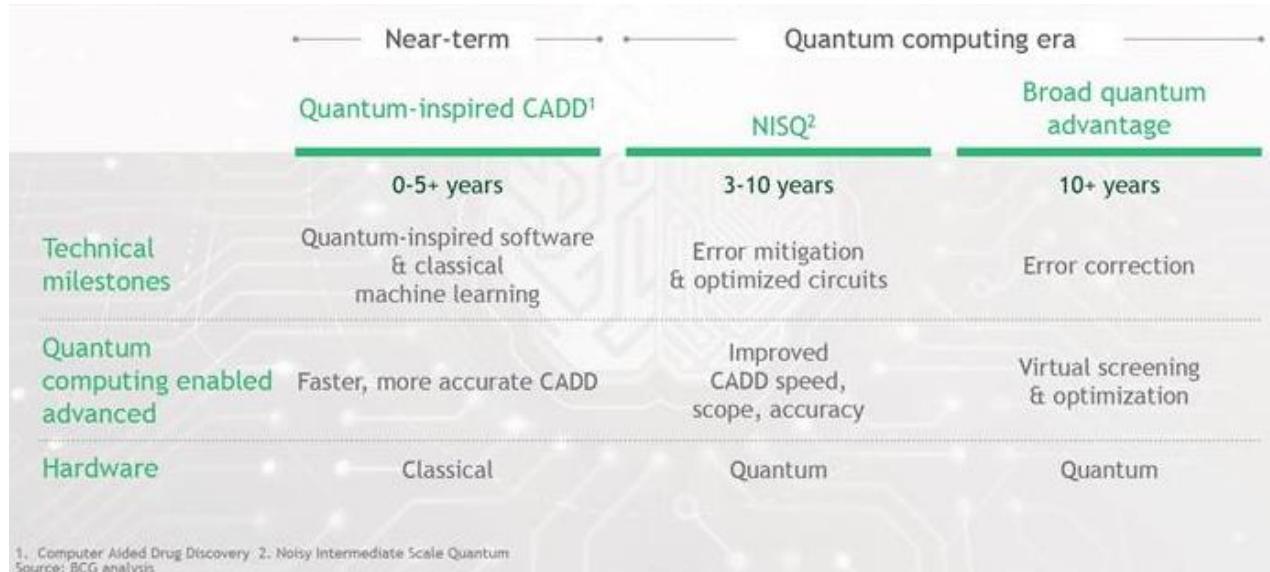
<sup>1235</sup> The number of 2.5 or 3.5 million atoms is often mentioned, but this is not true. These are "Daltons" which are equivalent to one twelfth of the mass of carbon 12, or about the mass of a hydrogen atom. However, these organic molecules contain, in addition to hydrogen, a lot of carbon, nitrogen, phosphorus and oxygen. The latter contribute to a large part of the mass of the molecule, hence the fact that the number of daltons must be divided by 10 to obtain the number of atoms of an organic molecule.

<sup>1236</sup> See [Resource-efficient quantum algorithm for protein folding](#) by Anton Robert et al, 2021 (5 pages).

Another test was published in 2021 by GSK<sup>1237</sup>. It was about solving a mRNA codon optimization problem. Each amino acid in a protein sequence can be encoded by as many as six different codons, these series of three DNA/RNA bases encoding one amino acid. The goal was to find the right combination of these codons. The codon selection in mRNA impacts protein folding and functions. The main task is to balance G and C bases in mRNA to optimize gene expression. This was one of the first published case studies using D-Wave Advantage annealer and its 5000 qubits and their Leap Hybrid Solver. It worked well with 30 amino acids and could scale up to 1000 amino acids.

The codon optimization problem is formulated as a Binary Quadratic Model that is itself close to an Ising model adapted to D-Wave annealers. It did fare well when compared to genetic and machine learning algorithms running on classical computers.

The first small-scale tests of simulation using quantum algorithms were done on D-Wave and superconducting qubits accelerators. However, the most common approach is based on hybrid algorithms associating HPCs and quantum accelerators.



Quantum simulators are also machines suitable for simulating the interaction of atoms within molecules. BCG is thus presenting molecular simulation roadmaps spread out over time and following the rate of evolution of quantum computers between today's NISQ (intermediate-size noise computing) and LSQ (large scale quantum computing)<sup>1238</sup>.

One approach consists in relying on generic frameworks that can be distributed over classical computing in massively parallel architecture, and then progressively over quantum computing. This is the case of the **Tinker-HP** framework co-created by Jean-Philip Piquemal, co-founder of **Qubit Pharmaceuticals** and that the company plans to extend with hybrid quantum algorithms<sup>1239</sup>.

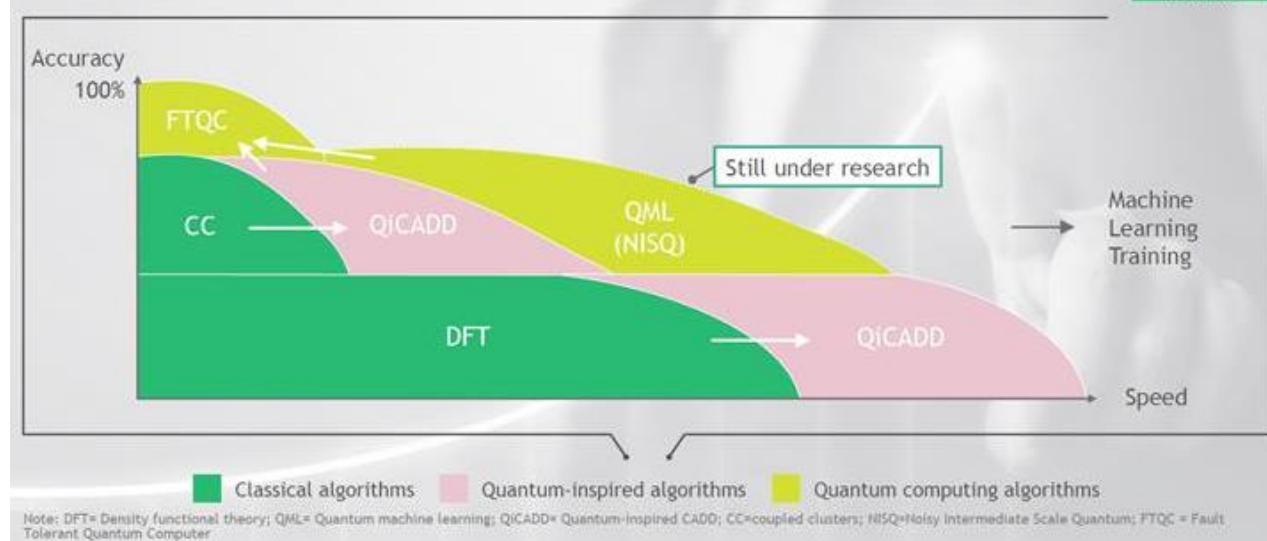
<sup>1237</sup> See [GlaxoSmithKline Marks Quantum Progress with D-Wave](#) by Nicole Hemsoth, February 2021 pointing to [mRNA codon optimization on quantum computers](#) by Dillon M. Fox et al, February 2021 (35 pages).

<sup>1238</sup> See [Will Quantum Computing Transform Pharma R&D](#) by Jean-Francois Bobier, April 2020 (14 slides) and the written version [Will Quantum Computing Transform Biopharma R&D?](#) by Jean-Francois Bobier et al, December 2019. This is the source of the diagrams on this page.

<sup>1239</sup> See [Computational Drug Design & Molecular Dynamics](#) by Jean-Philip Piquemal, April 2020 (28 slides) and [Tinker-HP: a massively parallel molecular dynamics package for multiscale simulations of large complex systems with advanced point dipole polarizable force fields](#) by Louis Lagardère, Jean-Philip Piquemal et al, 2018 (17 pages). The company plans to rely first on cold-atoms simulators like those from Pasqal.

# Quantum breaks speed vs accuracy trade-off

Illustrative



Most other quantum startups like **ApexQubit**, **HQS Quantum Simulations**, **MentenAI**, **ProteinQure** and **Qulab** are indeed adopting hybrid computing models, if only to have something practical to market<sup>1240</sup>. The most common hybrid method is the VQE (Variational Quantum Eigensolver)<sup>1241</sup>.

Another method is being developed to create quantum inspired algorithms, *aka* classical algorithms based on quantum algorithms<sup>1242</sup>.

Quantum and quantum inspired computation complete the vast field of machine learning which is already very common in the discovery of therapeutic molecules<sup>1243</sup>.

Molecules simulation can start with simple organic molecules like cholesterol up to protein folding which is many orders of magnitude more complex<sup>1244</sup>. This last feat is therefore bound to be a very long-term one.

Today, we can simulate peptides with about ten amino acids. The best algorithms require a number of qubits that evolves according to the power 4 of the number of amino acids<sup>1245</sup>. This simulation is also at the limit of feasibility in terms of complexity because it is in the class of NP-Complete problems as seen in the section dedicated to complexity theories, starting on page 485.

<sup>1240</sup> See [Can Quantum Computing Play a Role in Drug Discovery? At least one Startup Thinks so](#) by James Dargan, 2020, which mentions Menten AI.

<sup>1241</sup> See [Quantum Chemistry and the Variational Quantum Eigensolver](#) by S Kokkelmans et al, December 2019 (56 pages).

<sup>1242</sup> See [Quantum and Quantum-inspired Methods for de novo Discovery of Altered Cancer Pathways](#) by Hedayat Alghassi et al, 2019 (27 pages)

<sup>1243</sup> See [Concepts of Artificial Intelligence for Computer-Assisted Drug Discovery](#) by Xin Yang et al, 2019 (75 pages). A good summary paper with 879 bibliographical references!

<sup>1244</sup> See [Designing Peptides on a Quantum Computer](#) by Vikram Khipple Mulligan, September 2019 (20 pages) which presents Rosetta, a protein quantum design tool running on D-Wave.

<sup>1245</sup> See [Resource-Efficient Quantum Algorithm for Protein Folding](#) by Anton Robert et al, August 2019.

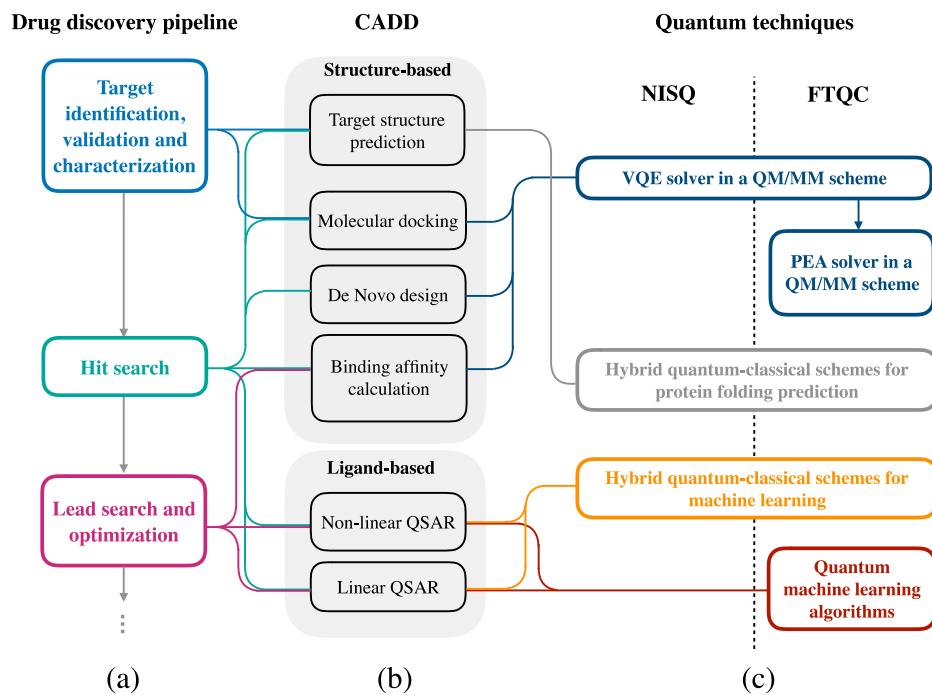


Fig. 1. (a) General workflow of drug discovery process. Here we focus on the early phase where computationally intensive quantum chemical analyses are involved. (b) Components of each stage of drug discovery that heavily involve quantum chemistry or machine learning techniques. (c) Quantum techniques that can be applied to the components listed in (b) and potentially yield an advantage over known classical methods. Here we make the separation between techniques for noisy intermediate scale quantum (NISQ) devices [21] and fault-tolerant quantum computing devices.

78% of the search for therapies is focused on light molecules of less than 900 Daltons, i.e. about a hundred atoms. Its function is to associate itself with a target in the cells, often a specific protein that controls a metabolism that we want to attenuate or amplify<sup>1246</sup>. The discovery of small molecules of a few dozen atoms could be within the scope of the NISQ quantum computers within a few years. The first molecular simulation experiments were carried out on D-Wave. They work with the search for energy minima, which can be suitable in theory for the simulation of the organization of molecules.

A collaboration was launched in June 2017 between **Biogen**, the Canadian quantum software company **1QBit**, and **Accenture** for the creation of new molecules. **Biogen** (1978, USA) is a mid-size biotech company with 7300 employees specialized in the treatment of neurodegenerative diseases and leukemia.



Their use of quantum computing was aimed at retargeting therapeutic molecules, looking for matching between existing treatments and therapeutic targets in neurodegenerative or inflammatory diseases. **Amgen** is also active in the search for new therapies and is working since 2020 with **QSimulate** (2018, USA).

A similar project was launched in Spain with the consortium “QHealth: Quantum Pharmacogenomics applied to aging” launched in August 2020 with **aQuantum** (alhambraIT, Prologue Group) with **Gloin, Madrija** and various Spanish Universities. Its goals are to find correlations between physiological and genetic variables, drug usage history, side effects and/or potential lack of response of new drugs to fight aging. They plan to do simulations using quantum algorithms. The project totals 5.1M€ including a grant of 3.7M€ from CDTI awarded in November 2022 by the **Center for the Development of Industrial Technology (CDTI)** of the Ministry of Science and Innovation of Spain.

<sup>1246</sup> See [Potential of quantum computing for drug discovery](#) by Alan Aspuru-Gusik et al, 2018 (18 pages). CADD = Computer Aided Drug Design. The schema on drug discovery pipeline / CADD / quantum techniques comes from this source.

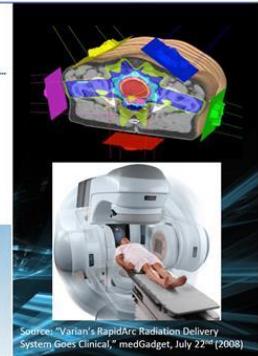
In June 2019, **Merck** announced a three-year partnership with the Karlsruhe, Germany-based startup **HQS Quantum Simulations** for the development of quantum algorithms for chemical simulation.

Still on D-Wave quantum annealing computers, an application of radiotherapy optimization was experimented (*opposite*).

The principle consists in minimizing patients' exposure to X-rays while optimizing their efficiency. It is a complex problem of simulating the diffusion of electromagnetic waves in the human body.

### Case Study: Radiotherapy Optimization

<b>PROBLEM:</b>	Deliver lethal dose to tumor whilst minimizing damage to healthy tissues
<b>APPROACH:</b>	<b>Hybrid:</b> QC + Conventional Computer <ul style="list-style-type: none"> <li>• Radiation treatment plan = bit string</li> <li>• Quality = result of running extensive radiation transport simulation</li> <li>• Results of radiation transport simulations drive adjustments to plan</li> </ul>
<b>IMPACT:</b>	<ul style="list-style-type: none"> <li>• Hybrid quantum-classical design found a radiation therapy treatment that minimized the objective function to 70.7 c.f. 120.0 for tabu, and ran in 1/3 the time making fewer calls to radiation transport sim.</li> </ul>



Sources: "Varian's RapidArc Radiation Delivery System Goes Clinical," medGadget, July 22<sup>nd</sup> (2008)

D-WAVE  
The System Defining Quantum Computing

Copyright © D-Wave Systems Inc.

27

David Sahner, who created his own consulting firm **Eigenmed**, is one of the promoters of precision medicine based on predictive machine learning techniques using D-Wave annealers<sup>1247</sup>.

**Omnicom Healthcare** did not hesitate to promote in 2017 the use of quantum computing in healthcare in a white paper containing strictly no relevant information on the subject, especially since they seem to confuse machine learning applications analyzing data from connected objects with the ability of quantum computers to manage problems that are intractable by traditional computers<sup>1248</sup>.

The **DNA-Seq Alliance** combines the startup DNA-Seq and D-Wave, which also does molecular retargeting by combining genomics, protein kinase crystallography, quantum computing and the search for effective cancer treatments.

Let's also mention that quantum computing, both annealing and gate-based, could be used to accelerate **DNA sequencing**, particularly in de-novo mode, when no existing DNA mapping exists. It's about reconstructing a giant puzzle with small parts of DNA sequences which come out of sequencing<sup>1249</sup>.

As with any new technology, quantum computing specialists must learn to interact with bioinformatics specialists. Fortunately, bioinformaticians are already bridging the gap between molecular biology and computer science and are well positioned to learn quantum methods<sup>1250</sup>.

Finally, the covid-19 pandemic has led to a renewed interest in quantum computing. Several market players have put the cart before the horse in this respect. D-Wave has thus offered some of its machine time in the cloud for researchers in the field.

A couple tests were run in 2020 using D-Wave and IBM systems. In one case performed by Turkish scientists to classify CT scans images<sup>1251</sup>. Their quantum software generated 94% to 100% success-

<sup>1247</sup> See [Predictive Health Analytics](#) by David Sahner, 2018 (54 slides).

<sup>1248</sup> See [Exponential Biometrics: How Quantum Computing Will Revolutionize Health Tracking](#), 2017 (7 pages).

<sup>1249</sup> See [QuASeR - Quantum Accelerated De Novo DNA Sequence Reconstruction](#) by Aritra Sarkar et al, TU Delft, April 2020 (24 pages).

<sup>1250</sup> See [Thirteen tips for engaging with physicists, as told by a biologist](#) by Ken Kosik, January 2020 which describes how to bring physicists and biologists together.

<sup>1251</sup> See [COVID-19 detection on IBM quantum computer with classical-quantum transfer learning](#) by Erdi Acar and Ihsan Yilmaz, November 2020 (16 pages).

ful classifications while its classical counterpart did achieve 90% successful results. It was using only 4 qubits from 5-qubits systems (IBM Q-Rome and Q-London).

It was a hybrid computing using the quantum transfer learning method. Quantum computing was used only for the classification part at the end of a convolutional network, not for the convolutions that remain classical, using 224x224 pixels versions of the CT scans, using a training set made of 2658 lung CT images with 1296 COVID-19 and 1,362 Normal CT images. They also tried emulators running with PennyLane, Qiskit and Cirq. The classification layer compressed 512 vectors into 4 vectors with a linear transformation.

Another test related to covid-19 research used a quantum assisted SVM classification using 16 qubits running on the IBM Q-Melbourne system and implementing feature mapping and hyperplane calculation with a variational quantum classifier<sup>1252</sup>. Classification was using time series of number of cases per counties in the USA. The classical part was done using the scikit-learn framework from Inria, France. Well, in the end, the research team observed that classical methods outperformed QML in accuracy, particularly with a high number of data points (>300).



cancers classification

multi-omics: genomics + symptoms in QML

source: D-Wave



liver donor optimization

NP-complet complete problem using QUBO

source: Accenture, D-Wave



radiotherapy optimization

to minimized x-ray dose

source: Roswell Park, D-Wave



de-novo proteins and polypeptides creation

with hybrid computing, tests in research against the covid-19 virus.

source: D-Wave



drug retargeting

with Biogen, 1QBit and Accenture research

source: D-Wave



cancer diagnosis

quantum rule based to diagnose and treat invasive ductal carcinoma (breast cancer type)

source: Atos

In practice, conventional HPCs helped molecules screening for therapies and to create 3D models of the covid virus and, in particular, of its glycoproteins that cling to the membranes of human cells in order to attack them and enable virus reproducing within cells<sup>1253</sup>. In the more or less distant future, quantum computing will probably have its say in similar pandemics<sup>1254</sup>.

## Energy and chemistry

When we move away from organic molecules and living organisms, everything suddenly becomes almost realistic in quantum computing! Indeed, the molecular structures that we want to study and simulate here are generally simpler than with organic chemistry of living organisms<sup>1255</sup>.

<sup>1252</sup> Another one: [Quantum-Enhanced Machine Learning for Covid-19 and Anderson Insulator Predictions](#) by Paul-Aymeric McRae and Michael Hilkea, December 2020 (25 pages).

<sup>1253</sup> See an example in [TACC Supercomputers Run Simulations Illuminating COVID-19, DNA Replication](#), March 2020.

<sup>1254</sup> See [Covid-19: Quantum computing could someday find cures for coronaviruses and other diseases](#) by Todd R. Weiss, April 2020.

<sup>1255</sup> See [Enabling the quantum leap Quantum algorithms for chemistry and materials Report](#), January 2019 (115 pages) which provides a good overview of chemical simulation methods. It is a report of a workshop organized by the NSF.

The first plausible applications deal with the creation of innovative materials. The energy and chemistry sectors are interested in solving complex analysis and optimization problems, in the in-silico simulation of crystalline molecules and structures, and in creating new materials<sup>1256</sup>. The first case studies were, not surprisingly, first carried out with D-Wave's annealers.

These seem to be well suited for simulations of atomic interactions in materials even though the provided accelerations are not stellar.

Simulations can also be with air, water and other liquid flows, and in particular their turbulence. In particular, they can exploit the famous Navier-Stokes equations<sup>1257</sup>.

In September 2017, **IBM** simulated on a 16-qubit superconducting quantum computer a set of [be-ryllium hydride molecules](#) and their minimum energy balance, which is not useful in itself, but is a good start<sup>1258</sup>.

Research is well underway to create batteries that are more efficient in terms of energy density and charging speed<sup>1259</sup>. Simulation is most often used to understand the operations of the chemical reactions taking place on cathodes and anodes and in particular in the crystalline intercalation structures and to find ways to improve energy density and avoid battery wear phenomena. This is one of Volkswagen's lines of research, which plans to do this eventually with Google's quantum computers as documented in this [November 2017 announcement](#).

Quantum sensing can also help develop new batteries. That's what **AMTE Power** (UK) is doing with leading the 3 years Project Quantum to use quantum sensing to develop lithium-based battery manufacturing solutions, which got a funding of £5.4M from Innovate UK. This project is about using NV center-based magnetic quantum sensing to evaluate the battery aging process<sup>1260</sup>.

Carbon capture is another issue and researchers are simulating its molecular functioning by biomimicry. This is an application area put forward by Microsoft researchers.

At the German chemist **BASF**, the idea is to simulate synthetic polymers, first on HP supercomputers, then eventually on quantum computers. Since 2017, **Dow Chemicals** has been collaborating with the Canadian software publisher **1Qbit** to create new molecules based on D-Wave.

**BP** is working on the design of algorithms for optimizing oil exploration. This involves using data from various sensors, particularly seismic sensors, to consolidate models for simulating geological layers under the ground. They joined in 2020 the **IBM Quantum Network** as an industry partner to get access to IBM's 65-qubit quantum computer, software and experts. It follows **ExxonMobil** who entered the program in 2019 as one of the major companies associated with IBM.

In 2019, the **Dubai Electricity and Water Authority** (DEWA) was working with Microsoft to solve complex power and water distribution problems. It was just a matter of testing a few algorithms on Intel simulators running on Azure. And for good reason, Microsoft did not yet have its own quantum computer<sup>1261</sup>. In 2020, DEWA announced that it would train their algorithms in D-Wave annealers<sup>1262</sup>!

---

<sup>1256</sup> See [Quantum hardware calculations of periodic systems: hydrogen chain and iron crystals](#) by Kentaro Yamamoto et al, September 2021 (13 pages) with some potential applications in steel manufacturing.

<sup>1257</sup> See [Quantum Navier-Stokes equations](#) by Pina Milišić from the University of Zagreb, 2012 (12 pages) and [Navier-Stokes equations using Quantum Computing](#), July 2020.

<sup>1258</sup> See [Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets](#), October 2017 (22 pages).

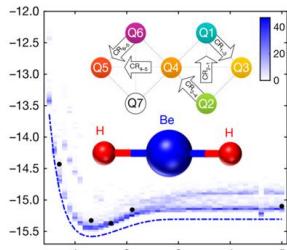
<sup>1259</sup> See [The Promise and Challenges of Quantum Computing for Energy Storage](#) (4 pages).

<sup>1260</sup> See [AMTE Power's Project Quantum Signals New Era of British Battery Manufacturing](#), September 2020.

<sup>1261</sup> See [Microsoft and DEWA bringing quantum computing to Dubai](#), June 2018.

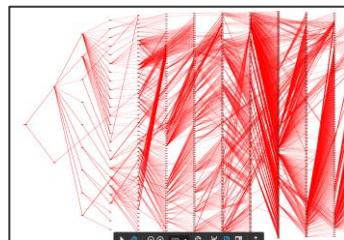
<sup>1262</sup> See [DEWA organises training sessions on quantum computing in partnership with D-Wave](#), February 2020.

### material ageing modelling



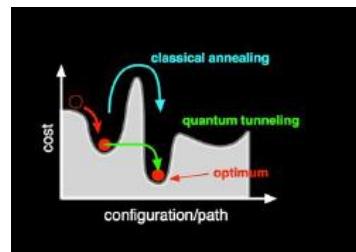
- Modelling ageing phenomena's with quantum physic laws.
- Stake : foresee material ageing patterns to gain operational margin.
- Contribute to regulatory studies for ASN IRSN

### safety probabilistic study



- Decision support tool for real time risk analysis
- Recalculate risk based on operation current state and maintenance operation
- Avoid roll back in case unintended events

### combinatorial Optimization for energy management



- Smart charging : optimizing VEs charging for the grid operator/charging operator/user Decentralized energy systems, exploiting large data volume

source : EDF, QCB Conference, 20 juin 2019

**Total** is one of France's leading industrial companies to take a very close interest in the uses of quantum computing. They also want to optimize the prospecting and evaluation of reserves using seismic probes. They plan to address complex optimization problems such as **MINLP** (Mixed Integer Non-Linear Programming<sup>1263</sup>) to optimize refining, planning, production and transportation. Finally, they are also interested in quantum chemical simulation.

The company has a team of about 12 researchers and engineers invested in quantum computing applications, mostly docs and post-docs<sup>1264</sup>. They announced a partnership with **CQC** (UK) in 2020 to develop carbon capture solutions<sup>1265</sup>.

Other industrialists are also experimenting with quantum computing. **Dow Chemical** has been a **1Qbit** partner since June 2017 for pilot projects in quantum chemical simulation. **BP** is interested in applications of quantum cryptography (QKD) with **IDQ**.

Finally, **Mitsubishi Chemical** and the **Materials Magic** subsidiary of **Hitachi Metals** are also testing quantum computing with **IBM**<sup>1266</sup>.

<sup>1263</sup> A version of the MINLP problem solving algorithm exists for D-Wave via their QUBO framework. See [QuantumComputing and Non-Linear Integer Optimization](#) by Sridhar Tayur February 2019 (42 slides).

<sup>1264</sup> Total has partnered with private players (IBM, Atos, Rigetti QC Ware, Google) and various research laboratories around the world: PCQC (Paris), LIRMM Montpellier, CERFACS, Université ParisSud, Jülich Forschungszentrum (Germany) and the University of Leiden.

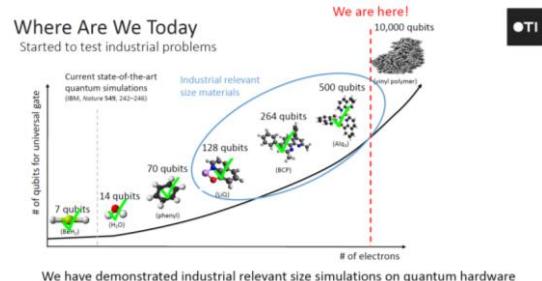
<sup>1265</sup> See [CQC and Total Announce Multi-Year Collaboration to Develop Quantum Algorithms for Carbon Capture, Utilization and Storage \(CCUS\)](#), April 2020 and [Total Exploring Quantum Algorithms to Improve CO2 Capture](#), May 2020.

<sup>1266</sup> See [Quantum computing for energy systems optimization: Challenges and opportunities](#) by Akshay Ajagekar and Fengqi You, 2020 (34 pages).

fertilizer production optimization  
Haber-Bosch cycle optimization  
nitrogenase and ferrodoxine  
*source: Microsoft*

## OTI Lumionics

**new OLED design**  
Alq<sub>3</sub> simulation, used in OLED  
*source: D-Wave, OTI*



Humans: Haber-Bosch process,  
 $N_2 + 3 H_2 \rightarrow 2 NH_3$ , 500°C, 20 MPa  
Consumes 2% of world energy

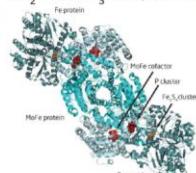


2013 Waco, Texas  
fertilizer plant explosion



Fertilizer sales in 2006:  
\$72,000,000,000

Nature: Nitrogenase  
aka "MNIST for QNNs"  
 $N_2 + 3 H_2 \rightarrow 2 NH_3$ , 25°C, 0.1MPa



Fe<sub>4</sub>S<sub>4</sub> center cannot be  
simulated (168 qubits)

We have demonstrated industrial relevant size simulations on quantum hardware



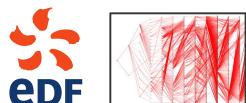
**synthetic enzyme design**  
directly estimate redox potentials  
*source: QcWare*

**EDF** is another major French company that is studying the use cases of quantum computing very closely: quantum new materials simulations, material aging simulations particularly under radiations, safety statistics, combinatorial optimization for smart grids and battery management and also customer segmentation using quantum Machine Learning.



**TotalEnergies**

**carbon capture**  
simulating interaction between CO<sub>2</sub> molecule and  
new complex materials to enable its storage, using  
MOFs (metal-organic frameworks like Al-Fu)  
*source: Atos, TotalEnergies, CQC*



**safety probabilistic study**

decision support tool for real time risk  
analysis, recalculates risk based on operation  
current state and maintenance operation,  
avoids roll back in case unintended events  
*source: EDF*



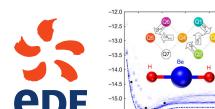
**battery simulation**  
lithium-oxygen  
*source: IBM*



**battery simulation**  
simulating magnetism and spins  
*source: Samsung, Honeywell*



**battery simulation**  
lithium-sulfur battery design  
*source: IBM*



**material ageing modelling**  
modelling ageing phenomena's with  
quantum physic laws, foresees material  
ageing patterns to gain operational margin.  
*source: EDF*

## Transportation and logistics

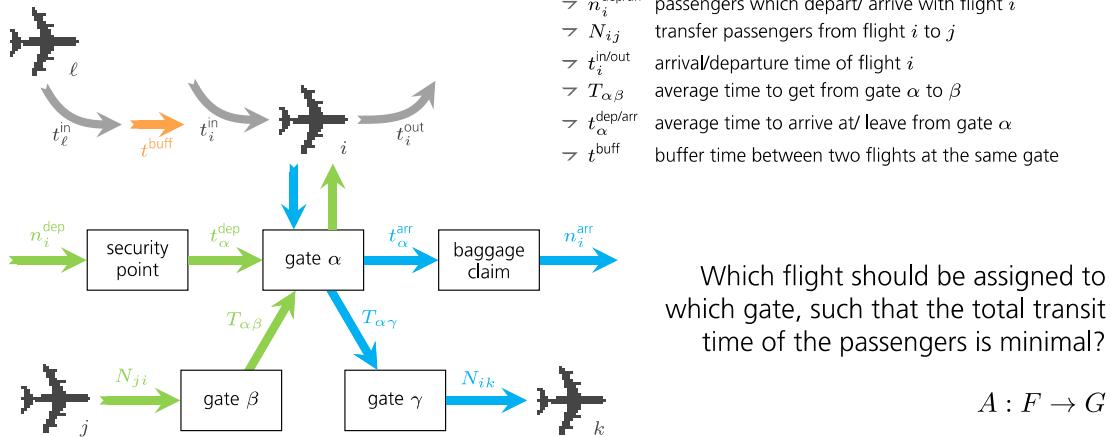
Beyond energy matters mentioned above, transportation industries are mainly interested in algorithms for optimizing complex systems<sup>1267</sup>. Let's look at what can be done with air, maritime and ground transportation.

With airlines, the current focus about optimizing aircraft fleets planning, to maximize the capacity to meet demand while optimizing the aircraft fill rate.

<sup>1267</sup> See this inventory of needs, but no solutions in [Quantum Applications Transportation and Manufacturing](#) by Yianni Gamvros, IBM, 2017 (20 slides).

Also, quantum computing can enable optimizing airport and aircraft gates management, in order to minimize passenger waiting time, as tested by **DLR** in Germany<sup>1268</sup>. This is an NP-difficult problem that is difficult to deal with using conventional algorithms.

## Passenger Flows



Another experiment was done by **Ferrovie dello stato Italia** to optimize train arrivals in railways stations, also in order to minimize passengers connection times, again with D-Wave.

In Japan, **Sumitomo** launched in June 2021 a pilot experiment for optimizing flight routes for urban air mobile vehicles (air taxis and unmanned drones). They will rely on resources from Tohoku University. No precision on the problem sizing and on which quantum system they plan to pilot their solution even if D-Wave is a logic contender.

Researchers from **Chalmers University** in Sweden prototyped a promising QAOA hybrid algorithm solving the “tail Assignment problem”, which is the task of assigning individual aircraft to a given set of flights, minimizing the overall cost for the airline. They said it worked with only 2 qubits, to optimize 2 flights and would scale well as flights are added<sup>1269</sup>.

These are needs that can be addressed both by machine learning algorithms to take into account the past or with quantum optimization algorithms based on a description of the parameters of the problem. The former does prediction and the latter simulation. Simulations avoids the back-mirror bias that can be induced by prediction methods based on past data. A combination of the two methods is possible.

**Airbus** is also involved in quantum. In 2015, one of their teams based in Newport in the United Kingdom began working on the subject. In 2016, the aircraft manufacturer invested in the American startup QC Ware. They experimented with the use of a D-Wave for fault tree analysis (FTA), which is used to determine the origin of complex failures with a gain of a factor of 4 compared with traditional methods.

<sup>1268</sup> See [Flight Gate Assignment with a Quantum Annealer](#) by Elisabeth Lobe and Tobias Stollenwerk of the German Aerospace Center (or DLR for Deutsches Zentrum für Luft- und Raumfahrt e.V.), March 2019 (15 slides). The case study uses a D-Wave. It shows that the solution is not obvious to develop.

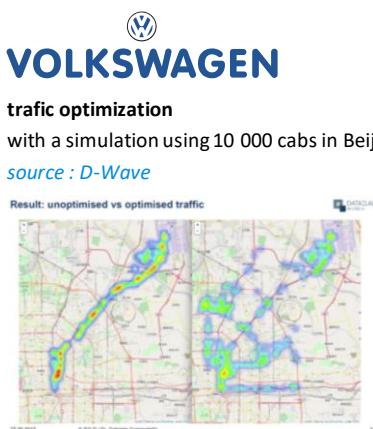
<sup>1269</sup> See [Two-Bit Quantum Computer Solves Real Optimization Problem](#) by Matt Swayne, December 2020 pointing to [Applying the Quantum Approximate Optimization Algorithm to the Tail-Assignment Problem](#) by Pontus Vikstål et al, September 2020 (11 pages).

This is a difficult NP-difficult combinatorial problem that is easier to solve in quantum programming. In January 2019, Airbus launched its "Quantum Computing Challenge", a way to outsource the development of quantum solutions to help them solve their business problems, in fluid mechanics, differential equations, flight optimization, wing design, cargo bay filling, etc.<sup>1270</sup>. As of May 2019, 475 teams from 57 countries had competed in this challenge. They came mainly from the USA and India, followed by Europe. They announced the challenge results in October 2020 with five finalists selected out of 36 contestants.

One team from **Capgemini** devised a new hybrid matrix inversion algorithm mixing the famous HHL algorithm and a QSVM (Quantum-enhanced Support Vector Machine (QSVM). Other teams worked on plane loading optimization problems, on quantum machine learning models and on fluids dynamics applied to aircraft design.

Back on the ground, the deployment of autonomous vehicles fleets is also a nice target application for quantum computers. The more autonomous the vehicles are, the greater the need for automation and route coordination. The problems to be solved will be to determine step-by-step the vehicle fleet routes in order to optimize each of these vehicles and passengers the travel time.

This was an experiment done in 2017 by **Volkswagen** on D-Wave annealers. Its goal was to optimize the routes of a (virtual) cab fleet in Beijing<sup>1271</sup>. The experiment was using the [T-Drive data set](#) published by Microsoft in 2008 which describes the routes of 10,357 cabs. The algorithm used was QUBO (Quadratic Unconstraint Binary Optimization). The diagram below shows the result of the optimization of the route of 418 cabs making the journey from the city center to the airport taking into account the route of 10,357 vehicles<sup>1272</sup>.



**vehicle recommandation**  
hybrid computing  
*source : D-Wave,*  
**painting planning optimization**  
*source : D-Wave*

**accenture**  
trucks routing  
trucks routing optimization  
*source: Accenture, D-Wave*

**DENSO**  
fleet optimization  
Denso and Toyota, presented at CES 2017 on Denso booth.  
*source: D-Wave, Denso*

**ExxonMobil**  
containers shipment optimization  
using VQE, MIP, QUBO  
*source: IBM, ExxonMobil*

**FERROVIE DELLO STATO ITALIANE**  
trains station optimization  
to reduce passengers connecting time  
*source: D-Wave*

**DLR**  
aircraft gate allocation in airports  
to minimize passagers transit time  
*source: DLR, D-Wave*



There is a lack of hindsight in estimating the size of quantum computers needed to practically handle such large-scale problems. How many qubits would be needed to optimize a fleet of hundreds or even millions of autonomous vehicles? Volkswagen also experimented small-scale algorithms with D-Wave for optimizing vehicle recommendations and also optimizing cars painting planning.

<sup>1270</sup> See [Airbus gets aerodynamic with quantum computing](#) by Michael Feldman, January 2019.

<sup>1271</sup> It is documented in [Quantum Computing at Volkswagen Traffic Flow Optimization using the D-Wave Quantum Annealer](#), 2017 (23 slides).

<sup>1272</sup> The results are published in [Traffic flow optimization using a quantum annealer](#), August 2017 (12 pages). As with many case studies from D-Wave, this one is also contested by HPC specialists.

**Daimler AG** is one of the leading companies working on quantum technology with IBM, with applications for logistics and planning optimization and everything to do with autonomous vehicle routing at the forefront. In 2018, they also launched an initiative with IBM to develop lithium-sulfur batteries, which improve energy density and make it possible to do without metals such as cobalt and nickel. All of this will be achieved through quantum simulation.

**BMW** is also willing to learn how to use quantum computing in various tasks, one being the optimization of its spare parts supply chain. They are partnering with Honeywell to do this as well as with Cambridge Quantum Computing, Zapata Computing and Entropica Labs. They started using the Honeywell trapped ions-based H0 and H1 with 10 qubits.

They used a Recursive Quantum Approximate Optimization Algorithm (R-QAOA) to manage their combinatorial problem. The quality of these trapped ions qubits made the trial promising although of course not usable at all given the small number of available qubits<sup>1273</sup>.

At last, maritime containers shipment is also a center of interest. **DP World**, the Dubai Port operator, is partnering with **D-Wave** to find ways to use quantum computing to optimize their port operations. At this stage, it's just exploratory work with no details at all about envisioned applications. The ones that are easy to guess are containers loading/offloading optimizations<sup>1274</sup>.

**ExxonMobil** and **IBM** are also working on finding algorithms to optimize maritime traffic routing. Existing solutions rely on heuristics and simplifications. They were willing to see whether quantum computing could transform these complex optimization problems and solve them more efficiently with quantum computing. Their vision is about container shipments volumes. They formatted their problem as a “vehicle routing problem with time windows” (VRPTW) which is a NP-hard problem. They compared various methods, using a QUBO algorithm that can be transformed on a lower-level VQE or QAOA hybrid algorithm and experimented it with Qiskit on the QasmSimulator IBM quantum emulator backend<sup>1275</sup>. As in many similar cases, the published paper does not provide any clear answers on the gain and on the quantum computer specification that would make it possible to solve a real-life problem. On top of that, it was not at all formulated as a container shipment optimization problem per se but as a simpler truck routing problem.

So, we're off wondering what they really achieved or could achieve. Similar trucks routing algorithms were already explored by **Accenture** and **Denso** using D-Wave annealers. Annealers are so far in a better position to solve these problems than existing superconducting gate-based qubits systems from IBM.

Here is at last one quantum software vendor that is entirely dedicated to one transportation market.



**AlphaRail** (2000, USA) is a railways software company using machine learning and quantum computing to improve railways operations.

They are relying on quantum and quantum-inspired approaches to solve routing and scheduling optimization problems.

## Telecommunications

At this stage, the main quantum involvement of telecom companies is mainly related to quantum telecommunications and cryptography.

---

<sup>1273</sup> See [How BMW Can Maximize Its Supply Chain Efficiency with Quantum](#), Honeywell, January 2021.

<sup>1274</sup> See [DP World explores quantum computing technology](#), April 2021.

<sup>1275</sup> See [ExxonMobil & IBM Explore Quantum Algorithms to Solve Routing Formulations](#) by Stuart Harwood et al, February 2021 which refers to [Formulating and Solving Routing Problems on Quantum Computers](#) by Stuart Harwood, January 2021 (17 pages).

In the USA, **Verizon** launched a QKD trial on three sites in the Washington, D.C., area<sup>1276</sup>. In 2021, they also tested a VPN using a PQC (post-quantum cryptography) solution based on the Saber NIST competition finalist, for connection between two sites in the US and UK.

In France, **Orange** participated to a QKD trial in the Nice region with partners including the In-PhyNi research lab.

**British Telecom** has also experimented a QKD setup to demonstrate some secured backup of data-center resources. In October 2020, they deployed a pilot 6 km long QKD infrastructure in Bristol to connect several industry sites, in partnership with **Toshiba** as part of the **AQuaSec** (Agile Quantum Safe Communications) program, cofunded by UKRI<sup>1277</sup>. In October 2021, BT and Toshiba announced the deployment of a commercial QKD network in London, mixed with PQC for non photonic endpoints.

Quantum computing can still play a role to solve various optimization problems in the telecom industry. The most commonly presented are the placement, power and frequency assignment of overlapping cells in 4G/5G mobile networks, the configurations of paths and wavelengths on land line fiber optics networks and similar optimization problems for satellite communications<sup>1278</sup>.

In Italy, the telecom operator **TIM** used a D-Wave QUBO based algorithm to optimize the setup of 4G/5G radio cells frequencies.

## Finance

Finance is another great playground for experimenting quantum technologies and particularly quantum computing<sup>1279</sup>. Both because this vertical is quite hungry with forecasting and optimization needs and also because it is a rather solvent market with many economic players having the critical mass to invest in new technologies.

Banks have a pressing need to transform themselves to adapt to constant technological and societal changes. They manipulate valuable data dumps. They need to optimize many facets of their business, starting with investment portfolios.

It's all about optimizing portfolio returns, minimizing risks, manage regulations, mainly the Basel III framework rules with their liquid coverage radio constraints, and at last detect fraud risks as efficiently as possible.

Also, assets are interdependent and transaction costs are variable depending on the type of assets. Their evolution responds to varying levels of uncertainty and risk.

Question	Broad approach solution
<i>Which assets should be included in an optimum portfolio? How should the composition of the portfolio change according to what happens in the market?</i>	Optimization models
<i>How to detect opportunities in the different assets in the market, and take profit by trading with them?</i>	Machine learning methods, including neural networks and deep learning
<i>How to estimate the risk and return of a portfolio, or even a company?</i>	Monte Carlo-based methods

Table I. Financial problems addressed in this paper, and possible approaches.

<sup>1276</sup> See [This Executive Director Is Leading Verizon Into the Future Through Quantum Computing](#) by Joanna Goodrich, IEEE Spectrum, November 2020.

<sup>1277</sup> See [BT and Toshiba install UK's first quantum-secure industrial network between key UK smart production facilities](#), October 2020.

<sup>1278</sup> See [Heterogeneous Quantum Computing for Satellite Constellation Optimization: Solving the Weighted K-Clique Problem](#) by Gideon Bass et al, Booz Allen Hamilton, 2017 (17 pages).

<sup>1279</sup> See overview in [Quantum Computing and Finance](#) from the Quantum World Association, August 2018, which refers to [Quantum computing for finance: overview and prospects](#) by Roman Orus et al, 2018 (13 pages).

There are also some interesting mathematical relationships between some key equations in finance and in quantum physics. This is the case of the Black-Scholes differential equation, which makes it possible to calculate the price of financial derivatives that are indexed on the price of underlying different financial instruments. It can indeed be considered as a variant of Schrödinger's wave function!

A recent review paper from Isaiah Hull, Or Sattath, Eleni Diamanti and Goran Wendum from Sweden, Israel and France, describes the wealth of quantum algorithms that can be used in the economic and financial spheres<sup>1280</sup>:

- **Numerical differentiation** algorithms used in financial econometrics, structural microeconomics, maximum likelihood estimation, dynamic stochastic general equilibrium (DSGE) modelling, and large-scale macroeconomic modelling conducted by central banks and government agencies.
- **Interpolation algorithms** used to solve dynamic economic models.
- **Linear systems algorithms** including matrices inversions, linear regressions and matrix powers.
- **Finite elements methods** used in some macro-economic models.
- **Computational finance** using most of the time quantum annealers. The most common task is portfolio optimization. Some algorithms exist that could run on a gates-based quantum computer<sup>1281</sup>.
- **Machine learning algorithms** including principal component analysis used in macroeconomics, forecasting, modeling credit spread and pricing financial derivatives<sup>1282</sup>.
- **Monte Carlo simulations** used in many applications like for the simulation of agent choices over time.
- **Quantum annealing** using D-Wave systems. One example is an investment quantum optimization model published in 2015<sup>1283</sup>. It was based on a QUBO model and graph modeling. Another case study was used to model market instability<sup>1284</sup>.
- **Random numbers generations** used beyond cryptography, for simulations and estimation.

When you look at some of the referenced papers, you discover that hardware constraints are quite high<sup>1285</sup>. For example, some credit risks analysis and derivative pricing use cases mention a need for

---

<sup>1280</sup> See [One Bit, Qubits, A Dollar: Researchers Say Economists Should Prepare for Quantum Money](#) by Matt Swayne, January 2021, making reference to [Quantum Technology for Economists](#) by Isaiah Hull, Eleni Diamanti et al, December 2020 (120 pages). The report was published by Sveriges Riksbank, the employer of one of the contributors. They didn't fund any research related to this paper.

<sup>1281</sup> See [Quantum computational finance: quantum algorithm for portfolio optimization](#) by Patrick Rebentrost and Seth Lloyd, 2018 (18 pages).

<sup>1282</sup> See for example [Study: Quantum Computers Can't Match Classical Computers in Derivative Pricing... Yet](#) by Matt Swayne, December 2020 making a reference to [A Threshold for Quantum Advantage in Derivative Pricing](#) by Shouvanik Chakrabarti et al, May 2021 (41 pages).

<sup>1283</sup> In [Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer](#), 2015 (13 pages).

<sup>1284</sup> See these slides in this [D-Wave presentation](#). See also [Applications of Quantum Annealing in Computational Finance](#), 2016 (29 slides) and the [Quantum For Quants](#) website they created.

<sup>1285</sup> See [Credit Risk Analysis using Quantum Computers](#) by Daniel J. Egger et al, 2019 (8 pages).

7500 logical qubits (*below*), which is a level above the 4098 minimum threshold for breaking a 2048 bits RSA key with Shor's algorithm<sup>1286</sup>.

Method	$(d, T)$		Error		T-count		T-depth		# Logical Qubits	
	Auto	TARF	Auto	TARF	Auto	TARF	Auto	TARF	Auto	TARF
Riemann Sum					$\geq 10^{43}$	$\geq 10^{18}$	$\geq 10^{43}$	$\geq 10^{18}$	-	-
Riemann Sum (no-norm)	(3, 20)	(1, 26)	$2 \times 10^{-3}$		$1.4 \times 10^{11}$	$5.5 \times 10^{10}$	$1.9 \times 10^8$	$1.7 \times 10^8$	24k	15k
Re-parameterization					$4.2 \times 10^9$	$3 \times 10^9$	$4.6 \times 10^7$	$6.2 \times 10^7$	7.5k	9.5k

TABLE I: Resources estimated in this work for pricing derivatives using different methods for a target error of  $2 \times 10^{-3}$ . We consider a basket autocallable (Auto) with 5 payment dates and a knock-in put option, and a TARF with one underlying and 26 payment dates. We find that Grover-Rudolph methods [10] are not applicable in practice (details in Appendix B) and that Riemann summation methods require normalization assumptions to avoid errors that grow exponentially in  $T$ . Even if those normalization issues were avoided, as detailed in the Riemann Sum (no-norm) row, the re-parameterization method still performs best. See Section IV A for a discussion of the Riemann summation normalization. The detailed resource estimation is discussed in Sections IV A 2 and IV B 3.

The Hull/Diamanti/et al paper also reviews the broad topic of quantum money, and idea born circa 1969 and published in 1983 par **Stephen Wiesner**. The idea is to use quantum objects properties and the non-cloning theorem to avoid any counterfeiting and forging. Any bill has two unique identifying numbers: one classical serial number that is public and one secret random quantum number called a “random classical bill state”. The central bank is the only one keeping the classical bill state. It’s encoded using for example polarized photons on a  $0^\circ$  or  $45^\circ$  basis. Only the bank knows this sequence of encoding.

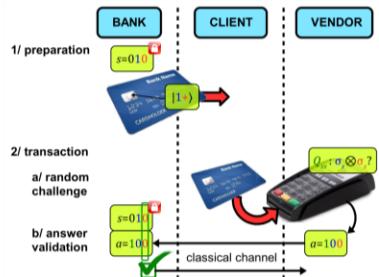


Figure 1. **Practical quantum money protocol.** The sequence of interactions between the credit card holder (client), the bank and the vendor involved in the transaction. In the preparation phase, the bank uses a secret key to prepare the quantum state loaded on the credit card, which is then given to the client. In the transaction phase, the vendor randomly selects one out of two challenge questions, measures the qubits and sends the outcome to the bank, who can then verify the validity of the credit card or detect a forgery attempt.

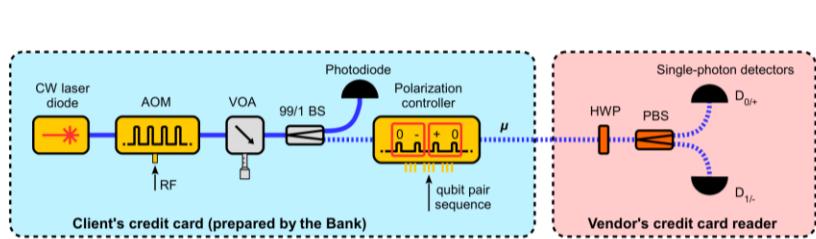


Figure 2. **Experimental setup of the quantum money system.** The credit card state preparation is performed using pulses carved from light emitted by a telecommunication wavelength laser diode using an acousto-optic modulator (AOM). A multi-stage polarization controller (EOSPACE) is then used to select the polarization states according to the protocol by applying suitable voltages. The average photon number of pulses  $\mu$  is set by a variable optical attenuator (VOA) and is calibrated with a 99/1 beam splitter (BS) and a photodiode. The credit card reader is materialized by a standard polarization analysis setup including a half-wave plate (HWP), a polarization beam splitter (PBS) and two InGaAs single-photon avalanche photodiodes (ID201). The entire setup is synchronized using a multi-channel delay generator and is controlled by software incorporating the random state generation and data acquisition and processing.

There are many variations of this concept of quantum money, with different degrees of anonymity and private and public schemes. Quantum money could be physical segmented into bills, coins and lightning schemes<sup>1287</sup>. An untraceable quantum coin proposal was made around 2010. But there are many shortcomings with these schemes which are just non implemented ideas at this stage.

One of these being that it requires quantum memory that doesn't exist yet, and which, by the way, is therefore not miniaturizable to be embedded in devices like a credit card<sup>1288</sup>. The Quantum Lightning variation prevents the bank to create multiple bills with the same serial number. You also have semi quantum money that requires no quantum communication infrastructure. All in all, it's quite difficult to assess the practicality of such quantum money ideas.

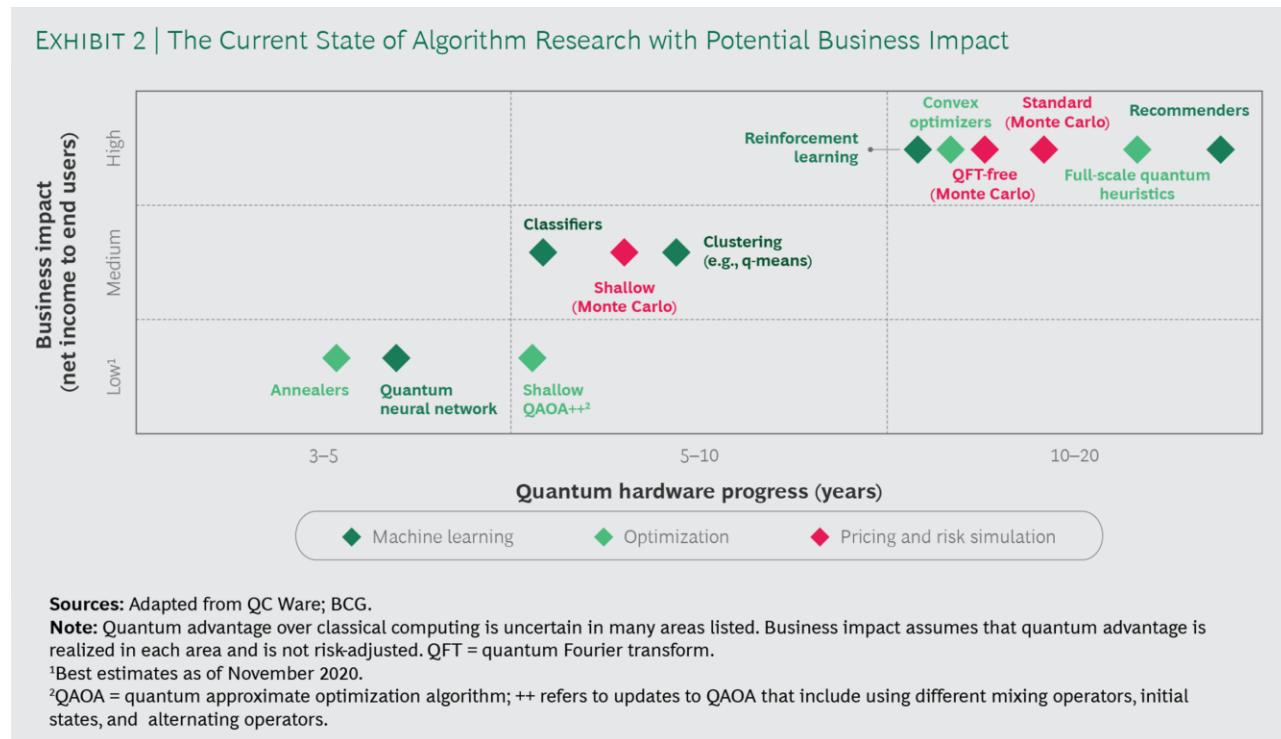
<sup>1286</sup> See again [A threshold for quantum advantage in derivative pricing](#). 7.5K logical qubits and T-depth of 54 million needed for pricing derivatives.

<sup>1287</sup> Quantum Lightning is a public key quantum money type.

<sup>1288</sup> See [Experimental investigation of practical unforgeable quantum money](#) by Mathieu Bozzio, Iordanis Kerenidis, Eleni Diamanti et al, 2017 (10 pages). The two schemas come from this document.

BCG published another review on quantum computing financial use cases including a roadmap against the estimated progress of quantum hardware in the next 5 to 20 years (*below*)<sup>1289</sup>. For its part, McKinsey is more upbeat and is pushing banks to evaluate as fast as possible the potential use cases of quantum computing<sup>1290</sup>.

D-Wave and IBM have been very active to push financial organizations to evaluate quantum computing benefits. So far, we have mainly proof of concepts and trials. Indeed, as the authors of another review paper published in 2020 point out : “*to date, quantum hardware is not advanced enough for solving any problem of practical relevance faster than classical computers*”,<sup>1291</sup>.



Since 2017, IBM has been highlighting partnerships with **JPMorgan Chase**<sup>1292</sup> and **Barclays**<sup>1293</sup> to study the uses of quantum in trading strategy optimization, investment portfolio optimization, pricing and risk analysis. Even if quantum algorithms that meet their business needs are conceivable, the capabilities of today's IBM quantum computers are insufficient to put anything into production.

<sup>1289</sup> See [It's Time for Financial Institutions to Place Their Quantum Bets](#) by Jean-François Bobier et al, 2020.

<sup>1290</sup> See [How quantum computing could change financial services](#) by Miklos Dietz et al, McKinsey, December 2020.

<sup>1291</sup> See [Quantum algorithms are coming to finance, slowly](#) by Sarah Butcher, November 2020, mentioning [Prospects and challenges of quantum finance](#) by Adam Bouland, Iordanis Kerenidis et al, 2020 (49 pages). This paper documents the quantum speedups theoretically achievable with Monte Carlo simulation and portfolio quantum algorithms.

<sup>1292</sup> See [JPMorgan Chase Prepares for FinTech's Quantum Leap](#) by Constantin Gonciulea, 2017. J.P. Morgan recruited an IBM veteran in quantum computing, Marco Pistoia, who had contributed to the development of Qiskit Aqua. See [JP Morgan Chase poaches an IBM 'Master Inventor' with 26 patents for quantum computing](#) by Hugh Son, January 2020. This quantum activity is integrated in their "Quantitative Research Group".

<sup>1293</sup> See [Why banks like Barclays are testing quantum computing](#), de Penny Crossman, July 2018, [Barclays demonstrates proof-of-concept quantum clearing algorithm](#) by Cliff Saran, October 2019 and [Quantum Algorithms for Mixed Binary Optimization applied to Transaction Settlement](#) by Lee Braine et al, October 2019 (8 pages).

TABLE 5: Algorithms can improve computational efficiency, accuracy, and addressability for defined use case.

	Quantum Algorithm	Description	Impact	Needs	Simulation	Optimization	ML
VQE	Variational Quantum Eigensolver	Use energy states to calculate the function of the variables to optimize	Procedure to assign compute-intensive functions to quantum and those of controls to classical	Qubit number increases significantly with problem size		x	
QAOA	Quantum Approximate Optimization	Optimize combinatorial style problems to find solutions with complex constraints	Simplify analysis clauses for constraints and provide robust optimization in complex scenarios	Uncertain ability to expand to more optimization classes		x	
AE	Quantum Amplitude Estimator	Create simulation scenarios by estimating an unknown property, Monte Carlo style	Handle random distributions directly, instead of only sampling, to solve dynamic problems quadratically speeding up simulations	High Quantum Volume required for good efficiency	x	x	x
QSVM	Quantum Support Vector Machines	Supervised machine learning for high dimensional problem sets	Map data to quantum-enhanced feature space to enable separation and better separate data points to achieve more accuracy	Runtime can be slowed by kernel computation and data structure		x	
HHL	Harrow, Hassidim, and Lloyd	Estimate the resulting measurement of large linear systems	Solve high dimensional problems speeding up exponentially calculations	Hard to satisfy prerequisites and high measurement costs to recover solutions	x	x	
QSDP	Quantum Semidefinite Programming	Optimize a linear objective over a set of positive semidefinite matrices	Estimate quantum system states with less measurements to exponentially speedup in terms of dimension and constraints	High Quantum Volume required for good efficiency		x	

TABLE 6: Financial services focus areas and algorithms.

Financial Services	Example Problems	Solution Approach	Quantum Algorithm
Asset Management	Option Pricing Portfolio risk	Simulation	AE
Investment	Portfolio Optimization	Optimization	Combinatorial: VQE, QAOA
Banking	Portfolio Diversification Issuance: Auctions		Continuous: QSDP AE
Retail & Corporate Banking	Financial Forecasting Credit Scoring (e.g. SME Banking) Financial Crimes: Fraud + AML	Machine Learning	QSVM HHL AE

In a recent review paper, IBM researchers describe some case studies of quantum computing in finance such as simulations (new customer identification, create new financial products, incorporate market volatility, improve customer retention), optimization and machine learning, options pricing, and quantum amplitude estimation with a quadratic speedup that can be used to estimate value at risk in an investment portfolio or in a credit<sup>1294</sup>.

**D-Wave** is at the origin with some of its customers such as **Deutsche Bank** of the creation of the [Quantumforquants](#) website, dedicated to the uses of quantum in finance. **Atos** also published a white paper on quantum applications in finance<sup>1295</sup>.

**NatWest** is experimenting quantum inspired algorithms running on traditional computers to optimize its investment portfolios (HQLA for High Quality Liquid Assets).

**Goldman Sachs** recruited Will Zeng, from Rigetti Computing, who had developed the Quil language. Will also works for the Unitary Fund which promotes open-source quantum solutions.

**Microsoft** devised a way to make stock value predictions using topological computing, a far fetched idea given the state of the art of their Majorana fermion based qubits<sup>1296</sup>.

<sup>1294</sup> See [Quantum Computing for Finance: State of the Art and Future Prospects](#) by Daniel Egger et al, IBM Quantum, January 2021 (24 pages). This is the source of the “algorithms can improve computational efficiency...” table.

<sup>1295</sup> See [Quantum finance opportunities: security and computation](#), 2016 (20 pages). This is also the case of Everest Group with [Quantum Computing in the Financial Services Industry-Infinite Possibilities or Extreme Chaos](#), 2018 (15 pages, \$990... not really worth it).

<sup>1296</sup> As documented in [Decoding Stock Market Behavior with the Topological Quantum Computer](#), 2014 (24 pages).



trading optimization

tax optimization of investment portfolio

*source: 1Qbit, D-Wave*



risk analysis

redefine Monte-Carlo techniques

*source: Atos*



The Quantum Computing Company™

**detect market instability**

seek signature of impending market instability by detecting onset of anomalously correlated moves

*source: D-Wave*



investment portfolio optimization

risk analysis

*source: Accenture, D-Wave*



risk analysis

Monte Carlo method

*source: JPMorgan, IBM*



The Quantum Computing Company™

**investment optimization**

solving optimal trading trajectory problem with QUBO

*source: D-Wave*

Also, noteworthy is the investment by the **Royal Bank of Scotland** (RBS) in the 1Qbit along with Fujitsu and Allianz.

Of course, you must add to this quick review all the quantum software startups that are entering this market. They are either using quantum inspired algorithms or pilot projects using gate-based or annealing-based quantum computing. Among these are **1Qbit**, **Multiverse**, **ApexQubit**, **JosQuantum** and **QuantFi**.

## Insurance

The insurance market is a vertical that also has to fix complex optimization problems, particularly related to risk modelling. The various related surveys and review papers I have found are not as rich as in the financial services vertical<sup>1297</sup>.

Some analysts are using the usual Shor based codebreaking attacks cybersecurity red flag and explaining all the risks businesses may face in the future<sup>1298</sup>. The related reports are clearly misleading, stating for example that quantum-based communications could be “*quicker over long distances*” on top of being better secured<sup>1299</sup>.

A 11 pages report was published late 2019 by **Novarica**, an US insurance consulting services company<sup>1300</sup>. Besides the usual generic description of the whereabouts of quantum computing, it contains only one and a half pages of insurance related use cases ideas. They are related to risk modeling and portfolio optimization. It also mentions quantum machine learning used to better detect and mitigate fraud, risks assessment with actuarial models for enhanced pricing and risk pooling precision, investments portfolio optimization and model life expectancy algorithms for large populations.

One risk modelling algorithm created by **JoS QUANTUM** is indeed documented<sup>1301</sup>.

---

<sup>1297</sup> See [The impacts of quantum computing on insurance - From theory to reality](#) from Lloyds's, February 2021 (34 pages).

<sup>1298</sup> See [Quantum computing a potential cyber risk for re/insurers](#) by Charlie Wood, November 2019.

<sup>1299</sup> See [Top 5 insurance quantum computing use cases](#) by Danni Santana, January 2018. One speaker in [Quantum Computing in Insurance - Interactive discussion](#), February 2021 (59 mn) estimates that the Shor threat can materialize in between 7 and 10 years, this being “conservative”. Well that’s kind optimistic.

<sup>1300</sup> See [Quantum Computing to Affect Insurer Tech Strategies](#), December 2019.

<sup>1301</sup> In [A Quantum Algorithm for the Sensitivity Analysis of Business Risks](#) by M. C. Braun et al, March 2021 (21 pages).

**NOVARICA | Executive Brief**

**QUANTUM COMPUTING AND INSURANCE: OVERVIEW AND POTENTIAL PLAYERS**

**Summary**

Quantum computing has the potential to break the barriers of classical computing, forcing a redesign of the fundamental technology underlying data protection, risk modeling, and select insurance third-party services.

This report provides an overview of quantum theory, current challenges, potential areas of impact, and insurance research and development activities preparing to become quantum-ready. It also features profiles of players actively developing solutions in this space, including Accenture, Cisco, D-Wave, Google, Guardtime Federal, IBM, ID Quantique, ISARA, MagQ, Microsoft, Post-Quantum, QC Ware, QuantICor Security, Qutu Labs, Qibranch, Rigetti, SpeQtral, Willis Towers Watson, Kanadu, and Xofia.

**Contents**

Introduction	2
Quantum Computing and Impact	3
How is Quantum Different?	3
Technology Overview	3
Areas of Insurer Impact	4
Quantum Computing Providers	5
Cisco, Google, Guardtime Federal	6
Artificial Intelligence and Machine Learning	7
Risk Modeling	7
Security	8
Getting Ready for Quantum	10
Concluding Thoughts	10

**Primary Report Contacts**

	Mitch Wein Executive Vice President mwein@novarica.com
	Tiffany Wang Senior Research Analyst twang@novarica.com

Page Count: 11  
Figures & Tables: 3

**best analysts report to date:** decembre 2019,  
11 pages, 1,5 pages on « solutions »

#### showcased QC applications domains:

- quantum machine learning to better detect and mitigate fraud.
- risks assessment with actuarial models for enhanced pricing and risk pooling precision.
- portfolio optimization.
- model life expectancy for large populations.
- faster (**no**) and more secure data transfer (**yes**).

#### one Evergreen

##### Actuarial case study running on D-Wave, on optimizing Solvency matching adjustment

###### Insurance - Optimisation of the Solvency II Matching Adjustment

Evergreen Actuarial  
Insurance, Optimization

An exploration of whether quantum computing can be used to select an optimal subset of assets such that an insurer's Solvency II matching adjustment is maximized: If an insurer has 1,000 assets, such as corporate and government bonds, then there are  $2^{1000}$  permutations of assets that could be selected. Being of order of  $10^{301}$  means that it would not be possible for a classical computer to consider each permutation. This work considers a simplified matching adjustment problem and tests whether a quantum computing approach finds the optimal solution.

## Reinsurance News

### Quantum computing a potential cyber risk for re/insurers: Fitch

12th November 2019 - Author: Charlie Wood

The day when quantum computing power can be applied to real world scenarios is fast approaching, posing a number of important questions around the parameters of cyber risk and security of data encryption.

Fitch Ratings analysts note how quantum computers – estimated to run 100 million times faster than current technology – stand to revolutionize research efforts, new product development and operating efficiency.

Concurrently, Fitch warns of the potential implications should a 'bad actor' be the first to fully develop and make operational a quantum computer.



**wrong risk assessment:**  
we're far far away from a quantum computer breaking RSA codes

## Marketing

Marketing is also an area where optimization algorithms for complex systems based on quantum computers could be of interest. This concerns the optimization of the marketing mix, that of media plans, or the maximization of advertising revenues, various areas that are also invested by the AI field.

**Volkswagen** experimented a vehicle recommendation system in online sales sites, with a D-Wave.

Once again, predictive systems based on the exploitation of past data and simulation based on the knowledge of market operating rules are once again opposed to each other. However, these rules do not fall under the notion of AI expert systems, which manage logical predicates, but more complex causality models<sup>1302</sup>.

## Content

Wonder how we could use quantum computing to create some content? That's the weird idea some have, at least with regards to music creation. Computer have played a role in music creation for a while so why not quantum computers? Quantum mechanics is about waves, like music<sup>1303</sup>!

The **Quantum Music** project<sup>1304</sup>, was run by Volkmar Putz and Karl Svozil in Austria from 2015 to 2018. It led to the **QuTune** project<sup>1305</sup>.

<sup>1302</sup> See for example [Display Advertising optimization by quantum annealing processor](#) by Shinichi Takayanagi, Kotaro Tanahashi and Shu Tanaka of Waseda University and [A quantum-inspired classical algorithm for recommendation systems](#) by Ewin Tang, July 2018 (36 pages). The latter classical algorithm exceeds the performance of a quantum algorithm realized for D-Wave quantum computers.

<sup>1303</sup> See [Quantum music Physics has long looked to harmony to explain the beauty of the Universe. But what if dissonance yields better insights?](#) by Katie McCormick, May 2021.

<sup>1304</sup> See [Quantum music](#) by Volkmar Putz and Karl Svozil, 2015 (5 pages).

<sup>1305</sup> It was linked to [QuTune Project Quantum Computer Music Resources](#), about making music with quantum computing, and making quantum computing with music. This project started in Spring 2021.

**Eduardo Miranda** from the Interdisciplinary Centre for Computer Music Research (ICCMR) at the University of Plymouth (UK) also works on using quantum computers to create music<sup>1306</sup>. At this point, quantum music is about finding another source of randomness to create melodies (using quantum walks-based algorithms) and to generate credible synthetic voice.

It led to the organization in November 2021 of a quantum music online event, organized, unsurprisingly, by the University of Plymouth (UK) with the sponsoring from IBM and Cambridge Quantum Computing<sup>1307</sup>.

## Defense and aerospace

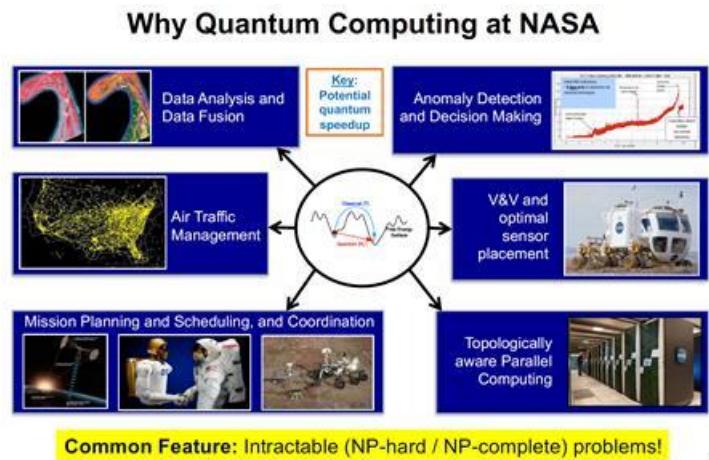
The military-industrial complex has always been a big consumer of advanced IT. It is therefore not surprising that it is interested in quantum. This is obviously the case in the USA but also in Europe, with Airbus being one of the first to take an interest in quantum applications.

Here are some published case studies of quantum use in this vast sector.

It starts with **Lockheed Martin** partnering with **Google** and **NASA** to test D-Wave annealers starting in 2014. They developed with it a solution for formal proof of software operation.

NASA co-founded the Quantum Artificial Intelligence Laboratory (QuAIL) with Google, operating a D-Wave Two. They test quantum optimization algorithms in different directions.

To optimize the filling of spacecraft, a variant of the car trunk filling (aka bin-packing) algorithm, on quantum versions of machine learning and deep learning algorithms, on problem decomposition and embedded computing<sup>1308</sup>.



In 2015, **Raytheon** and **IBM** demonstrated the efficiency of a quantum algorithm using a "black box" or "oracle" to reconstruct an unknown bit string, all running on an IBM 5 qubit general purpose quantum computer<sup>1309</sup>. This is obviously far from a real-world use case.

The **Airbus** group has created a team based at their Newport site in Wales, which is tackling the uses of quantum, particularly in the analysis of aerial imagery (not obvious...) or for the design of new materials (more obvious). They also want to optimize the air flow on the wings, a problem that is nowadays dealt with by finite element simulation. They could try to optimize the air conditioning in airplanes, the biggest source of cabin noise, above the plane's engines!

In a different field, navies are interested in quantum metrology and more precisely in the precision gravity measurement tools used to detect submarines. In fact, quantum sonars! This is the specialty of **Muquans** (France).

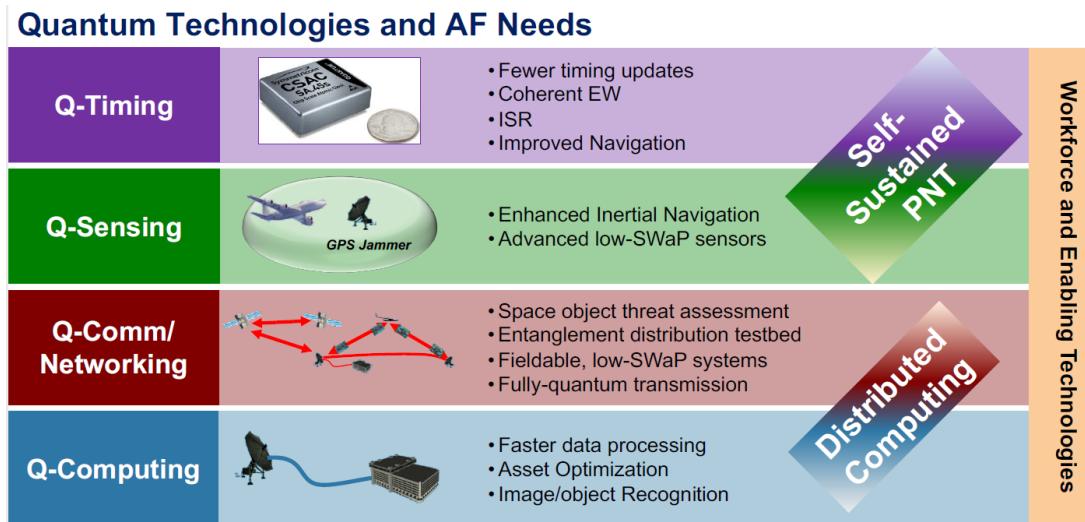
<sup>1306</sup> See [Quantum Computer: Hello, Music!](#) by Eduardo R. Miranda, June 2020 (32 pages), [Creative Quantum Computing: Inverse FFT Sound Synthesis, Adaptive Sequencing and Musical Composition](#) by Eduardo R. Miranda, 2021 (32 pages) and [The Arrival of Quantum Computer Music](#) by Eduardo R. Miranda, May 2020.

<sup>1307</sup> See [1st International Symposium on Quantum Computing and Musical Creativity](#).

<sup>1308</sup> This is well described in [Quantum Computing at NASA: Current Status](#) by Rupak Biswas, September 2017 (21 slides) where the schematic on this page comes from.

<sup>1309</sup> This is documented in [Demonstration of quantum advantage in machine learning](#) (12 pages).

The **US Air Force** has also identified various needs that can be covered by the four categories of quantum technologies with a special mention for quantum sensing in time measurement and navigation<sup>1310</sup>. They are also interested in quantum radars and, finally, in quantum computing applied to optimization problems.



In France, the **DGA** has funded or co-funded since 2011 about twenty theses on quantum and eight projects for €6.6M. The **Defense Innovation Agency** (reporting to the DGA) planned to launch a call for projects for quantum sensors in 2020 and in 2021 to fund a research project to support PQC in dedicated hardware. In July 2020, it became an ASTRID RFP on sensors, cryptography and quantum communications and on the creation of quantum computing algorithms<sup>1311</sup>.

**Thales Alenia Space** is investing with CNES and DGA in quantum satellite telecommunications.

The use of quantum technologies in the military field also gives rise to elucidations that hybridize the plausible and the offbeat, such as those of the American political scientist James Der Derian, director of Project Q at the University of Sydney<sup>1312</sup>.

## Intelligence services

The world of intelligence and targeted eavesdropping is obviously on the lookout for the quantum. Shor's algorithm is the main application targeted by organizations managing electronic eavesdropping such as the **NSA** and all its colleagues. They are firefighters who are eager to decode information intercepted from various targets (embassy communications, economic intelligence, etc.) and to protect the sensitive communications of their own states against this type of decryption. They are therefore investing simultaneously in quantum computing (the "arsonist" dimension) and in quantum keys and post-quantum cryptography (the "firefighter" dimension).

On the other hand, these investments are not very public. The NSA has communicated well for almost ten years on the firefighter dimension but very little on the arson dimension.

<sup>1310</sup> Source of the diagram: [Quantum Information Science at AFRL](#) by Michael Hayduk, December 2019 (21 slides).

<sup>1311</sup> See [Defense Research and Innovation: launch of a new ASTRID call for projects on quantum technologies](#), July 2020.

<sup>1312</sup> See [Drones, radars, nuclear: how the quantum will change the war](#) by Vic Castro, February 2020. Some remarks on this article: Rydberg atom-based qubits are only one of the types of qubits currently being studied. They are said to be "cold atom-based" and are moreover the specialty of a French startup called Pasqal. There are many other types of qubits. The text also makes a big confusion in qubits and logical gates between qubits. These gates connect qubits together. They are often systems based on the diffusion of microwaves, photons emitted by lasers or magnetic couplers. Rydberg atoms are qubits and not qubit couplers.

They have surely acquired the various generations of D-Wave computers to get their hands on, in conjunction with **Lockheed Martin** which is one of their major suppliers. NSA also maintains a joint laboratory with NIST and the University of Maryland, **QuICS**, which will be launched in 2014.

One way to lift a veil on these activities is to detect laboratory and startup grants awarded by **IARPA**, the intelligence innovation agency led by the DNI (Director of National Intelligence), who oversees all American intelligence. It consolidates collaborative research funding for all intelligence agencies. It has already launched five programs around quantum technologies: in superconducting qubits (CSQ), logical qubits (LogiQ, with IBM), error correction (MQCO, also with IBM), the creation of development tools (QCS, with Raytheon and GeorgiaTech) and quantum annealing computation (QEO). But it is not clear that this has significantly advanced the state of the art.

Other Western intelligence services may also have acquired D-Wave, notably the British CGHQ. The NSA is also in contact with IBM and Google to explore the path of superconducting quantum general-purpose computers.

## Industry

Industry in the broadest sense of the term is another outlet for quantum computing. As soon as there is a complex optimization problem for scheduling, logistics or complex system design support, quantum will have its say.

The Japanese **JSR Corporation** is one of the companies working with IBM in the quantum field, mainly for the creation of new materials.

Finally, it seems that quantum computing can be used within computer-aided design tools<sup>1313</sup>. But the document cited in the note comes back to the basics of quantum computing without being very elaborated on quantum computing uses in CAD, a very common phenomenon when quantum computing is pushed in various industries.

The routing of electronic circuits is also a complete NP-complete problem that could be partly handled by quantum algorithms, provided they have a sufficient number of qubits. This could be useful for designers of ASIC-type circuits and especially FPGAs, these circuits whose operating logic is dynamically programmable via two key parameters: the decision tables of the processing units and the links between these units.

## Science

Fundamental research is starting to test and use quantum computing, particularly in materials development and particle physics research<sup>1314</sup>.

After having investigated quantum computing for a good number of years with a first workshop organized in November 2018, **CERN** launched a formal **Quantum Technology Initiative** (QTI) in September 2020<sup>1315</sup>.

---

<sup>1313</sup> According to [Computer-Aided Design for Quantum Computation](#) by Robert Wille, Austin Fowler and Yehuda Naveh (Google and IBM), 2018 (6 pages).

<sup>1314</sup> See [Applying quantum computing to a particle process](#) by Glenn Roberts Jr., Lawrence Berkeley National Laboratory, February 2021, referring to [Quantum Algorithm for High Energy Physics Simulations](#) by Benjamin Nachman et al, February 2021 (6 pages). The algorithm used to detect particles using the 20 qubits IBM Q Johannesburg quantum system in the cloud is not providing any quantum advantage but would be promising with a larger number of qubits.

<sup>1315</sup> It was later formalized in their [CERN Quantum Technology Initiative Strategy and Roadmap](#) by Di Meglio et al, October 2021 (46 pages).

They want to use quantum computing to analyze the noisy data coming from their ultrasensitive particles detectors and to simulate the behavior of many-body quantum phenomena. CERN also participates to international quantum computing education and training with its online training resources.

Back in 2017, **Caltech** used a D-Wave Two X quantum annealer with 1098 qubits to "rediscover" the Higgs boson using CERN LHC data and a QAML algorithm (quantum annealing machine learning)<sup>1316</sup>. Later in 2020, they improved it with their QAML-Z algorithm, quantum annealing machine learning model zooming in on a region of the analyzed energy surface<sup>1317</sup>.

Superconducting qubits are also used to detect dark matter, in the form of axions, a dark matter candidate and hidden photons, that would interact with the photons<sup>1318</sup>. Other researchers are also using squeezed states to detect axions<sup>1319</sup>. Quantum computing is also tested to simulate exotic magnetic materials<sup>1320</sup>.

## Software and tools vendors

There are already many quantum software and development tools startups, particularly with regards to what suitable hardware is available. Many of them are developing software running on D-Wave annealers.



Others adopt hybrid software approaches that combine business knowledge, associated algorithms and their execution on classical machines and quantum computers, hybrid classical-quantum algorithms, or so-called "quantum inspired" algorithms that run on classical computers.

<sup>1316</sup> See [Solving a Higgs optimization problem with quantum annealing for machine learning](#) by Alex Mott et al, 2017 (5 pages).

<sup>1317</sup> See [Quantum adiabatic machine learning with zooming](#) by Alexander Zlokapa et al, Caltech, October 2020 (9 pages).

<sup>1318</sup> See [Searching for Dark Matter with a Superconducting Qubit](#) by Akash V. Dixit et al, April 2021 (7 pages).

<sup>1319</sup> See [A quantum enhanced search for dark matter axions](#) by K. M. Backes et al, 2021 (8 pages).

<sup>1320</sup> See [Quantum computing enables simulations to unravel mysteries of magnetic materials](#) by Elizabeth Rosenthal, Oak Ridge National Laboratory, February 2021, using a 2000Q D-Wave annealer.

These approaches are essential for survival. Indeed, a startup cannot be exclusively dedicated to quantum computing at the risk of only being able to sell proofs of concepts on a very small scale that cannot generally be deployed industrially<sup>1321</sup>.

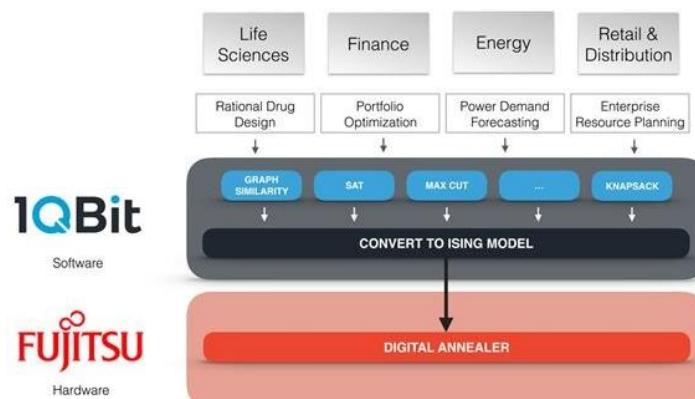
There are real opportunities to position yourself in this emerging market! You will notice that this inventory does not include any Chinese startup. This is probably not by chance. This ecosystem is therefore still very young. It will evolve in parallel with the development of commercial quantum computers. China is not very well versed in software compared to hardware and seems to have put the quantum priority on cybersecurity more than on quantum computing.



**1QBit** (2012, Canada, \$35M) is a multi-sector quantum software company. It was funded among others by Fujitsu, as well as by Accenture and Allianz.

They have developed various low-level quantum algorithmic components that are hardware neutral. This includes, for example, the graphs processing that they apply in several markets, via their consulting activity. They cover financial markets, for the dynamic optimization of investment portfolios or to simplify the allocation of asset classes in a portfolio<sup>1322</sup>.

They also developed QEMIST, a library for accelerating innovation in materials science and drug discovery. In addition to being a long-standing partner of D-Wave, they also work with IBM. The startup already has above 100 employees. Their customers include Dow Chemical (chemicals), Biogen (biotechs) and Allianz. In April 2020, they launched the "Quantum Insights Network", a network of around 100 experts and content in quantum computing.



1QBit Software running on Fujitsu Hardware - Source: Fujitsu



**Adaptive Finance Technologies** (2020, Canada) came out of the Creative Destruction Lab. It was created by Roman Lutsiv, Vlad Anisimov and Edward Tang and develops investment and credit risk management software for the finance industry.

They used classical machine learning methods and are prototyping quantum machine learning solution running on D-Wave annealers.



**Algorithmiq** (2020, Finland) is a spin-off from the University of Turku which develop quantum software for life science and data science. They also created an online quantum science and technologies learning. Their CEO is Sabrina Maniscalco.



**AiQTECH Inc** (2018, Canada) is a machine learning specialist that explores the uses of QML. They are partners of the IBM Q Network. It's a two men shop.

<sup>1321</sup> This principle of reality is well described in [The hard sell of quantum software](#) by Jon Cartwright, 2019.

<sup>1322</sup> See [Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer](#), 2015 (13 pages).



**Aliro Quantum** (2018, USA, \$2.7M) is a startup that came out of the blue in September 2019. It develops software tools telling developers whether cloud quantum computing resources are available to perform calculations faster than on traditional processors, especially on GPUs.

The startup founded by Prineha Narang and Jim Ricotta is providing a kind of a "quantum cloud resources provisioning" tool. It is supposed to be neutral with regards to the quantum computer technologies that are proposed. This kind of tool has to be associated with compilers taking advantage of the specific hardware specifics of each and every type of quantum computer. They are partnering with HQAN (Hybrid Quantum Architectures and Networks, funded by the NSF, and belonging to the University of Illinois) to develop the seeds of a distributed quantum computing network in the USA.



**Apply Science** (2019, Italy) is an applied mathematics services company who is experimenting quantum computing in the IBM Q Network. They are testing QML algorithms for virtual drug development.



**ApexQubit** (2018, Belarus and USA) is a drugs discovery company that develops quantum software solutions for the pharmaceutical sector targeting rare diseases. They operate in project mode and publish some research papers on their web site.



**Aqemia** (2019, France, 1.6M€) is a software company developing drug discovery and retargeting algorithms using statistical physics, AI and quantum inspired algorithms. The startup is a spin-off from Ecole Normale Supérieure run by Maximilien Levesque and Emmanuelle Martiano. In December 2020, they announced a partnership with Sanofi to discover new treatments for covid-19.



**aQuantum** (2018, Spain) is quantum software engineering service company doing contract research, development and consulting. They develop hybrid classical-quantum computing software and provide quantum software project management expertise, particularly in quantum machine learning.

They also developed |QuantumPath⟩ (aka Q|Path⟩), a quantum software development and lifecycle application platform. It contains all the tools to handle the whole software design and execution lifecycle covering both gate-based, quantum simulators and quantum annealing based computing, supporting QisKit (IBM), Forest (Rigetti), Ocean (D Wave), ProjectQ and |tKet⟩. They embed the open-sourced Quirk graphical tool in their development environment.



**A\*Quantum** (2018, Japan, \$3M) specializes in the development of quantum software solutions for both annealers (including digital annealers from Fujitsu) and gate-based quantum computers (from IBM). Their ambition is to create high-level software libraries for users.



**Ankh.1** (2018, USA) has developed Anubis Cloud, a virtual machine in the cloud for data scientists that integrates with the open-source solution Jupyter as well as with the Tensorflow and Keras learning machine frameworks.



**AppliedQubit** (2019, UK) presented itself as a publisher of quantum software for businesses.

In particular, they targeted the two main markets: finance and chemical simulation, in addition to generic optimization problems and predictive analysis.

They were developing both classical/quantum hybrid computing and quantum machine learning solutions. The company stopped operating in March 2021.



**Arline** (2020, Germany) is developing a compiler optimizing QML algorithms execution, reducing the number of quantum gates used and taking into account all qubits characteristics such as their connectivity.

They also propose Arline Benchmarks, an automated benchmarking platform for quantum compilers. It compares gate count, circuit depth and compiler runtime.

It can also be used to combine compiled circuits and optimization routines coming from different compilers in a custom pipeline to optimize algorithms performance.



**Artiste-qb.net** (2018, Canada) has a business model similar to that of 1Qbit: they develop algorithmic bricks of intermediate levels that they then assemble according to the needs of their customers.

They have even filed patents for certain methods. The startup was created by an international team including German researchers. They develop a Python based set of libraries in open-source, available on Github.



**Automatski** (2014, USA) is a software company established in London, India in Bengalore and in California. They do applied contract research to develop quantum algorithms on any form of computer and quantum simulator. They have developed a software solution for emulating a large, unspecified number of qubits on conventional computers. They focus on creating biochemistry algorithms and claim to have solved protein folding and to cure diabetes, cancers and 4000 other diseases. Seems like some sort of overselling.



**Avanetix** (2019, Germany) develops hybrid algorithms dedicated to solving supply chain problems. They combine classical optimization methods, machine learning and quantum computing. They target the automotive and logistics markets. The startup is founded and managed by serial entrepreneur Naimah Schütter.



**beit.tech** (2016, Poland, \$1.4M) is specialized in quantum machine learning. It is mainly a research project funded by the European Union, covering the period 2017-2010. The founder Wojtek Burkot is a former Google employee who even tries to make D-Wave useless by creating algorithms for optimizing complex graphs that can run on traditional computers.



**Black Brane Systems** (2016, Canada) is a startup focused on the development of quantum machine learning solutions. They are very "stealthy" at this stage.



**Blueqat** (2008, Japan, \$2.3M), formerly MDR for Machine learning and Dynamics Research, is creating algorithms integrating AI and chemistry, working among other with customers from the cosmetics industry like KOSE<sup>1323</sup>.

<sup>1323</sup> Blueqat developed an algorithm that analyzes the distribution of cosmetics product features in a multidimensional space. It visualizes existing areas and reveals unknown product areas they were able to open up, to create possibilities for new cosmetic designs that humans never thought of. The solution was patented and thus, is not yet publicly documented.

They are working with D-Wave annealers. The startup was founded by Yuichiro Minato and various other alumni of the University of Tokyo.



**Boltz.ai** (2020, Canada) is specialized in the development of AI and quantum software for the agriculture business. They create crop field allocation optimization tools.

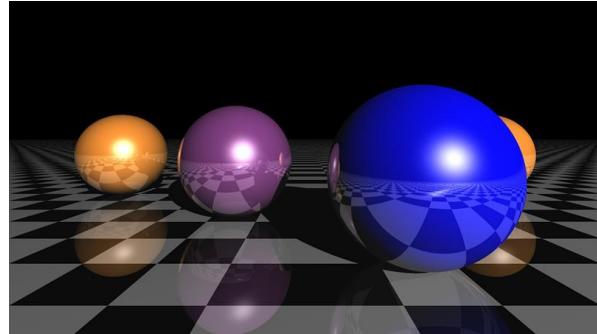


**BosonQ Psi** (2020, India) develops quantum software solutions including fluid dynamics, structural dynamics, computational heat transfer, multidisciplinary optimization and computational aeroacoustics.

It targets aerospace, automotive, power generation, chemical manufacturing, polymer processing, petroleum exploration, medical research, meteorology, and astrophysics.

## BOXCAT

**Boxcat** (2017, Canada) develops image and video processing solutions based on quantum algorithms. They target the media and medical imaging markets. Their algorithms are hybrid and are based on currently available hardware architectures (D-Wave, IBM, Rigetti). The process they present on their site is an image realized on a D-Wave, which could have been realized with Nvidia's latest GPUs.



**Cambridge Quantum Computing Limited** (2015, UK, \$72.8M) develops the  $t|ket\rangle$  quantum operating system and various quantum algorithms including Arrow for machine learning<sup>1324</sup>. They are partnering with Oxford Quantum Circuits and with IBM which is one of their investors. CQC is also active in post-quantum cryptography.

$t|ket\rangle$  is available broadly and for free to everyone since February 2021 and also open sourced. It covers many quantum computing platforms (IonQ, Honeywell, AQT, IBM Qiskit, Rigetti, Amazon Braket and Azure Quantum) and incorporates circuit optimization and routing. It's interfaced with Python with Pytket.  $t|ket\rangle$  is also used by EUMEN, CQC's quantum computational chemistry platform, and the company's QML framework. QQC is also partnering with Roche to use quantum algorithms for drug discovery targeting Alzheimer's Disease, as announced in January 2021.

In 2021, CQC launched a cloud software random quantum number generator. It is using a classical random generator, a quantum random number generator amplifying the randomness of the first and a Bell test used to check the resulting randomness, all running on an IBM quantum system<sup>1325</sup>.

CQC has also been demonstrating how NLP (Natural Language Processing) could be implemented on current NISQ IBM quantum computers. Their researchers explain that the structure of natural language is natively quantum, which could lead to efficient translating, and better understanding of complete sentences and texts. The paper however doesn't provide much indication on the way data was actually encoded in the qubits. It lacks supporting data on actual system performance<sup>1326</sup>. In October 2021, this was packaged in an open-source Quantum Natural Language Processing (QNLP) toolkit and library, lambeq.

<sup>1324</sup> See [t|ket> : A Retargetable Compiler for NISQ Devices](#), April 2020 (43 pages).

<sup>1325</sup> See [Quantum-Proof Cryptography with IronBridge, TKET and Amazon Braket](#) by Duncan Jones, March 2021 and more details in [Practical randomness and privacy amplification](#) by Cameron Foreman et al, 2020 (26 pages).

<sup>1326</sup> See [Foundations for Near-Term Quantum Natural Language Processing](#) by Bob Coecke et al, December 2020 (43 pages). By the way, they are using ZX calculus in this work.

The company announced a merger with Honeywell Quantum Systems in 2021. In December 2021, it became Quantinuum with a staff of over 350 employees.



**ChemAlive** (2014, Switzerland) is a quantum computational chemistry startup and contract research company. It provides simulation tools for getting molecular properties and synthetic reactions using basic 2D chemical syntax.

They deal with reaction mechanism elucidation and optimization, kinetic observed rate modeling, molecular design, virtual screening and drug discovery, molecular and spectroscopic property prediction, materials modeling and design, data and computation driven synthetic planning, experimental execution of chemical synthesis and experimental research on spectroscopic and electronic molecular properties. They developed ConstruQt, a software tool transforming molecular drawings into 3D structures and energies.

All of this is quantum... but seems to be computed classically. Quantum chemistry doesn't necessarily mean quantum-computed quantum chemistry. Once quantum computing hardware will scale, they'll naturally switch to it.



**ClassiQ** (2020, Israel, \$15.8M) develops a quantum programming tool providing a higher level of abstraction than classical quantum gate programming.

All the tools improving the level of abstraction of quantum programming that I have been able to discover continue to use quantum gates. The company was created by Nir Minerbi (CEO), Amir Naveh (VP-R&D) and Yehuda Naveh (CTO, who spent 20 years at IBM Research in Haifa, including quantum, condensed matter specialist).



**CogniFrame** (2016, Canada) is a software publisher of data analysis platform software exploiting machine learning. They also develop hybrid algorithms for the financial sector based on D-Wave annealers.

One of their first customers is the Canadian investment bank Alterna Savings. The proposed applications are classic in the financial field: credit risk assessment and investment portfolio optimization.



**CreativeQuantum** (2010, Germany) is specialized in quantum physics-based R&D in the chemical and pharmaceutical industries.

They seem however to run these many algorithms with classical computers. Which makes sense given quantum computers are not yet powerful enough to run these physics simulation tasks efficiently.



**CULGI** (2004, Netherlands) is yet another computational chemistry company that will someday adopt quantum computing or simulation for its software. It was founded in 1999, changed its name in 2004 and was acquired by Siemens in 2020.

$$\frac{d\vec{v}}{dt}$$

**dividiti** (2014, UK) develops quantum algorithms, particularly in machine learning and using hybrid methods. Their solutions are open-source. It is a service model, which is rather the standard in this market at the moment.



**D Slit Technologies**

**D Slit Technologies** (2018, Japan) develops custom quantum software solutions for creating proofs of concept. Their website is not very talkative about their achievements.



**Elyah** (2018, Japan/Dubai) is developing quantum software to "improve people's lives". The company is made up of two people, a certain Salman Al Jimeely based in Dubai and an American, Sydney Andrew, based in Tokyo. I'm still looking for those developing software worsening people's lives, besides pirates.



**Entanglement** (2017, USA) is a quantum software development service company. One of their achievements was to create a quantum inspired software for vaccine distribution optimization in the USA in 2021.



**Entropica Labs** (2018, Singapore, \$1.8M<sup>1327</sup>) is a startup dedicated to the creation of quantum (and non-quantum) algorithms for life sciences and in particular for genomics, based on quantum machine learning.

The result is faster development of therapies, in partnership with pharmaceutical companies. The company was founded by Tommaso Demarie, Ewan Munro, joined in 2018 by Joaquin Keller, a former Orange researcher based in France. It offers its Entropy Development Framework that manages the workflow of quantum software. They are working with Honeywell and BMW to create proof of concepts for supply chain optimization.



**ExaQ.ai** (2020, Singapore) creates QML algorithms under the Polyadic brand. The Polyadic QML Library is a Python library used to create QML models.



**FAcTs** (2016, Germany) is a spin-off from Max Planck Institute for Chemical Energy Conversion that develops ORCA, a quantum-chemical software package.



**FAR Biotech** (2016, USA) does drug discovery based on quantum representation of molecular structures done, so far, on classical computing.



**Grid** (2009, Japan) is a specialist in deep learning and learning by reinforcement with their ReNom platform.

They have adapted this library in a quantum version called ReNomQ. And they have been IBM Q partners since September 2019. On the other hand, their AI was probably not very efficient to help them find a company name easy to be found via search engines.



**Groovenauts** (2012, Japan, \$4.5M) developed in 2016 a D-Wave based cloud service called Magellan Blocks to solve complex optimization problems.

They exploit hybrid algorithms combining machine learning and quantum algorithms. Their first customers include a Japanese retailer who optimizes its planning and Mitsubishi Estate who optimizes household waste collection<sup>1328</sup>.



**Hafnium Labs** (2016, Denmark) develops software that provides physical property data for molecules and mixtures by combining quantum chemistry and AI. So, not yet a quantum software vendor.

<sup>1327</sup> See [Singapore quantum computing startup Entropica Labs bags \\$1.8m in seed funding](#) by Miguel Cordon, May 2020.

<sup>1328</sup> See [Groovenauts and D-Wave collaborate on hybrid Quantum Computing](#), December 2019.



**Horizon Quantum Computing** (2018, Singapore, \$3.23M<sup>1329</sup>) creates quantum development tools. Their ambition is to compile code from classical development tools such as Matlab and then run it on quantum computers, in order to make quantum computing accessible to traditional developers.

In short, they want to democratize quantum software development. The startup was launched by Joe Fitzsimons and Si-Hui Tan, both coming from Singapore's CQT research center. There were about ten employees as of April 2020.



**HQS Quantum Simulations** (2018, Germany, €2.3M) is a Karlsruhe startup led by Michael Marthaler developing quantum algorithms in the field of organic and inorganic molecular simulation of simple molecules (methane, light emission in OLEDs, diffusion of molecules in liquids).

They announced in July 2018 an open-source porting tool for ProjectQ code (IBM platform) to Cirq (Google platform). They already have BASF and Bosch as customers. They were called before Heisenberg. In practice, they also develop classical versions of their algorithms, running on datacenters or supercomputers<sup>1330</sup>.



**Innovatus Q** (2018, Singapore) is a spin-off from the Centre for Quantum Technologies in Singapore. They work on hybrid quantum algorithms based on trapped ions and superconductors.

**Jaynes Computing** (2019, Canada) is creating a cloud-based solution based on some quantum machine learning (QML) in the supply chain market. They are supposed to use some NISQ hardware, without any details. The startup was created by German Alfaro and was spun out of the Creative Destruction Labs.



**Jij** (2018, Japan, \$1.9M) was created by researchers from the Tokyo Tech Institute of Technology. It develops software for quantum annealing, including OpenJij, an open-source framework for implementing Ising models to model particle interactions, built on D-Wave's QUBO APIs. They are also partners of Microsoft Azure.



**JoS Quantum** (2018, Germany) develops quantum software solutions for the financial services industry, particularly in risk management and fraud detection. They also do contract research.



**Ketita Labs** (2018, Estonia) develops unspecified quantum software for NISQ computers, and for good reason. It is a university spin-off.



**KiPu Quantum** (2021, Germany) was created by Enrique Solano, a prolific and outspoken peruvian researcher working in Spain (Bilbao) and Germany. The startup's goals are to "*design and manufacture of modular and co-designed Quantum computers*" tailored to solve specific tasks with NISQ, without waiting for LSQ generations.

<sup>1329</sup> See the QSI Seminar presentation: [Dr. Joe Fitzsimons, Horizon Quantum Computing, Abstracting Quantum Computation](#), April 2020 (1h26).

<sup>1330</sup> See [HQS Quantum Simulations: How to survive a Quantum winter](#) by Richard Wordsworth, 2020.

In 2021, they announced their NISQA paradigm merging digitized-counterdiabatic quantum computing (DCQC) and digital-analog QC (DAQC) for NISQ computers without error correction overhead. It uses digital and analog compression techniques to reduce the physical qubits required to solve specific industry problems (combinatorial and optimization problems, chemistry, QML, ...).



**Kuano** (2020, UK, \$3.6M) creates quantum software solutions for the design of molecules and in particular for the inhibition of enzymes, which is used both in pharmaceuticals and to create protective agents in agriculture.

They use quantum emulation and quantum algorithms as well as machine learning. The company was founded by defectors of GTN, including their CEO Vid Stojovic who was the CTO of GTN.



**Menten.ai** (2018, USA, \$4M) develops hybrid algorithms combining machine learning and quantum programming to simulate organic chemistry and design enzymes, peptides and proteins.



**Molecular Quantum Solutions** (2019, Denmark) or MQS, provides computational tools for pharma, biotech and chemical industries. It's using HPC and quantum computers.



**Multiverse Computing** (2017, Spain, 11,5M€) develops quantum and quantum-inspired software for finance, with portfolio optimization, risk analysis and market simulation. They are partnering with Xanadu, Microsoft, Fujitsu, IBM, Rigetti, DWave, NTT and Strangeworks. They are one of the few international startups to have participated in the Creative Destruction Lab in Toronto.

They also use more traditional techniques based on machine learning and digital annealing (with Fujitsu). They announced in August 2021 their Singularity Spreadsheet app solution which gives access to some portfolio optimization algorithm running on D-Wave annealers in the cloud, directly from within Microsoft Excel ([video](#)).



**NetraMark** (2016, Canada) develops quantum software solutions for the pharmaceutical industry to define therapeutic targets. They are part of the Quantum Machine Learning program at the Creative Destruction Lab in Toronto. It was acquired by the brain biotech **Nurosene Health** (2019, Canada) in October 2021.



**Novarion** (2016, Austria) is a server storage and GPU servers vendor who wants to create the first hybrid quantum computer by 2025, without mentioning what sort of quantum processor it will integrate.

In October 2020, they started a partnership with **Terra Quantum AG** (Switzerland) to create a Joint Venture to create '<Qa|aS>' by QMware'. It supports machine learning and big data analytics. QMware's customers will be able to develop and effectively run completely Hybrid Quantum Applications. Applications built on QMware's Hybrid Quantum Cloud are supposed to run on upcoming native quantum processors when they show up. Meanwhile, it runs on some classical emulators, seemingly a QLM from Atos. And it's Gaia-X and GDPR compatible.



**Nordic Quantum Computing Group** (NQCG) (2000, Norway) does R&D in areas at the crossroads between AI and quantum computing. They are creating a platform agnostic quantum software using superconducting and photonic qubits.



**ODE L3C** (2018, USA) is an American NGO involved in the creation of chemical simulation algorithms. Its ambition is to solve "difficult NP" problems with quantum computation, which is far from obvious.

This sounds more like a service provider than a software publisher. The company was created by a certain Keeper Layne Sharkey.



**Origin Quantum Computing** (2017, China, \$15M) is based in Hefei, and seems to develop quantum algorithms. They are behind one of the records for 64-qubit quantum algorithm emulation on a supercomputer<sup>1331</sup>. They also created cloud based emulation appliances supporting 32 and 64 qubits.

They also indicate that they are developing their own quantum chipsets, including a superconducting version of 6 qubits (KF C6-130) and of 100 qubits (XW B2-100), using tunable couplers. A bit like IBM, they expect to reach 1024 qubits by 2025 with intermediate steps of 64 qubits in 2021 and 144 qubits in 2022.

They developed the OriginQ Quantum AIO, a quantum computer control system as well as the QRunes language, the QPanda architecture integrating language and compiler and the EmuWare virtual machine. On the application side, they have notably invested in chemical simulation. They also provide the Qurator quantum integrated development environment (IDE).



**Opacity** (2020, Australia) offers Quiver, a quantum code optimization software compatible with IBM's Qiskit.

Their hardware-agnostic solution maps processor errors at the global and individual qubit level, including parasitic interactions between qubits. It then allows the code to be optimized to take into account this duly mapped noise. The tool seems to be dedicated to developers as well as to quantum computers designers.



**OTI Lumionics** (2011, Canada, \$5.7M) is specialized in the design of new materials and in particular LEDs and OLEDs. They have developed quantum and "quantum-inspired" molecular simulation algorithms for this purpose.

In particular, this allows them to predict the properties of the created materials, model chemical relationships and determine geometric structures. They are partners of Microsoft Azure ([video](#)).



**ParityQC**

**ParityQC** (2020, Austria) is a spin-off of the University of Innsbruck created by Wolfgang Lechner and Magdalena Hauser, the first being the scientist and the second, originally an investor in the project<sup>1332</sup>.

By August 2020, the company already had a dozen employees. They develop software solutions to solve optimization problems (CADD, N-body problems, constraint problems) adapted to digital and analog quantum computers (qubits with universal gates or quantum simulators).

Their ParityOS software suite optimizes the software parameters of the solution as well as those of the hardware control.

They support an architecture called LHZ, created by Wolfgang Lechner and Austrian colleagues Philipp Hauke and Peter Zoller, which is compatible with different hardware quantum platforms with 2D qubit connectivity architectures<sup>1333</sup>.

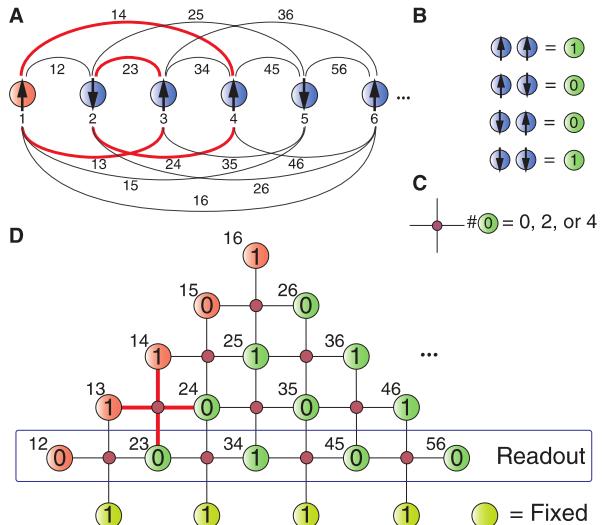
---

<sup>1331</sup> See [Researchers successfully simulate a 64-qubit circuit](#), June 2018.

<sup>1332</sup> She is the daughter of Hermann Hauser, the co-founder of Arm, now a serial entrepreneur and investor in deep techs, including Graphcore (UK).

Its principle consists in encoding a problem requiring n-to-n relations between qubits (all to all) to run it on a physical architecture where qubits are only connected to their close neighbors as is the case in most quantum computers, except for some that rely on trapped ions.

Their solution also includes an in-house error correction system<sup>1334</sup>. They are in discussion with the startup Pasqal whose cold atom-based quantum simulator architecture is adapted to their model. They announced in 2021 a partnership with NEC to help them with their superconducting qubits.



PHASE SPACE COMPUTING



PHASE CRAFT



**pine.ly**

POLARISQB

**Phase Space Computing** (2017, Sweden) is a spin-off from the University of Linköping that develops training solutions on quantum computing for secondary and higher education.

**PhaseCraft** (2018, UK, \$1M) is a quantum software company spun out of University College London and the University of Bristol. They are also partnering with Google. They want to exploit quantum computing to create better energy collection and storage systems (batteries, solar PV, ...). They developed an optimized version of an algorithm solving the Fermi-Hubbard model with fewer resources which could be helpful to create high-temperature superconducting materials<sup>1335</sup>.

**PiDust** (2019, Greece) is a startup launched by Vasilis Armaos, Paraskevas Deligiannis and Dimitris Badounas, who are alumni of University of Cambridge, Stanford and the University of Patras. They develop quantum algorithms in chemistry.

**Pine.ly** (2019, Canada) is positioned on software to assist in the creation of innovative materials with quantum computing. They aim in particular at the recycling of CO<sub>2</sub> emissions. The startup was created by three women, Nayer Hatefi, Shabnam Safaei and Rachelle Choueiri, all three scientists.

**POLARISqb** (2020, USA, \$2M) is a startup that wants to use quantum computing to create new therapies. One more!

<sup>1333</sup> This LHZ architecture is documented in [A quantum annealing architecture with all-to-all connectivity from local interactions](#) by Wolfgang Lechner, Philipp Hauke and Peter Zoller, October 2015 (5 pages) for universal gated qubit platforms (source of the schema) and in [Rapid counter-diabatic sweeps in lattice gauge adiabatic quantum computing](#) by Andreas Hartmann and Wolfgang Lechner, September 2019 (11 pages) for quantum annealing computing. See also [Quantum Approximate Optimization with Parallelizable Gates](#) by Wolfgang Lechner, 2018 (5 pages) which describes the implementation of a QAOA optimization algorithm with CNOT and unit gates. Note that their architecture is not adapted to D-Wave ECUs. On the other hand, it is adapted to 2D quantum simulators such as those of Pasqal.

<sup>1334</sup> See [Error correction for encoded quantum annealing](#) by Fernando Pastawski and John Preskill, 2015 (4 pages).

<sup>1335</sup> See [Strategies for solving the Fermi-Hubbard model on near-term quantum computers](#) by Chris Cade, November 2020 (27 pages).

The startup was founded by Shahar Keinan (CEO) and Bill Shipman (CTO). They are partnering with Fujitsu, probably to use their conventional supercomputers and their digital annealing computer. Their idea is to use personalized medicine techniques to create ad-hoc therapies. Shahar Keinan received a PhD in chemistry from the Hebrew University of Jerusalem. She specializes in computational chemistry.

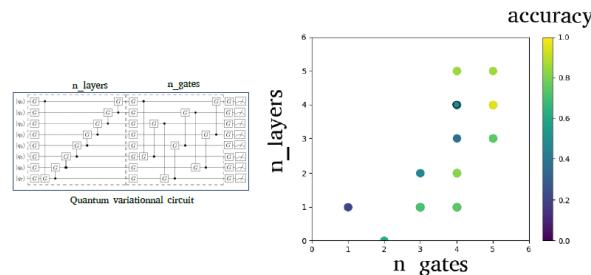
## Prevision.io

**Prevision.io** (2016, France, €1.5M) is specialized in machine learning. They have developed a platform that automates the choice of machine learning models to exploit structured data, aka AutoML.

Their QNN (“Quantum Neural Network”) and QUADS (“Quantum Algorithms Development Services”) are now integrated in their cloud offering.

In May 2019, startup founder Nicolas Gaudé and startup researcher Michel Nowak, PhD, presented the results of their quantum acceleration study of a hybrid machine learning algorithm, "Quantum Variational Circuits" on a MNIST handwriting recognition test, the same as for the early convolutional neural networks of Yann LeCun in 1988. The principle consists in optimizing the hyperparameters of a neural network in the quantum part of the computation, coupled with a Bayesian optimization working in a classical way. It is thus a hybrid quantum algorithm.

Prevision.io Bayesian optimisation of the VC



Prevision.io Benchmark

n_classes	Classic			Quantum	
	DT	LR	NN	VC	VC-BO
2	0.993	0.996	0.996	0.920	0.969
3	0.922	0.977	0.968	0.752	0.807

Their model illustrated the interest of a quantum acceleration with just 20 qubits, simulated on Xanadu's PennyLane quantum simulation library<sup>1336</sup>.

They estimate that a quantum advantage would be demonstrable on their algorithm from 28 qubits allowing to superpose the equivalent of a billion hyperparameters of a neural network.

## ProteinQure

**ProteinQure** (2017, Canada) is a Toronto-based startup that uses various technologies including quantum computing to create and simulate new "*in silico*" therapies. They use quantum algorithms to simulate protein folding.

They are also developing hybrid algorithms also using GPUs. They support different hardware architectures including D-Wave computers.

In their experiments, they manage to simulate molecules with 6 atoms in universal quantum computers and reach 11 atoms with D-Wave. In practice, however, it would seem that they have put quantum computing on the backburner and are now focused on classical learning machines in the meantime.

## Q1t

**Q1t** (2018, Netherlands) creates mathematical models and software for classical and quantum computers in the field of quantum chemistry, quantum optics and financial analysis. They have tried these algorithms on quantum simulators and quantum optics.

<sup>1336</sup> See their publication "One step towards quantum hyper parameter search", Michel Nowak and Nicolas Gaudé (June 2019).

They developed the q1tsim quantum simulation library published on Github which implements new quantum gates types for creating simpler circuits, the ability to simulate measurements without affecting qubit quantum states and the option to re-run a circuit starting with the previous quantum state for debugging purpose.

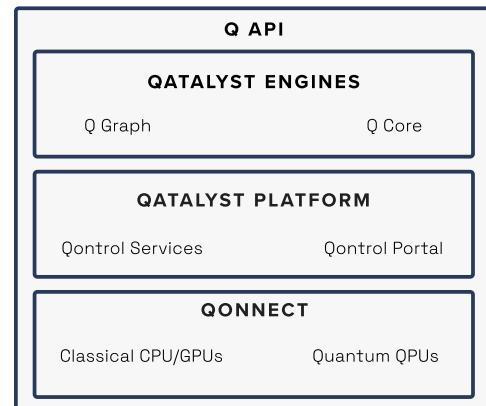


**QbitLogic** (2014, USA, \$1.5M) is another startup that develops quantum machine learning applications, without more precision in their communication. They also develop an AI based system, CodeAI, to debug software.



**Quantum Computing Inc** aka QCi (2018, USA, \$7,5M) is a quantum software company that created Qatalyst, a high-level software development and cloud provisioning tool.

It's mainly enabling developers to solve constrained optimization problems (QAOA, QUBO, graph optimization) with either gate-based accelerators, quantum annealers or classical computers. It's based on using six simple high-level APIs. It is commercially available. They support their home QikStart Program, a marketing initiative to accelerate real-world use cases with their customers. Qatalyst supports D-Wave, IonQ and Rigetti accelerators through Amazon's Braket cloud services. In March 2021, the company hired a "Chief Revenue Officer" (Dave Morris) and a Marketing VP (Rebel Brown) after having announced in December 2020 that they were filing for a Nasdaq IPO.



In July 2021, it became the first publicly traded pure player quantum computing company. QCi also created QUBT University in August 2021, an online initiative to train students on their Qatalyst tool. It's also a tactic to partner with academic institutions, like Notre Dame University in Indiana.



**Q-Ctrl** (2017, Australia, \$40.4M) is a startup created by Michael Biercuk of the University of Sydney. They are developing a set of enabling software tools to improve the operations and programming of quantum computers.

They also have a tool to visualize the effect of the modification of the qubit state by quantum gates... in the Bloch sphere. They are partners of IBM. They are also active in the field of quantum sensing, starting with a partnership with the Australian company **Advanced Navigation**, which specializes in geopositioning.

Boulder Opal is quantum control infrastructure software working at the firmware level. It leverages machine learning to improve qubits control pulses and optimize quantum error correction. It's a Python toolkit used by quantum computers designers. It works with IBM Qiskit, Rigetti and with Quantum Machines pulse generators.

They are relying on Google Cloud and TensorFlow to run the classical machine learning algorithms of their solution<sup>1337</sup>. Then, Fire Opal is developer tools for quantum algorithm designers. And Black Opal is an educational tool for students new to quantum programming.

They mention that they also work on optimizing quantum sensing solutions. At last, they are also working on creating prototype algorithms for buses dynamic scheduling of buses in Sidney, Australia (*disclaimer: it can't be operational given the power of existing quantum computers*).

---

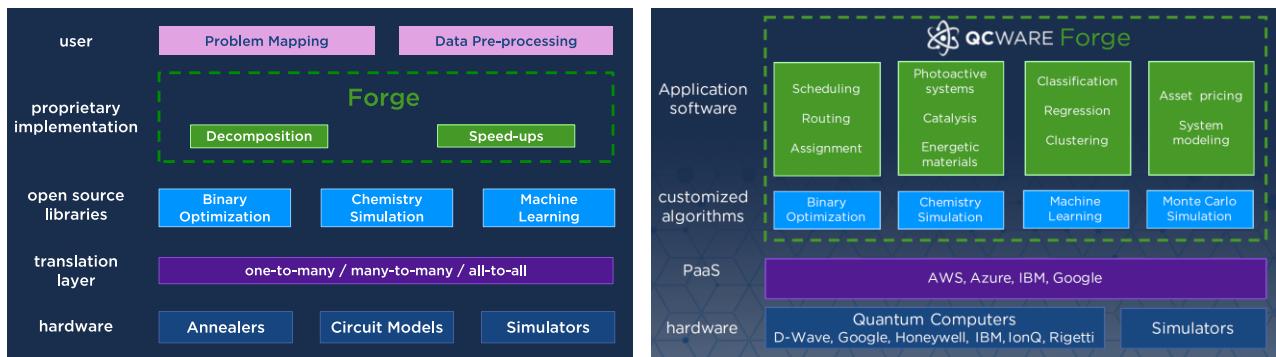
<sup>1337</sup> See [Boosting quantum computer hardware performance with TensorFlow](#) by Michael J. Biercuk, Harry Slatyer, and Michael Hush, October 2020.



**QC Ware** (2014, USA, \$39.7M) develops a platform for cloud-based quantum software development. They create quantum algorithms and software for large companies with two layers: their proprietary Forge platform and open-source libraries for optimization, chemical simulation and machine learning.

They provide tools to load training data from learning machine models into memory more quickly. They have also developed an algorithm for calculating the distance between objects, which can be used to train both supervised (classification) and unsupervised (clustering) machine learning models. Their first customers include **Equinor** for oil exploration optimization, Japan's **AISIN** for certification testing of automatic gearbox software, **Airbus** for aircraft flight envelope optimization and **BMW** for autonomous vehicle route optimization. They are also targeting financial markets as well.

It supports universal gate quantum computers (IBM, Rigetti), D-Wave quantum annealing computers and software emulators (IBM, Google, Microsoft, Rigetti)<sup>1338</sup>.



The Airbus Group is one of their investors on top of the Koch group. They have received a \$1M US public funding via the NSF in 2017. The startup, which already includes over 20 people, was created by Matt Johnson, who has a financial background, and Kin-Joe Sham and Randy Correll, who seem to have gotten late into quantum computing. The team also includes Iordanis Kerenidis, who is based in France and is a leading specialist in quantum machine learning. He oversees international algorithms development. Scott Aaronson is their Chief Scientific Advisor. Finally, the startup organizes an annual conference on quantum computing, the **Q2B**, the last edition of which was held in December 2020 online<sup>1339</sup>.



**Qindom Inc.** (2018, Canada, \$2M) is a startup developing quantum machine learning (QML) software running on D-Wave quantum annealers.



**QRithm** (2018, USA) develops quantum algorithms in diverse and rather disparate fields: machine learning, materials science, cryptography and finance.



**Qu&co** (2017, The Netherlands) was created by Benno Broer and Vincent Elfving, both quantum physicists who worked at TU Delft. They develop tailor-made quantum software solutions for large companies, accompanied by benchmark tools, particularly for chemical simulation applications based on DFT.

They develop solutions for simulating fluid mechanics with nonlinear differential equations solved with VQE algorithms (hybrid variational quantum eigensolvers). They even solve Navier-Stokes 1D equations. They partner with IBM, Microsoft and Schrodinger (USA).

<sup>1338</sup> Source of diagrams: [Enterprise Solutions for Quantum Computing](#) by Yianni Gamvros, December 2019 (25 slides).

<sup>1339</sup> View [presentation materials and videos](#) from the 2019 Q2B conference, in December 2019.

In March 2021, they launched a beta release of QUBEC, a chemistry and materials science toolkit. It comprises Q-time, a tool estimating when quantum advantage can be expected for solving chemistry or materials problems. QUBEC workflow manager supports quantum systems from IBM, IonQ and Rigetti. It is available through the IBM Q Experience and Amazon Braket platforms. LG Electronics is one of their customers.

In August 2021, they announced a new funding round with Quantonation, Runa Capital and SPIInvest, with an undocumented amount.



**QuantFi** (2019, France/USA) is a young startup specializing in the creation of quantum software solutions for finance.

It was created by Paul Hiriart (French, ex of Lehman Securities, who left the startup early in 2021), Kevin Callaghan (coming from the New York financial sector) and Gabrielle Celani (on sales and marketing). They are creating goals-based investment optimization algorithms, and also handle trends detection, derivatives pricing and risk management. In 2020, they joined the IBM Q network.

**Quanterro Labs** (2019, Abu Dhabi) is an association of researchers and entrepreneurs created by Kaisar Parvez and Ram Soorat and AiFi Technologies, an AI software startup, working in quantum information and security. They work on middleware and software development for D-Wave, Google, IBM and others. It's mostly a consulting services company.

#### QUANTICA COMPUTACAO

**Quantica Computacao** (2019, India) is the first Indian quantum startup and a software company working on creating a cloud development environment and QML algorithms. It's incubated in the Indian Institute of Technology Madras from Chennai.



**Quantopticon** (2017, UK) develops modeling and simulation software for the design of photonic components for quantum applications. It is a tool for the design of new materials.



**Quantum Benchmark Inc** (2017, Canada) provides an error-correcting code software solution for general-purpose quantum computers and error evaluation. It is thus apparently a competitor to the Australian Q-Ctrl. They also offer a quantum computer performance validation system.

The package is integrated into the True-Q suite, launched in 2018, with True-Q Design, which is used to evaluate the error rate of a quantum computer and to optimize its architecture, and True-Q OS, which helps optimize the accuracy of software solutions.

The target market is initially the manufacturers of quantum computers and those who evaluate them. Eventually, it will be that of user customers.

Note that they have already tested Google's Cirq framework, having been part of Google's beta test program for this language, and that Google is using their solution. They are also partners of IBM.

The company was acquired by **Keysight Technologies** in May 2021, on top of Labber Quantum in 2020. Keysight Technologies is a spin-off from Agilent in 2014 who specialized in electronics and radio products, while Agilent kept its healthcare business, all coming from a spin-out from HP in 1999.

**Quantum Flytrap** (2020, Poland) is a quantum computing and cryptography software company. They created a real time browser-based emulator using photonic elements instead of quantum gates. They created the "Quantum Lab" that is being used at Stanford University and the University of Oxford.

## Quantum-South

**Quantum-South** (2019, Uruguay) is a spin-off from the University of Montevideo who is specialized in developing quantum optimization software first targeting the cargo shipments in ships and airlines.

They also target the financial sector which may be more dynamic although more crowded with many existing quantum software startups. In cargo shipments, they are partnering with Quantum Brilliance (Australia) with their prototype (5) NV centers qubits.

## QBaltic



QSIMULATE



QUANTUM THOUGHT

**QBaltic** (2019, Estonia) develops algorithms for quantum computing, quantum cryptography and artificial intelligence. QBaltic is a contract research spin-off from the University of Latvia, University of Tartu in Estonia and QuBalt, Germany and Latvia.

**Qsimulate** (2018, USA, \$1.5M) develops quantum solutions for molecular simulation for healthcare and chemistry. They are partners of Amazon Braket and Google and are already working with Amgen. The company was co-founded by Toru Shiozaki and Garnet Chan, both specialized in chemistry.

**Quacoon** (2020, USA) develops software solutions combining AI and quantum. Yes another quantum machine learning vendor.

**Quantum Thought** (2019, USA) develops quantum or quantum inspired algorithms for chemical, AI and security markets. According to their website, it seems to be mainly a service company operating in project mode and doing consulting services. Their CEO is Rebecca Krauthamer.

**Quantumz.io** (2019, Poland) develops the Quantum Simulator Platform (QSP), a quantum program emulation solution running with GPUs. They are also developing a PQC (post-quantum cryptography) solution called banax, including some dedicated hardware to implement it.

## QUANTASTICA

**Quantistica** (2019, headquarter in Finland with offices in Estonia and Serbia) develops hybrid quantum algorithm software tools including Quantum Programming Studio, a graphical web development environment for creating quantum algorithms executable on quantum computers or simulators, including a classical simulator they have developed themselves.

**Quantiq** (2020, France) is a stealth startup created by Alain Habra and Fabien Niel. They work on the creation of software solutions for automatic diagnosis, particularly in the detection of pathologies with the analysis of electrocardiograms.

**Quantum Mads** (2020, Spain) was created in Bilbao by Eriz Zárate and Alain Mateo Armas and is positioned in the financial market. It offers four software tools with a mix of quantitative/classical/hybrid/quantum-inspired software.

With Q-MADS, an investment strategy analysis framework for traders, Q-RETAIL, a framework for retail banks, Q-ALLOCATE, for asset allocation optimization and Q-CRYPTO, a framework for optimal path finding in graphs. The whole is based on the HHL linear algebra algorithm.



# Quantopo

**Quantopo LLC** (2017, USA) is a company specialized in machine learning algorithms. They focus on biotechs, supply chain and logistics. They are part of the Creative Destruction Lab in Canada. But as they don't have an active website, it is not certain that they still exist.



**Quantum Open Source Foundation** got a \$4K grant from Unitary Fund. It publishes a list of quantum open-source projects on [Github](#), with various software development tools and libraries for gate-based quantum as well as and quantum annealing computing.

It's a repository of existing open-source projects including IBM Qiskit and Pennylane from Xanadu. NISQ. Provides financial funding for quantum open-source software projects. Organize events. More a community than a foundation like the Apache or Mozilla foundations.



*(Qubit|Era)*

**QuantyCat** (2020, USA) creates cloud-based APIs for quantum software development, supporting D-Wave, IonQ and Rigetti through Amazon Braket.

**Qubit Engineering** (2018, USA) was founded by University of Tennessee alumni. They develop classical and quantum optimization algorithms suitable for wind turbine design and location optimization. Another very niche market. They are partners of Microsoft Azure.

**Qubitera** (2018, USA) develops solutions combining AI and quantum.

**Qubitel Quantum Technologies** (2018, India) is a contract research laboratory developing quantum machine learning software. They were initially specialized in cybersecurity, having created a QRNG solution (Q-RandCon), a PQC protected healthcare solution (HealthCetra) and a Quantum Differential Phase Shift technology for QKD (Q-Shift).

**Qubit Pharmaceuticals** (2020, France/USA) is a startup co-founded by Jean-Philip Piquemal, a CNRS professor-researcher at Sorbonne University, a long-time specialist in molecular dynamics simulation that mathematically models the quantum mechanics of organic molecules.

The co-founders of the startup are based in Austin and at Washington University in Saint Louis. Its algorithms have been in use for a long time. Jean-Philip Piquemal is the co-author of the Tinker molecular simulation library and its Tinker-HP version adapted to supercomputers. It exploits massively parallel CPU-based systems and Nvidia GPU tensors, all with high-precision computation. In particular, it uses the Jean Zay computer from GENCI in Orsay, France, as well as those from the DoE in the USA. In this context, they have been involved in molecule screening for the search for covid-19 treatments by therapeutic retargeting. Re-targeting is easier to simulate than the 3D structure of the whole covid-19 which is more than 200,000 atoms or the simulation of protein folding.

What about quantum computing in all this? It could be used to define optimized parameters for classical simulation, in short, within the framework of hybrid algorithms.



They will also be able to exploit quantum simulators in the future, such as those being developed with cold atoms at Pasqal<sup>1340</sup>.

Jean-Philip Piquemal's laboratory at Sorbonne University has received a €9M ERC for the development of simulation solutions for organic systems of several million atoms<sup>1341</sup>. They finally welcomed the investment fund Quantonation in their capital in June 2020<sup>1342</sup>.



**QuDot** (2018, USA) develops software for the simulation of quantum circuits on traditional computers, the QuDot Net. They use techniques based on Bayesian networks to optimize the in-memory representation of qubits.

**QunaSys** (2018, Japan, \$2.8M) also develops quantum algorithms for health. From the universities of Tokyo, Osaka and Kyoto, they also maintain the Qulacs simulator developed at Kyoto University.

**QuSoft** (2014, The Netherlands) is a spin-off from TU Delft University specializing in quantum algorithms and software. Like its sister company QuTech, it is more a private applied research laboratory than a startup.

**QxBranch** (2014, USA, \$8.5M) was created by former Lockheed Martin employees. It offers solutions, probably tailor-made, for the financial, insurance, aerospace and cyber security markets.

Based in Washington DC, they already have offices in Hong Kong, London and Adelaide, Australia. They are partners of D-Wave and IBM. The startup was acquired by Rigetti (USA) in July 2019.



**Rahko** (2018, UK, £1.3M) is a quantum machine learning and chemical simulation software development company based in London. It was founded by Leonard Wossnig. They are among the first Amazon AWS partners for the use of quantum resources in the cloud, and the first in Europe.

In May 2020, they announced that they would work with Merck on "quantum inspired" algorithms, i.e. on conventional computers. In 2021, they announced that they were collaborating with Honeywell and achieved excellent accuracy executing a Discriminative Variational Quantum Eigensolver algorithm on Honeywell's H0 6-qubit trapped ion system.



**ReactiveQ** (2018, Canada) develops quantum simulation algorithms for the design of innovative materials such as high-temperature superconductors, all on a NISQ quantum computer.



**Riverlane** (2016, UK, \$24.1M) is a spin-off from the University of Cambridge that provides services in quantum computing and develops new algorithms combining machine learning and quantum in chemistry.

They develop with [dividiti Ltd](#), a one man shop created by a certain Grigori Fursin, the [Quantum Collective Knowledge](#), a benchmark SDK for quantum hardware and software.

<sup>1340</sup> See the presentation [Computational Drug Design & Molecular Dynamics: an HPC perspective](#) by Jean-Philip Piquemal, April 2020 (28 slides).

<sup>1341</sup> See [Extreme-scale Mathematically-based Computational Chemistry \(EMC2\)](#), 2020.

<sup>1342</sup> See [Qubit Pharmaceuticals closes a pre-seed round with Quantonation](#), Quantonation, June 2020.

They have also developed what they call a quantum operating system, Deltaflow.OS dedicated to NISQ systems and which optimizes access to hardware resources for qubit control. It was deployed in mid-2020 at several sites in the UK and in partnership with SeeQC and, later, CQC.

In July 2021, Riverlane created a consortium with **Astex Pharmaceuticals** and **Rigetti UK** to develop quantum drug discovery algorithms running on Rigetti platforms in the cloud. This is part of a 18-month feasibility study funded by a grant from UKRI as part of the UK quantum plan<sup>1343</sup>. Of course, you may wonder what they will do with the 31 qubits from Rigetti.



**RQuanTech** (2018, Switzerland) develops RTranscender, a quantum machine learning tool for finance, healthcare, automotive, seismology and cyber security. It supports Fourier transforms, qubit-based arithmetic operations which can help craft oracles (additions, multiplications, divisions, exponentials), factorization, discrete logs, etc.



**Schrodinger** (1990, USA, \$193) is a digital drug design company, mainly using molecules screening and doing drugs retargeting.

It is an established competitor of Qubit Pharma (France). They work with Sanofi. The company is listed on the NASDAQ. They inevitably became interested in quantum computing and have started a partnership with Qu&Co to ramp-up their skills in quantum computing.



**Semicyber** (2018, USA) develops algorithms in various fields: data analysis (non-quantum), quantum and others for critical applications for the USA defense sector, particularly the US Air Force.

So they are probably closer to the service company than to the product-oriented startup. The startup is co-founded and managed by Kayla Farrow, an engineer specializing in algorithm creation and signal processing.



**Sigma-i Labs** (2019, Japan, \$3.7M) is a consulting company and private laboratory that grew out of the Tohoku University Quantum Annealing Computing Research Laboratory, based in Sendai and led by their CEO Mazayuki Ozeki. They started by doing consulting around the creation of software for D-Wave's annealers, using their cloud Leap platform since 2019<sup>1344</sup>.



**SolidState.AI** (2017, Canada) develops machine learning solutions for the industry covering yield improvement, production calibration and predictive maintenance.

All of this is based on hybrid classical/quantum algorithms. They work with Bosch, Applied Materials, Mercedes-Benz as well as with D-Wave, Rigetti, Microsoft and IBM Q, among others.



**Spin Quantum Tech** (2018, Colombia) develops quantum algorithms in the field of cybersecurity that combine AI and quantum. They seem to create PQC (post-quantum cryptography) that exploits new encryption algorithms. They are also working on chemical simulation, which has nothing to do with it.

<sup>1343</sup> See [Riverlane and Astex Pharmaceuticals join forces with Rigetti Computing to drive drug discovery forward](#) by Amy Flower, July 2021.

<sup>1344</sup> See [Sigma-i and D-Wave Announce Largest-Ever Quantum Cloud-Access Contract | D-Wave Systems](#), July 2019.



**SHYN** (2016, Bulgaria) develops solutions for the visualization of data coming from quantum calculations. So, some quantum dataviz! With a use case consisting in detecting quantitative fake news. It was co-funded by Google's Digital News Information Fund dedicated to the press. This €150M fund distributed funding of a few 100K€ to more than 400 projects in Europe.



**SoftwareQ** (2017, Canada) offers development software for quantum computing: compiler, simulator, optimizers. The company was co-founded by Michele Mosca and Vlad Gheorghiu of the Canadian Institute of Quantum Computing.

It is a startup from the Quantum Machine Learning program at Creative Destruction Lab in Toronto.



**Strangeworks** (2018, USA, \$4M) develops quantum software. Like many colleagues, they target the aerospace, energy, finance and healthcare markets. They are at the origin of the creation of a Q&A site on [quantum computing](#), [Quantum Computing Stack Exchange](#). The company was founded by William Hurley aka whurley, and is based in Austin, Texas, with a staff of about 15.

In 2019, they launched a beta of their multi-platform development environment for quantum applications supporting quantum computers or emulators from Rigetti Computing (Forest), DWave (Leap), Microsoft (Q#), Google (Cirq) and IBM (Qiskit). This environment seems to facilitate collaborative work and sharing of results. In February 2021, it turned into an initiative to “humanize quantum computing”. It’s based on Strangeworks QS (Quantum Syndicate) which consolidates quantum hardware vendors solutions and software tools, Strangeworks QC (Quantum Computing), a free quantum computing ecosystem to learn quantum code using common quantum programming languages and Strangeworks EQ (Enterprise Quantum), an enterprise infrastructure solution consolidating QC and QS with better security, IP protection, quantum machine access, resource aggregation, custom integrations, private deployments, project management and the likes.



**Stratum.ai** (2018, Canada) develops a quantum software dedicated to a very specialized market, the optimization of mineral prospecting, particularly in gold.



**Super.tech** (2020, USA, \$150K) is a startup launched by Pranav Gokhale, Fred Chong and Teague Tomesh that develops a software stack dedicated to the control of quantum computing systems ranging from a hundred to a thousand qubits.

The solution is the result of the NSF-funded Practical-Scale Quantum Computation (EPiQC) research project involving five Chicago-area and MIT universities and stars such as Peter Shor and Aram Harrow. It is creating a software infrastructure targeting the development of NISQ solutions.



**Terra Quantum AG** (2019, Switzerland, €10M) develops quantum software solutions in all possible quantum fields: cryptography, quantum sensing and quantum computing. It is probably more a service company than a product company. They modestly position themselves as being in a position to build the "*European quantum ecosystem*"<sup>1345</sup>.

<sup>1345</sup> See [Terra Quantum secures EUR10m to build the European Quantum Ecosystem](#) by James Dargan, April 2020. On 1<sup>st</sup> April, their CTO [declared](#): “We plan to implement a useful quantum algorithm on the IBM machine with 20 qubits in order to test quantum supremacy”. Well, 20 qubits for a quantum supremacy? It’s fine if it’s an April’s fool.



**Tokyo Quantum Computing** (2017, Tokyo) wants to develop quantum annealing computer simulation software like many of the software startups from Japan.



**Tradeteq** (2016, UK, \$6.3M) is a financial trading platform that uses AI for risk assessment and portfolio optimization. Their ambition is to use quantum computing to develop their own quantum tools.

In April 2020, they announced that they would work in this direction with the Singapore Management University (SMU) and with quantum neural network algorithms.



**Unitary Fund** (international) is a kind of equivalent of the Mozilla Foundation for quantum technologies. It's a non-profit organization creating open-source quantum libraries, tools, hardware and content.

They fund through a microgrant program (\$4K) developers. They sponsored about 20 projects including the open-source compiler mitiq, Qrack (emulator accelerator on GPUs), OLSQ (Optimal Layout Synthesizer for Quantum Computing, a pre-compiler optimizer reducing the SWAP gates count), a quantum machine training textbook and Pulser, developed by Pasqal. They partner with Rigetti and IBM.



**Xofia** (2019, USA) develops software solutions based on quantum machine learning for classification. They want to distribute their software in open-source. They exploit Atos' 40 qubit quantum emulator, a QLM server, sitting in the cloud.



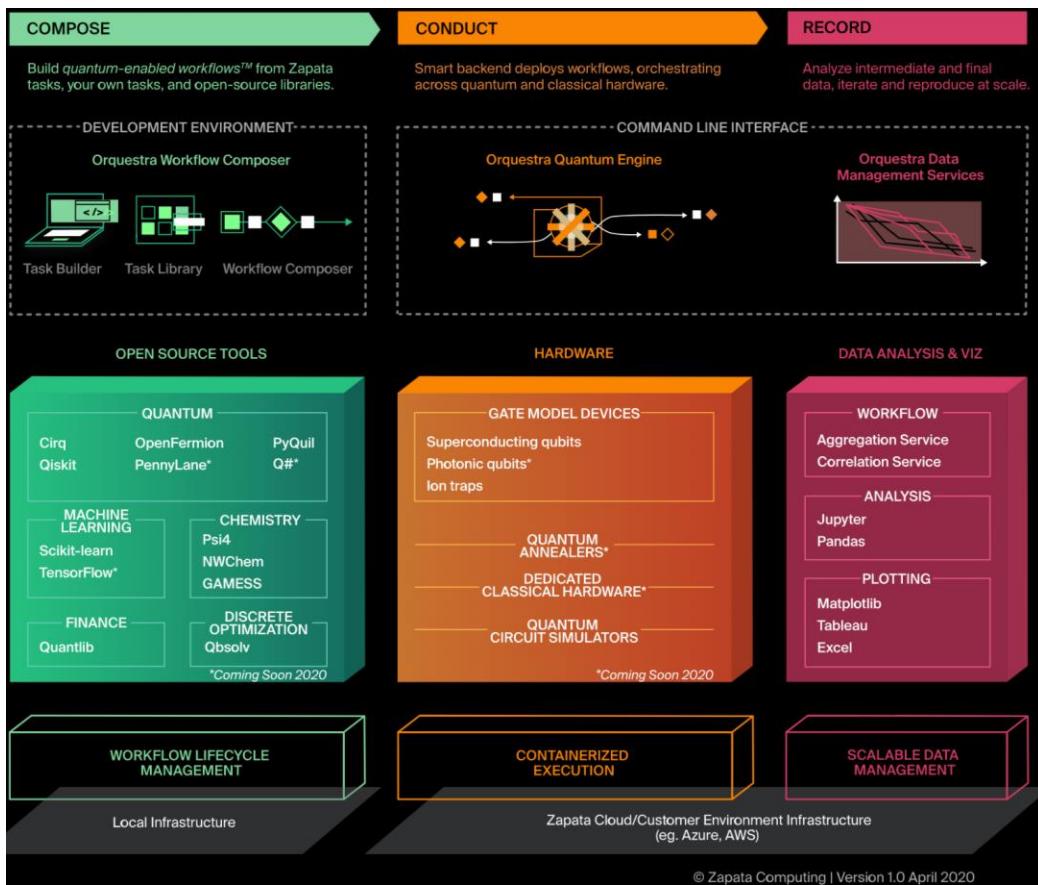
**Zapata Computing** (2017, USA, \$67.4M) is a quantum software and services company founded by Harvard researchers including Christopher Savoie and Alán Aspuru-Guzik from the University of Toronto who has developed many founding algorithms in chemistry quantum applications. Their partners include Google and IBM.

They initially developed a complete quantum operating system serving as a hub between application algorithms and quantum accelerators of all types. In April 2020, this took the form of Orquestra, a platform for managing quantum application workflows programmed with their home-grown Zapata Quantum Workflow Language (ZQWL), which is YAML-compatible and supports various quantum hardware architectures (NISQ, quantum annealing) and classical computing (quantum emulators such as those from Atos, supercomputers, cloud servers)<sup>1346</sup>.

It offers a set of code libraries supporting Cirq (Google), Qiskit (IBM), PennyLane (Xanadu), PyQuil (Rigetti), Q# (Microsoft) as well as pyAQASM (Atos). Orquestra includes tools for managing batch calculations. The Orquestra Data Correlation Service (ODCS) collects treatment data in a MongoDB database which is then exported as Excel tables, a Jupyter notebook or for the Table software.

---

<sup>1346</sup> YAML is a language that dates back to 2001. It is used to create configuration files. It is used in conjunction with Python.



Orquestra has been in beta since April 2020 as part of an Early Access Program. Honeywell invested in the company in March 2020. The company established an office in the UK in June 2021.

## Quantum computing business applications key takeaways

- Most quantum computing market forecasts are highly optimistic and plan for an early advent of scalable quantum computers. They also sometimes tweak forecasts with pushing business value numbers instead of an actual market for quantum technologies.
- There are interesting potential use cases of quantum computing in nearly every vertical market, particularly in energy, chemistry, healthcare, transportation and then finance.
- Most of them are theoretical or have been evaluated at a very low scale given the capacity of existing quantum computers. Some may be useful with advanced noisy computers (NISQ) while most of them will require highly scalable fault-tolerant quantum computing systems (LSQ/FTQC). Others may find their way on quantum simulators.
- In some cases, the potential use cases are in the overpromising twilight zone like simulating very complex molecules, fixing global warming, curing cancers or optimizing large fleets of autonomous vehicles. All these are dubious long-term promises.
- The main purveyor of case studies is D-Wave with its quantum annealer although it has not demonstrated yet a real quantum advantage. IBM is second there, having evangelized a broad number of customers since 2016.
- Beyond computing time, a quantum advantage can also come from the system energetic footprint and/or the precision of the outcome.
- There are already many software vendors in the quantum computing space. How do they strive as there are no real functional quantum computers around yet? They sell pilot projects, develop software frameworks, build quantum hybrid algorithms and create quantum inspired algorithms running on classical hardware. On top of being funded by venture capital!

# ***Quantum telecommunications and cryptography***

Quantum telecommunications cover a wide spectrum of use cases including quantum communications between quantum sensors, quantum computers and quantum key distribution used in cryptography. Most of these technologies are based on using photon entanglement and quantum teleportation as resources. The field started to develop experimentally and industrially with quantum cryptography. It is already being deployed while quantum telecommunications associated with quantum computers depend on the advent of these on a larger scale.

Interest in quantum cryptography (using entanglement as resource to share secured keys between two communication endpoints) as well as in post-quantum cryptography (classical cryptography using techniques that are resilient to attacks by quantum computers) was triggered by the creation of Shor's algorithm in 1994. It theoretically enables integers factoring on a quantum computer in reasonable times, provided large scale quantum computers are available. This algorithm has been destabilizing computer security specialists for at least fifteen years. It would make it possible to break the codes of many public key cryptography systems that are commonly used on the Internet. It is still highly hypothetical because quantum computers capable of executing Shor's algorithms for RSA keys of over hundreds bits are far from being available.

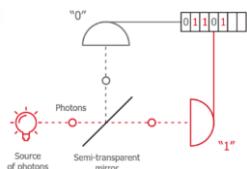
Once they are aware of the threat, however, governments, counterintelligence, intelligence and sensitive industries become seriously concerned or at least interested. The threat of quantum factorization even affects critical parts of Bitcoin and Blockchain signatures. Even though the threat is quite remote, the readiness inertia to counter this potential quantum threat means that it is necessary to launch it now.

Even before Shor's phantom menace materializes, the cyber security industry started to prepare countermeasures. The markets affected first will be the IT and telecommunications industry in general, which will have to update many software and hardware offerings, banks, the energy sector, healthcare, and government utilities.

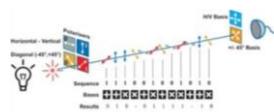
In this part, we will describe:

- The basic principles of classical cryptography, in particular **public key cryptography**, with the example of RSA public keys.
- The **nature of the threat** from integer factoring and the cryptographic solutions involved.
- **Quantum random number generators** which have become an indispensable complement to classical cryptographic solutions.
- **Quantum Key Distribution** based systems that secure the physical part of communications for the use of symmetric keys.
- **Post-Quantum Cryptography** that is used to distribute public keys using classical computation that are resilient to code-breaking done by quantum computers.
- **Quantum telecommunications** applications, outside of those related to cryptography, and in particular for the creation of distributed quantum computing systems.
- **Companies** in these sectors around the world, in a market that already includes many players and in particular many startups.

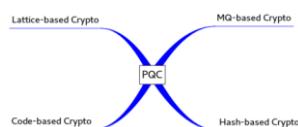
Encryption and cryptography involve mathematical concepts that are not always obvious. I'll share with you here what I have been able to understand about it and make it as accessible as possible.



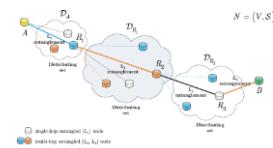
**random key generators**  
ensure the quality of  
public keys



**quantum key  
distribution**  
protects public keys sent  
through optical links



**post-quantum cryptography**  
resists to Shor algorithm



**quantum telecommunications**  
distributed quantum computing,  
connection between quantum  
computing and sensing, blind  
computing, ...

## Public key cryptography

Cryptology is the science of secrets. It allows the transmission of sensitive information between a transmitter and a receiver in a secure manner. Cryptology includes cryptography, which secures transmitted information, and cryptanalysis, which seeks to decrypt it by attack, or code-breaking.

In the case of asymmetric public-key cryptography, encryption uses only public keys and decryption uses both public and private keys. Code-breaking exploits only the public keys, while trying to deduce the private keys through intensive computing.

Cryptography secures transmitted information in several ways:

- **Confidentiality:** only the recipient can retrieve the unencrypted version of the transmitted information.
- **Integrity:** the information has not been modified during its transmission.
- **Authentication:** the sender and receiver are who they claim to be.
- **Non-repudiation:** the issuer cannot deny having transmitted the encrypted information.
- **Access control:** only persons authorized by the issuer and the recipient can access unencrypted information.

Before computer telecommunications, confidentiality was ensured by the knowledge of a common secret between transmitters and receivers, the encryption and decryption codes, which could be the position of the wheels of a German Enigma machine during the World War II. This worked in closed environments such as for military communications or between embassies and their home countries.

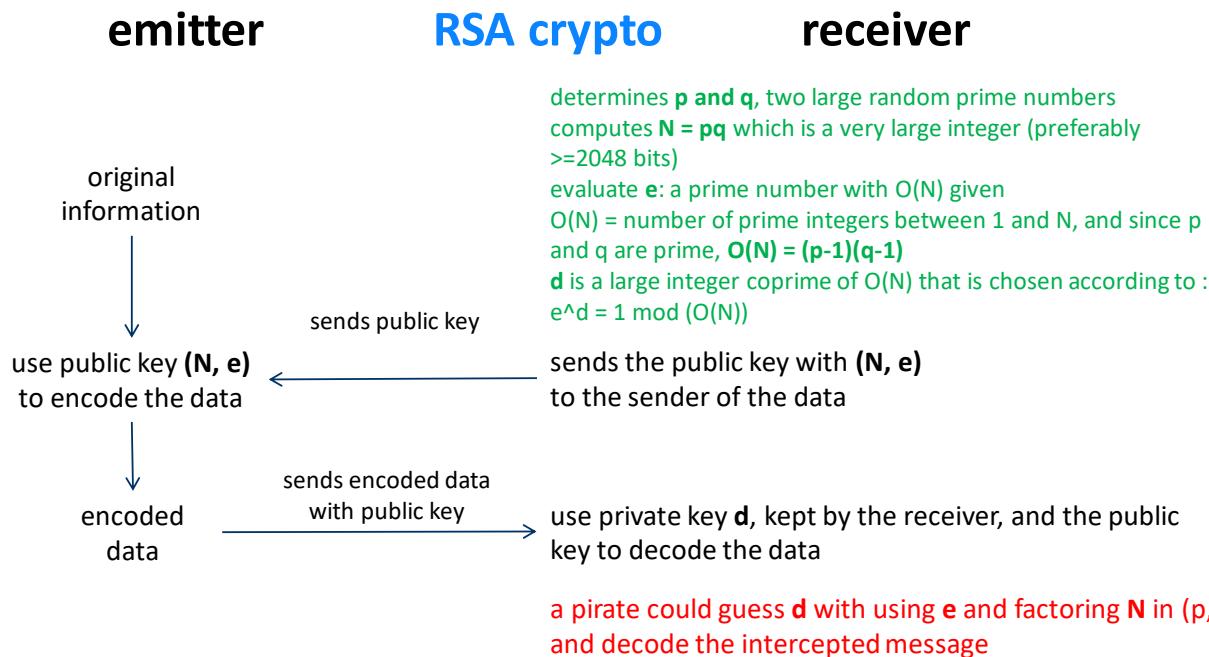
With Internet communications, this modus operandi is inapplicable for consumer applications and for business relationships in general. Hence public key cryptography systems, such as RSA, which enabled most open Internet data exchanges. There are still highly protected systems using private and symmetrical keys, mainly used in government related applications (army, security, intelligence) as well as in various other cases (some file transfers, email encryption, server/client exchanges, in smart cards and associated payment terminals).

Asymmetric (public-key) cryptography is also exploited for pre-establishing common encryption keys between users of private-key systems, for managing the integrity of communications, and for authentication as in the TLS Internet protocol. Sensitive information is then encrypted with these keys and a symmetrical AES-type algorithm. AES is used to encrypt communications in WhatsApp, Messenger and Telegram. These applications often also use asymmetric cryptography for authentication, key exchange and communication integrity management.

In many cases, symmetric cryptography systems coexist with asymmetric (public key) cryptography systems. As a result, when you communicate securely over the Internet, different complimentary security protocols are activated.

With public key systems, different keys are used for encryption and decryption of the information transmitted, so that it is very difficult (if not sometimes impossible) to guess the private decryption key from the public encryption key. The message receiver sends its public key to the sender, who in turn uses it to encrypt the message. The receiver uses the private key that was kept to decrypt the received message. As explained in the diagram *below*, the private key is never transmitted. This is also called a PKI, for "Public Key Infrastructure".

The **RSA** cryptography system is the most widely used system for protecting public key information transmissions over the Internet. It was created in 1978 by **Ron Rivest** (1947, American), **Adi Shamir** (1952, Israeli) and **Leonard Adleman** (1945, American).



(cc) Olivier Ezratty, septembre 2020

You don't necessarily need to understand the following that explains how keys are constructed. It starts by determining  $p$  and  $q$ , two large random prime numbers, with a "good" random number generator. We will see later that quantum physics can be used to create really random numbers. We calculate  $N = pq$  which is a very large integer. A good RSA key requires to have  $N$  stored on at least 2048 bits knowing that the NSA recommends 3072 bits keys for critical applications.

We then evaluate  $e$ , a prime number by exploiting  $O(N)$  which equals the number of prime integers between 1 and  $N$  relative to  $N$ , and which, as  $p$  and  $q$  are prime, equals  $(p-1)(q-1)$ .  $d$  is a large integer which is co-prime of  $O(N)$  and is chosen according to:  $e^d \equiv 1 \pmod{O(N)}$ . At the end, we get a public key that includes the integers  $N$  and  $e$ , and a private key that includes  $d$ . All of this is based on the theory of numbers and uses in particular the Fermat's little theorem and Euler's theorem which make it possible to create two distinct keys that are the inverse of each other.

With that, anyone can encrypt a message using the public key and this message is being decipherable only by the person who has the private key that splits the public key into primitives.

A hacker could decrypt the information sent by intercepting  $e$  (the end of the public key) and factoring  $N$ , the other end of the public key, into the integers  $p$  and  $q$ , and then rebuilding the private key  $d$  from it.

To date, prime number factoring requires a traditional machine power that grows with the square root of the number to be factorized.

The official RSA key factoring record was 768 bits in 2010, 795 bits in 2019 and 829 bits in February 2020<sup>1347</sup>. Even if this doesn't take into account undisclosed NSA records, it provides an idea of the problem scale. We're far from having a classical computer breaking an RSA 2048 bits code.

## Quantum cryptography

The diagram *below* points out the main encryption algorithms vulnerable or not to known<sup>1348</sup> quantum algorithms. Broadly speaking, common public key encryption systems are vulnerable. Only post-quantum cryptography systems are resilient. But they are not yet in production.

The table is a matrix from NIST comparing various cryptographic algorithms based on their type and purpose, and their resilience against quantum computers. The columns are: Name of Cryptographic Algorithm, Type, Purpose, and Resilience against Quantum Computer. The rows include AES-256, SHA-256, SHA-3, Lattice-based (NTRU), Code-based (Mc Eliece), Multivariate polynomials, Supersingular elliptic curve isogenies (SIDH), ECDSA, ECDH, RSA, and DSA. A green box highlights the first four rows. A red box highlights the last three rows. Red arrows point from the right side to the resilience column, with labels: 'High level of confidence' (for the first four), 'Under investigation' (for the last three), and 'threatened by quantum algorithms' (for the last three). The NIST logo is in the top right corner.

Name of Cryptographic Algorithm	Type	Purpose	Resilience against Quantum Computer
AES-256	Symmetric Key	Encryption	Ok but larger key sizes needed
SHA-256, SHA-3		Hash function	Ok but larger output needed
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed
Code-based (Mc Eliece)	Public Key	Encryption	Believed
Multivariate polynomials	Public Key	Encryption; signature	Believed
Supersingular elliptic curve isogenies (SIDH)		Encryption; possibly signature	Believed
ECDSA, ECDH (Elliptic Curve Crypto)	Public Key	Signatures, Key exchange	No longer secure
RSA	Public Key	Signatures, Key establishment	No Longer secure
DSA (Finite Field Crypto)	Public Key	Signatures	No Longer secure

### Shor's Phantom Menace

**Peter Shor's** algorithm sparked interest in quantum computing when there was even no single working qubit around that was controllable by quantum gate! Shor's algorithm enables theoretically to factor integers in a reasonable time that is proportional to their logarithm. It is thus a factorization in a linear time as a function of the number of key bits. This could be detrimental to all public key-based cryptography<sup>1349</sup>.

But this will happen only in a relatively distant future! In 2019, Google researchers published an algorithm allowing to quickly break an RSA key (of 2048 bits) and with "only" 20 million qubits having an error rate of 0.1% and in a calculation carried out in 8 hours. This is more "acceptable" than the billion qubits that were needed in previous instances of Shor's algorithm.

Today's quantum computers have a coherence time much shorter than a second, but the decoherence counter is reset after each error correction code that is used in the algorithm<sup>1350</sup>.

<sup>1347</sup> This factorization of an RSA-250 digits (829 bits) and the previous RSA-240 digits (795 bits) was achieved by an international team led by French researchers from Inria: Fabrice Boudot (Université de Limoges), Pierrick Gaudry (CNRS), Aurore Guillevic, Emmanuel Thomé and Paul Zimmermann (Inria) and Nadia Heninger (University of California). Computation used 2700 core-years, of Intel Xeon Gold 6130 CPUs running at 2.1 GHz.

<sup>1348</sup> Seen in [IDQ: Quantum-Safe Security relevance for Central Banks](#), 2018 (27 slides) and slightly supplemented by some captions.

<sup>1349</sup> See this presentation which describes in great detail how Shor's algorithm works: [On Shor's algorithms, the various derivatives, their implementation and their applications](#) by Martin Ekerå, 2019 (135 slides).

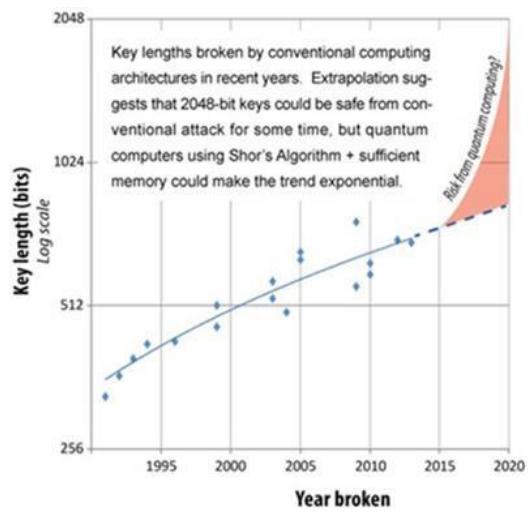
<sup>1350</sup> See [How a quantum computer could break 2048-bit RSA encryption in 8 hours](#) and [How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits](#) by Craig Gidney and Martin Ekerå, 2019 (25 pages). On the other hand, the title of the article [A quantum computer breaks 2048-bit RSA encryption in 8 hours](#) by Arthur Vera (2019) is misleading since this computer does not exist yet!

This means that we may be able to overcome the limit of the coherence time that is generally quite short, like around 100  $\mu$ s for superconducting qubits.

Breaking a 2048-bit RSA key requires at least a number of logical qubits equal to twice the size of the key used +2, so 4098 qubits. Depending on the technologies used, this number should be multiplied by 50 to 20,000 for the number of physical qubits. This scalability is one of the greatest challenges for building viable quantum computers as we've seen in other parts of this ebook.

Moreover, as we have seen in the section on Shor's algorithm, the quantum Fourier transform underlying it uses phase controlled R-quantum gates whose implementation is far from obvious. Indeed, when the phase is an angle of 1/2048 times a 360° turn in the Bloch sphere of a qubit, the controlled rotation of the phase can be inferior to the error rate of a one or two-qubit quantum gate. We must therefore bet on the ability of error correction codes to handle this.

A 762-bit RSA key close to the 2010 record would require a **D-Wave** annealer computer with 5.5 billion qubits, far from the existing 5000<sup>1351</sup>. A D-Wave of 5893 qubits could do the job if all qubits could be arbitrarily coupled to the other, which is not possible due to the chimera design of D-Wave chipsets, and most other types of qubits for that matter. And trapped ions and their any-to-any connectivity won't save us since they don't seem to scale. Shor's menace is visualized over time in this diagram from the European standardization organization ETSI<sup>1352</sup>. It is based on very optimistic predictions about the capabilities of quantum computers to exploit Shor's algorithm. The orange part of the graph should be shifted into the future by at least 5 to 10 years.



Shor's algorithm applied to RSA public key breaking could however have quite a negative impact on most Internet use cases. It is indeed integrated in the **TLS** and **SSL** protocols that protect websites and file transfers via **HTTPS** and **FTP**, in the **IPSEC** protocol that protects IP V4 in the IKE sub-protocol, in the **SSH** protocol for machines remote access and in the **PGP** protocol that is sometimes used to encrypt emails. RSA and derivatives are also used in many **HSM** (Hardware Security Modules) such as in cars ECU (Electronic Central Units)<sup>1353</sup>.

The threat also concerns software **electronic signatures** and therefore their automatic updates, **VPNs** used for remote access to protected corporate networks, email security with **S/MIME**, various **online payment** systems, **DSA** (Digital Signature Algorithm, an electronic signature protocol), **Diffie-Hellman** codes (used for sending symmetrical keys) as well as **ECDH**, **ECDSA** and **3-DES** elliptic curve cryptography. The **Signal** protocol used in Whatsapp would also be in the spotlight. So a lot of Internet security is more or less in the line of sight.

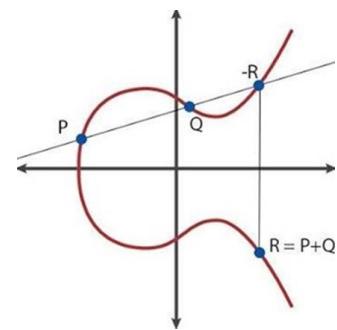
<sup>1351</sup> According to [High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311](#) by Nike Dattani, Xinhua Peng and Jiangfeng Du, June 2017 (6 pages).

<sup>1352</sup> See [Quantum Safe Cryptography and Security](#), 2015 (64 pages).

<sup>1353</sup> See [Post-Quantum Secure Architectures for Automotive Hardware Secure Modules](#) by Wen Wang and Marc Stöttinger, 2020 (7 pages).

ECC (Elliptic Curve Cryptography) is the first algorithm with elliptic curves, created in 1985 by Neal Koblitz and Victor Miller. The most common variants today are **ECDH** (Elliptic-curve Diffie-Hellman) and **ECDSA** (Elliptic Curve Digital Signature Algorithm, launched in 2005).

These variants were deployed from 2005 and more widely only from 2015, so 30 years after the creation of the first ECC! Incidentally, the elliptic curves allowed Andrew Wiles to demonstrate the Fermat's last theorem in 1992, which has nothing to do with cryptography<sup>1354</sup>.



One of the interests of elliptic curve-based codes is to use shorter public keys than with RSA encryption. But these elliptic curves are also breakable with quantum computing with a reasonable time because of our friend Peter Shor and the resolution of the discrete logarithm problem (DLP)<sup>1355</sup>. Moreover, an ECDSA backdoor was revealed by Edward Snowden in 2013, housed by the NSA in its Dual EC DRBG random number generator and not in the elliptic curve itself. It was then recommended by NIST in 2014 and NSA in 2015 for the transmission of sensitive information<sup>1356</sup>.

The other reason for alternative cryptography solutions is that today's sensitive communications can be stored for a long time by private or state hackers, and exploited much later, when quantum computers are up to the task. Some present day information may have some value later, whether it is financial transactions, private communications, trade secrets or other state secrets. And forward secrecy, a feature used to protect the transport layer like SSL used with HTTPS with separate keys for each session, is not enough against quantum computing-based attacks. Quantum computing is thus a veritable sword of Damocles whose fall is difficult to predict and rather distant in time by at least a good decade. Beyond that time, it is almost impossible to make sound predictions.

### Mosca's inequality

**Michele Mosca** created an inequality that explains the time risk. It is expressed in the form  $D+T > G_c$ , where D is the length of time during which today's data circulating in encrypted form must be secured, T, the time needed to make my transition from its encryption systems to solutions resistant to quantum computing, and  $G_c$ , the time it will take to develop quantum computers capable of breaking the public keys of current encryption systems. You specify D. You can plan for T according to your information systems and available commercial solutions and standards. How about  $G_c$ ? You have to evaluate it with your gut feeling because current estimates span from 5-10 years to... never!

For example, some researchers from the UK and USA tried in 2020 to predict when a FTQC would show up<sup>1357</sup>. With a sort of logistic regression, their model predicted that proof-of-concept fault-tolerant quantum computers will be developed between 2026 and 2033 with 90% confidence with the median in early 2030, and that RSA-2048 Shor attacks will become feasible between 2039 and 2058 with a 90% confidence and median in 2050. Making predictions with such a method for a 30 years timeframe seems preposterous.

---

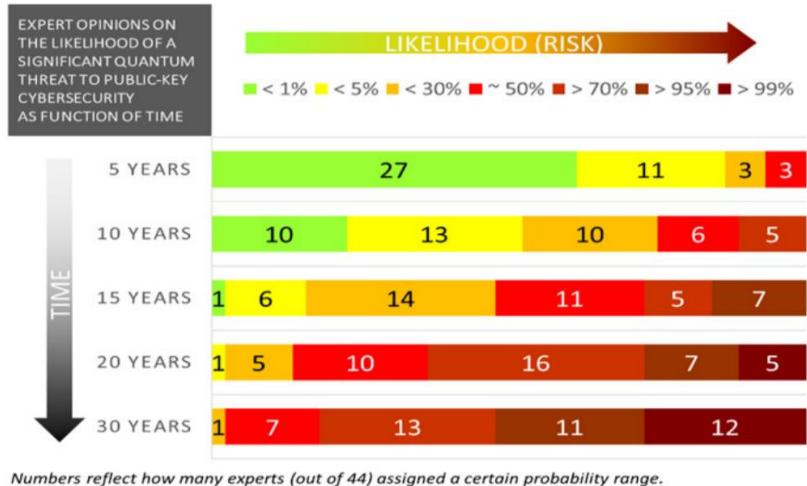
<sup>1354</sup> As in [Elliptic curves cryptography and factorization](#) (86 slides).

<sup>1355</sup> As documented in [Shor's discrete logarithm quantum algorithm for elliptic curves](#) by John Proos and Christof Zalka, 2003 (34 pages). The discrete log problem consists in finding an integer k verifying  $a^k = b$  modulo p, a, b and p being known integers. This allows to break the elliptic and Diffie-Hellman curve keys.

<sup>1356</sup> See Ben Schwennesen's [Elliptic Curve Cryptography and Government Backdoors](#), 2016 (20 pages).

<sup>1357</sup> See [Forecasting timelines of quantum computing](#) by Jaime Sevilla and C. Jess Riedel, December 2020 (23 pages).

The report [Quantum Threat Timeline Report 2020](#), Michele Mosca and Marco Piani from evolutionQ (52 pages) collected in 2020 the opinion from 44 experts on the potential advent of a quantum threat to public-key cryptography. We see a broad spectrum ranging from 3 experts thinking that it would materialize in fewer than 5 years and most of them thinking it would do so before 30 years. All-in-all, the best prediction should be: “we don’t know”!



### Grover, Dlog and Simon

Symmetric cryptography systems are not affected by Shor's algorithm. These include the **Data Encryption Standard** (DES) which uses keys of 64 bits or more and is outdated, replaced by the **Advanced Encryption Standard** (AES) which has been a US government standard since 2002, with private keys ranging from 128 to 256 bits.

To date, the best quantum breaking algorithms for symmetric AES keys would take more than the age of the Universe (13.8 billion years) to run on 128-bit keys. With AES-256 bits, we are therefore in peace! They are based on mechanisms that are quite different from the mathematical problem-solving of public key ciphers.

Keys are shared upstream of the exchanges and are generally themselves encrypted with the asymmetric **Diffie-Hellman** algorithm. But this Diffie-Hellman encryption is based on elliptic curves, which is breakable by Shor's algorithm. The problem lies then with the vulnerability of the majority of encryption systems using asymmetric keys which are used to share symmetric keys.

A hash function converts data of arbitrary size such as a file to a number of fixed size. This makes it possible to do quick searches to compare files. For example, it can be used to check that a file has not been altered during transmission.

SHA algorithms (Secure Hash Algorithms) are standard hash functions that consist in replacing data of arbitrary size by a unique key size.

The **SHA-1** hash algorithm is resistant to Shor's algorithm, but it has been broken by other methods and is therefore considered outdated. It is the **SHA-3** which is the most up-to-date and since 2015. The SHA algorithm can be broken by Grover's search algorithm, but with a large number of logical qubits, at least 6,000 logical qubits for common keys<sup>1358</sup>. This represents an order of magnitude close to the qubit requirements for breaking RSA keys with Shor's algorithm.

<sup>1358</sup> Based on [Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3](#), 2016 (21 pages), which is also the source of the table on this page.

For example, a hash key or fingerprint can be used to verify the integrity of content such as software or simply a password.

The problem is to resist collisions, i.e., methods to find or create an object whose fingerprint would be the one you have, which is quite different from finding the original object (like an image) from its fingerprint, which is rather difficult.

	SHA-256	SHA3-256
Grover	$T\text{-count}$	$1.27 \times 10^{44}$
	$T\text{-depth}$	$3.76 \times 10^{43}$
	Logical qubits	2402
	Surface code distance	43
	Physical qubits	$1.39 \times 10^7$
Distilleries	Logical qubits per distillery	3600
	Number of distilleries	1
	Surface code distances	{33, 13, 7}
	Physical qubits	$5.54 \times 10^5$
Total	Logical qubits	$2^{12.6}$
	Surface code cycles	$2^{153.8}$
	Total cost	$2^{166.4}$
		$2^{166.5}$

Table 3. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.

The number of qubits needed to break keys depends on the size of the key. SHA-1 and SHA-2 have small key sizes that can be recovered in a reasonable time with **Grover's** quantum search algorithm, but this is not the case for SHA-3 which exploits larger keys. This is the same logic as for AES.

At last, let's also mention **Shor's Dlog** (discrete log) algorithm that threatens Digital Signature Algorithms, Diffie-Hellman key exchanges and El-Gamal encryption. And **Simon's** algorithm can also break Even-Mansour ciphers that are used in some disk encryption solutions, although with a lot of caveats, the attacker needing to encrypt a superposition of inputs all with the same keys<sup>1359</sup>. All in all, Shor is not the only quantum threat on cybersecurity!

#### Peter Shor factoring algorithm - 1994

integer factoring  
exponential acceleration

$$O\left(\frac{\sqrt{N}}{2}\right) \Rightarrow O(\log(N)^3)$$

**threatens public key based cybersecurity**

RSA, ECDH, ECDSA, SSL/TLS, VPNs (IPSEC), SSH, PGP, S/MIME, Signal (Whatsapp), Bitcoin & Blockchain signatures

#### Peter Shor dlog algorithm - 1994

exponential acceleration

$$O\left(\frac{\sqrt{N}}{2}\right) \Rightarrow O(\log(N)^3)$$

**threatens Digital Signature Algorithm, Diffie-Hellman key exchanges and El-Gamal encryption**

#### Lov Grover search algorithm - 1996

brute force to break symmetric codes  
polynomial acceleration

$$O(N) \Rightarrow O(\sqrt{N})$$

**threatens symmetric keys cybersecurity**

improves brute force attack of hash functions (SHA) and block ciphers (AES) used in symmetric encryption

#### David Simon algorithm - 1996

exponential acceleration

$$O(2^N) \Rightarrow O(N)$$

**Even-Mansour ciphers used in some disk encryptions**

(cc) Olivier Ezratty, July 2021

## Blockchain and Cryptocurrencies vulnerabilities

What about **Bitcoin**, other crypto-currencies and the **Blockchain**? The answer is summarized *below* with a good inventory of the cryptosystems used by use as a starting point<sup>1360</sup>.

Otherwise, experts have opposite views on the quantum risk, from let's forget it<sup>1361</sup> to it will come sooner than expected<sup>1362</sup>.

<sup>1359</sup> See [Breaking Symmetric Cryptosystems Using Quantum Algorithms](#) by Gaëtan Leurent with Marc Kaplan, Anthony Leverrier and María Naya-Plasencia (58 slides).

<sup>1360</sup> The answer is well documented in [The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption](#) by Long Finance, 2018 (60 pages).

Basically, the Blockchain is based on a patchwork of cryptographic algorithms including AES, RSA and SHA-3. It uses a hash algorithm to ensure the integrity of the chain of trust, and a digital signature to authenticate new transactions that are incrementally added to the Blockchain.

Bitcoin uses a SHA-256 crypto hash, which is quantum resistant, and a signature that exploits ECDSA elliptic curves, which is not.

**Table 3. Main Algorithms Types Used for Cryptography, and Uses For Smart Ledgers<sup>19</sup>**

Type of Algorithm	General Use	Example Algorithms of This Type	Example Uses for Smart Ledgers
Symmetric	Secret communications	AES, DES, 3DES, RC4	Protection of resources stored on ledger
Public key	Secret communications (including key exchange) or digital signature	RSA, Diffie-Hellman, El Gamal, ECDSA	User authentication; signature of transactions, data or software
Hash	Generating fixed-length digest of arbitrary-length text	SHA-256, SHA-512, SHA-3	Ensuring authenticity of blockchain

In a similar manner, **Ethereum** uses a quantum resistant SHA-3 hash and a vulnerable ECDSA signature. However, an Eth2 upgrade to Ethereum published in 2021 has replaced ECDSA based signatures by Lamport Q-R signatures which are quantum safe, with the inconvenient of being very large (over 200 times bigger than an ECDSA signature).

A recent review paper lists Bitcoin, Ethereum, Litecoin, Monero and ZCash as highly vulnerable to Shor's algorithm and all these, except Monero, to be moderately vulnerable to Grover search<sup>1363</sup>.

All in all, quantum computing will not allow to alter the Blockchain nor the proof of work used by Bitcoin which relies on the repeated use of quantum-resistant hash. The vulnerability of the Blockchain lies in the signature that relies on the ECDSA elliptic curve algorithm which can be broken with Shor's algorithm. This would make it possible to impersonate someone else in a transaction involving a Blockchain or Bitcoins. That's still whole lot of potential troubles! For example, if a Bitcoin transaction was intercepted to retrieve the sender's ECDSA signature, it could be exploited to transfer Bitcoins from that sender's wallet.

Workarounds can obviously be created until a quantum threat to transaction integrity is confirmed. This can be done by encrypting the signatures used by the blockchains with a PQC system, as we'll see later<sup>1364</sup>.

It is also possible to encrypt the data circulating in a Blockchain with a quantum computationally resistant algorithm such as AES-256, with the disadvantage that it is symmetrical and therefore requires keys to be exchanged beforehand. However, there are already some workarounds. A protocol using a longer validation time for Bitcoin transactions would allow to bypass the use of integer factoring to break the Bitcoin electronic signature algorithm, ECDSA<sup>1365</sup>. But this would only amplify a key flaw of Bitcoin as a currency: a lengthening of transaction times that are already far from real time!

<sup>1361</sup> See [Here's Why Quantum Computing Will Not Break Cryptocurrencies](#) by Roger Huang, December 2020.

<sup>1362</sup> See [Q-Day Is Coming Sooner Than We Think](#) by Arthur Herman, Forbes, June 2021. It mentions a crack of a RSA-2048 bit encryption key in 10s with 4,099 stable qubits without mentioning the source of this performance. I have searched it and didn't found the source reference of these 10 seconds mentioned in various places. The only detail is it would require a perfect quantum computer executing one million operations per second.

<sup>1363</sup> See [Vulnerability of blockchain technologies to quantum attacks](#) by Joseph J.Kearney et al, 2021 (10 pages).

<sup>1364</sup> See [Blockchained Post-Quantum Signatures](#) by Chalkias Browny Hearnz, 2018 (8 pages).

<sup>1365</sup> It is documented in [Committing to Quantum Resistance A Slow Defence for Bitcoin against a Fast Quantum Computing Attack](#), 2018 (18 pages).

Bitcoin mining is potentially vulnerable by Grover's algorithm although its real practical speedup on a LSQC (large scale quantum computer) is questionable. Researchers are proposing some changes in the rules (and timing) applied by miners to mitigate this threat<sup>1366</sup>.

We can also mention the open-source Blockchain project resisting quantum attacks, [Quantum Resistant Ledger](#). It is based on the XMSS (Extended Merkle Signature Scheme) electronic signature protocol<sup>1367</sup>.

There is also a risk of attack at the mining level, with Grover's algorithm. But here again, there are solutions available<sup>1368</sup>. The **Long Finance** document from which this table is extracted summarizes all these risks on Smart Ledgers by separating the transactions that are relatively protected and those that rely on vulnerable electronic signatures that are not vulnerable to hacking of the SSL and TLS protocols<sup>1369</sup>.

#### The Quantum Countdown Quantum Computing And The Future Of Smart Ledger Encryption

**Table 4. Risks to Blockchain Architectures from Quantum Computing**

	Transactions	Data on Blockchain	Software on Blockchain
Read historical records without authorization	No (blockchains are intended to allow access to transaction information)	No, unless confidential and secured with vulnerable cryptography	No, unless confidential and secured with vulnerable cryptography
Alter historical records	No	No	May be able to run software without authorisation if signature used
Spoof ongoing records	Yes, possibly	Yes, possibly	Yes, possibly

This section on threats would not be complete without mentioning the disagreements between cybersecurity specialists. Some are rather conservative and consider that one should not touch too much of what works well. They think Shor's threat is exaggerated. Others, such as the NIST in the US, are more alarmist and believe that the most critical cryptographic systems should be updated as soon as possible<sup>1370</sup>. And we also have arguments between the compared advantages of QKD and PQC, the two systems that can protect cybersecurity from quantum computing.

## Quantum Random Numbers Generators

Quantum, post-quantum and traditional cryptographic systems are all fed by random number generators. They have been around for ages. Random numbers are also used in a large set of applications beyond classical cryptographic protocols. It includes gaming and casinos to draw lottery winning numbers, playing card shuffling, and various bets-related numbers, statistical analysis like the ones using Monte Carlo simulations in the finance sector, selecting random samples from large data sets like with machine learning, various scientific simulations and testings (like the [Wheeler which-way or delay-choice experiment](#) we already described), and smart networks simulations.

<sup>1366</sup> See [On the insecurity of quantum Bitcoin mining](#) by Or Sattath, February 2019 (22 pages).

<sup>1367</sup> See also [Blockchain Post-Quantum Signatures](#) by Chalkias Browny Hearnz, 2018 (8 pages).

<sup>1368</sup> See [On the insecurity of quantum Bitcoin mining](#) by Or Sattath, February 2019 (22 pages).

<sup>1369</sup> For more information, see also [The quantum threat to payment systems](#) by Michele Mosca of the University of Waterloo, 2017 (52 minutes). Mosca is one of the world references in the quantum cryptography field. See also [The Quantum Countdown Quantum Computing And The Future Of Smart Ledger Encryption](#), Long Finance, February 2018 (62 pages).

<sup>1370</sup> Analysts are amplifying the fear, as in [Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity](#) from Hudson Institute, a US conservative think tank, March 2019 (24 pages), [Preparing Enterprises for the Quantum Computing Cybersecurity Threats](#) by CSA, May 2019 or [Global Risk Report 2020](#) from the World Economic Forum.

In all these use cases, the main concern is to create truly random numbers. Namely sequences of 0s and 1s without repetitions of any sequence and a balanced proportion of 0 and 1, as in the decimals of  $\pi$ . These numbers generation processes must also be non-deterministic, not reproducible and with no correlations, meaning that series of randomly generated numbers must be statistically independent. We could indeed generate good random numbers but if they were similar in time, it wouldn't be satisfactory at all.

Unfortunately, most commonly used random number generators are pseudo-random and happen to be deterministic. These are branded **PRNGs** (Pseudo-Random Number Generators).

Some mathematical formula deterministically produces a series of number and some randomness is introduced by using as seed parameters some highly variable elements such as time with a millisecond precision, GPS coordinates, thermal noise or other contextual information. It still generates deterministic sequences of numbers with some repeat period, although passing regular randomness tests successfully.

Most PRNG systems now use a randomness extractor merging the output of a random entropy source and a short random seed. Despite these initialization variables and various tricks of the trade, common random number generators still create some periods within their generated numbers<sup>1371</sup>. Still, it may be useful to use deterministic RNGs in some cases where reproducibility is mandatory. Also, PRNGs have the advantage to be fast<sup>1372</sup>.

To avoid determinism, we must use a truly random physical process for the generation of numbers, aka **TRNGs** (True Random Number Generators), based on some chaotic physical phenomenon. One common technique consists in measuring the thermal noise of an electronic component or the atmospheric electromagnetic noise<sup>1373</sup>. Thermal noise TRNGs are implemented in most microprocessors like those from **Intel** since 2013 and from **AMD** since 2015 but with various identified weaknesses<sup>1374</sup>. It can for example rely on voltage randomness in resistive materials (Johnson's effect), Zener noise in diodes or, more commonly, on some amplified free-running oscillator.

So here come **QRNGs** (Quantum Random Number Generators), a subclass of TRNGs. They rely on quantum physics laws and one that is particularly important: Born's probability rule, based on Schrödinger's wave equation. It replaces a generic chaotic system by a non-deterministic measurement of a physical property of some quantum objects, usually individual photons. In quantum physics, a quantum object's properties measurement is intrinsically random, at least, as far as we know.

Quantum is the kingdom of randomness! But this randomness is not a guarantee to obtain truly nondeterministic random numbers. There are weaknesses in all these systems, particularly with their classical or semi-classical components like the beam splitters or photon detectors it is using, or with the software part handling the so-called randomness extraction. Its consequence is an intense competition between QRNG vendors. They all claim to generate "truly" random numbers contrarily to their QRNG competitors.

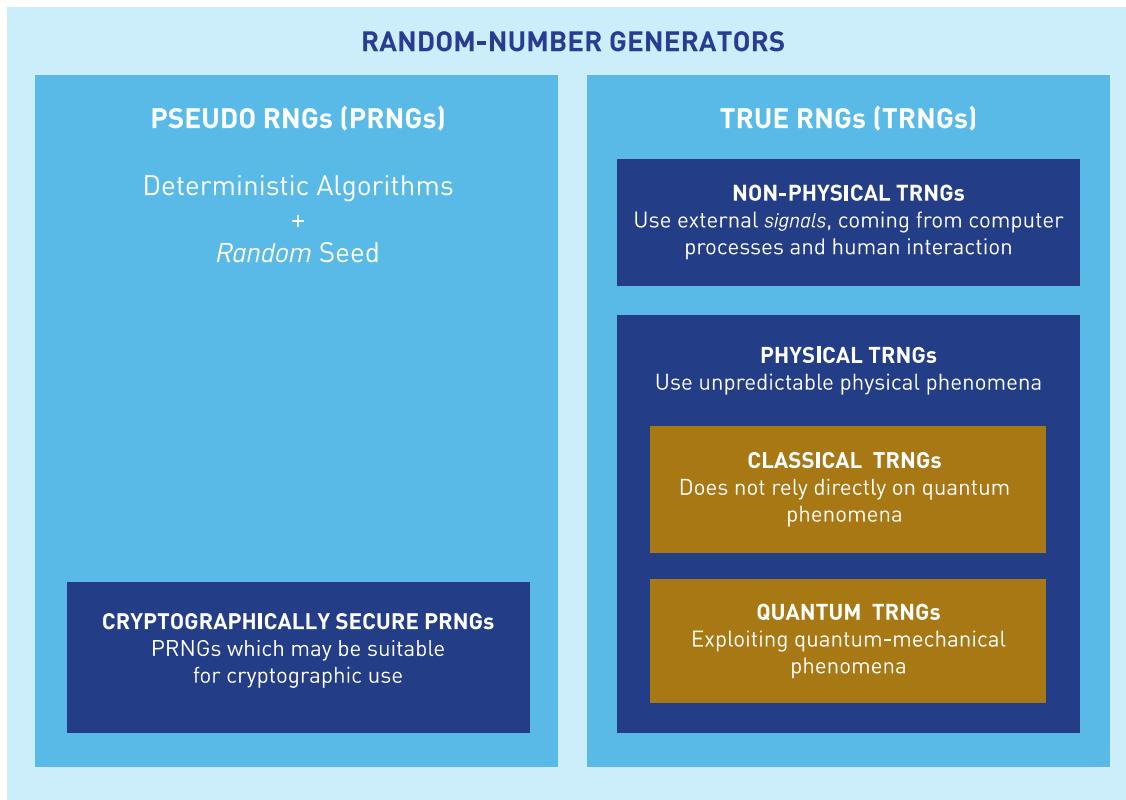
---

<sup>1371</sup> However, there are still other solutions for generating non-quantum random numbers that need to be equally random, although this is still questionable. See for example [Scientists Develop 'Absolutely Unbreakable' Encryption Chip Using Chaos Theory](#) by Davey Winder, 2019.

<sup>1372</sup> Illustration source: [Quantum Random-Number Generators: Practical Considerations and Use Cases Report](#) by Marco Piani, Michele Mosca and Brian Neill, EvolutionQ, January 2021 (38 pages). This is the best document I found that explains the various subtleties of QRNGs, particularly about the device dependent and device-independent species.

<sup>1373</sup> Atmospheric noise is used by the service [random.org](#) operated by Randomness and Integrity Services Ltd (1998, Ireland).

<sup>1374</sup> Since 2013, Intel processors have been using the RDRAND function that is part of their 32 and 64 bits instruction set, returning a random number generated by an on-chip thermal noise based entropy source. AMD provides support for this instruction set since June 2015.



Many differentiation features are also important: the random numbers generation rate (in bits/seconds, some applications may be very demanding), the time it takes to warm up and stabilize the system (some QRNGs are slow to warm-up and may require hours to stabilize), is it device independent (impacts randomness quality but also RNG rates; but no such commercial systems are available yet), certifiability (some are black-boxes that are really difficult to audit, others are said to be self-certified) and other standard characteristics that may be important depending on the use case (weight, size, price and power drain).

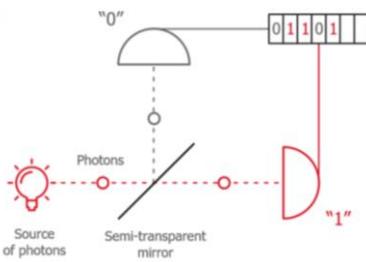
At last, vendor trust is a key criterion, particularly when you discover that some Switzerland cybersecurity products contained backdoors created on behalf of the CIA<sup>1375</sup>. It also explains why, whatever the technology used, western countries may not and probably should not rely on Chinese or Russian TRNG/QRNG vendors.

It's now up to you to understand how these systems are benchmarkable and benchmarked to figure out whether such and such QRNG is safe or not. Many different QRNG techniques have been created to date. The most commonplace are those using photons, with components that are now easy to miniaturize, even in a smartphone.

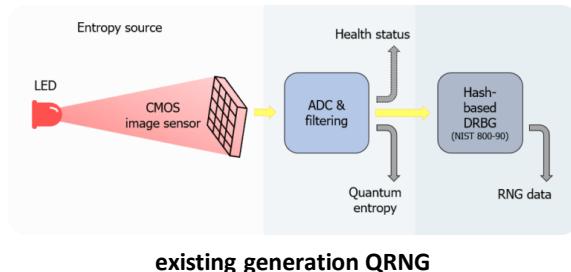
**Photons counting** is the most common method, based on the measurement of single photons emitted individually in series, passing through a regular balanced beam splitter and analyzed by two detectors<sup>1376</sup>. The series of generated 0s and 1s are theoretically random. Quantum physics mathematical formalism and experiments say so!

<sup>1375</sup> See [The intelligence coup of the century' - For decades, the CIA read the encrypted communications of allies and adversaries](#) by Greg Miller, Washington Post, February 2020. It deals with the Crypto AG company created in 1952 and dissolved in 2018.

<sup>1376</sup> See [Quantum Random Number Generators](#) by Miguel Herrero-Collantes, 2016 (54 pages). This setting is frequently referred to as a welcher-weg experiment, or “which way” experiment.



**first generation QRNG**



**existing generation QRNG**



USB (legacy)



**250 kbits/s to 19.64 Mbits/s  
of real random numbers**



network appliance

Each detected photon creates at most only one bit, but not all photons are detected. The detection speed is limited by the photon detectors bandwidth and their saturation level. This QRNG technique was pioneered by **IDQ** (Switzerland) in 2001.

One of its shortcomings is the used light source that can't necessarily be certified. In some products, there's also some warm-up time before real random numbers can be generated. Some solutions can certify the numbers generation randomness in such situation, like using a first beam splitter and detector before photons are separated by a polarizing beam splitter<sup>1377</sup>.

Nowadays, photon counting is (seemingly) done without a polarizing beam splitter. The light source is some LED diode, lighting a small CMOS image sensor, and generating "shot noise". That's what IDQ is now selling with its miniaturized Quantis chipset. It's adapted to mass market use cases, in smartphones, laptops and car. Such QRNG first appeared in a consumer product in 2020 in a version of the **Samsung Galaxy A71 5G** smartphone called **Galaxy A Quantum**, marketed by **SK Telecom** only in Korea. It probably won't change much in terms of user security, but it can make a lasting impression.

In April 2021, Samsung announced a new version of this smartphone, the **Galaxy Quantum2**, adapted to 5G and with similar QRNG features using an IDQ Quantis chipset<sup>1378</sup>. The same chipset is found in a Vsmart Aris 5G smartphone, coming from Vietnam! **Q→NU**, **CryptaLabs** and **Qrypt** are also commercializing such type of QRNGs.

**Photon arrival time** aka "time bin qubits" is about evaluating the arrival time of successive single photons in a simpler setting coupling a photon source like a LED or a laser and a photon counter to a high-resolution counter, down to a couple nanoseconds<sup>1379</sup>. Practically, randomness comes from evaluating the variation of this arrival time compared with the decaying exponential waiting-time distribution.

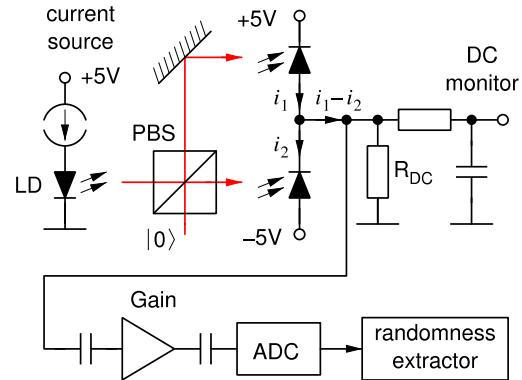
<sup>1377</sup> See [Using the unpredictable nature of quantum mechanics to generate truly random numbers](#) by Bob Yirka, 2021 that refers to [Certified Quantum Random Numbers from Untrusted Light](#) by David Drahic, December 2020 (32 pages). Its RNG output is 8.05 Gb/s.

<sup>1378</sup> The QRNG chipset is a square of 2.5mm creating random codes by capturing noise from an LED and a CMOS sensor.

<sup>1379</sup> See [Photon arrival time quantum random number generation](#) by Michael A. Wayne et al, 2009 (7 pages) which describes the principles of this random numbers generation methods.

The system can also use a photon counting setting with a regular beam splitter and two photon detectors coupled each with a counter<sup>1380</sup>. It has low latency and is quickly up to speed. **Qnu Labs**, **PicoQuant** and **QuTools** are providers of such QRNGs. A variation of this technique recently developed uses a LED light illuminating a matrix of SPADs (single photon avalanche detectors) on a CMOS circuit, with a RNG capacity of 400 Mbit/s<sup>1381</sup>.

**Quantum vacuum fluctuations** uses a balanced homodyne measurement of vacuum fluctuations of the electromagnetic field contained in the radio-frequency sidebands of a single-mode (usually 780 nm) laser diode<sup>1382</sup>. Two diodes compute the difference of the signals coming from the two exits of a polarizing beam splitter and the resulting signal is amplified and digitized, to be processed by a randomness extractor. Such a QRNG system is implemented in a web site run by ANU (Australian National University) with the qStream QRNG from **Quintessence Labs**, which generates keys at a >3.5 Gbps rate<sup>1383</sup>.



**Spontaneous emission** uses amplified spontaneous emission, detection and digitization of optically filtered amplified spontaneous emission noise from a light source such as superluminescent diode (SLD).

**Phase noise** and **phase diffusion** (PD-QRNG<sup>1384</sup>) are variations of spontaneous emission QRNGs. It uses a photons counting method variation proposed in 2009<sup>1385</sup>. In one implementation, a VCSEL laser (single mode vertical cavity surface emitting laser) is associated with a phase noise measurement using a delay self-homodyne method.

The photons from the laser are traversing a beam splitter. Among its benefits are a very high-bit rate, of several tens of Gbits/s of random bits. The technique is used by vendors like **Quside**, **Quan-tumeMotion** and **Kets**.

One way goes to the next beam splitter, and the other traverses a delay line, and is then merged back with the main line. An APD (avalanche photodetector), then counts the exiting photons and its signal is converted from analog to digital with an ADC<sup>1386</sup>.

<sup>1380</sup> See [First high-speed quantum-safe randomness generation with realistic devices](#), NTT, February 2021, which refers to [A simple low-latency real-time certifiable quantum random number generator](#) by Yanbao Zhang et al, 2021 (8 pages).

<sup>1381</sup> See [A High Speed Integrated Quantum Random Number Generator with on-Chip Real-Time Randomness Extraction](#) by Francesco Regazzoni et al, February 2021 (9 pages).

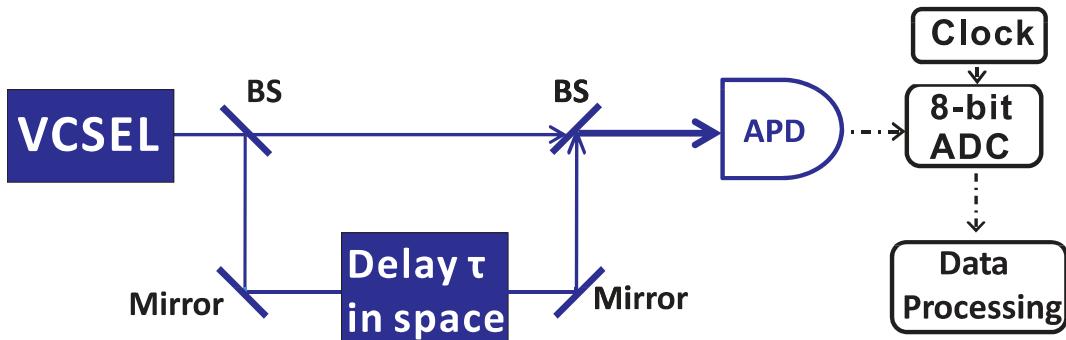
<sup>1382</sup> A homodyne measurement consists in extracting information encoded as modulation of the phase and/or frequency of an oscillating signal. In the mentioned case, it's the phase. See an example in [Random numbers from vacuum fluctuations](#) by Yicheng Shi et al, 2016 (5 pages) and in [A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers](#) by Francesco Raffaelli et al, University of Bristol, Quantum Science and Technology, February 2018 (10 pages).

<sup>1383</sup> See <https://qrng.anu.edu.au/> and [Real time demonstration of high bitrate quantum random number generation with coherent laser light](#), by T. Symul et al, 2021 (4 pages) and [Maximization of Extractable Randomness in a Quantum Random-Number Generator](#) by J. Y. Haw, 2015 (13 pages). The operations are linked to the offer of QuintessenceLabs.

<sup>1384</sup> See [Quantum entropy source on an InP photonic integrated circuit for random number generation](#) by Carlos Abellan et al, Optica, 2016 (7 pages) and [Real-time interferometric quantum random number generation on chip](#) by Thomas Roger et al, Journal of Optical Society, 2019 (7 pages).

<sup>1385</sup> In [Experimental demonstration of a high speed quantum random number generation scheme based on measuring phase noise of a single mode laser](#) by Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo and Li Qian, 2009 (7 pages).

<sup>1386</sup> See [Truly Random Number Generation Based on Measurement of Phase Noise of Laser](#) by Hong Guo et al, Peking University, January 2010 (4 pages).



**Radioactive decay** was one of the first developed QRNG technologies, based on the random timing of decay of particular radioactive atoms, detected with a Geiger counter. It has limited bit rates and is not widely used, on top of being not very practical to implement given it's based on radioactive materials. There is however a vendor in that space, **EYL**.

Other various techniques are mentioned but seemingly not widely used: **laser chaos** that creates a time-delayed optical feedback via a reflector, **raman scattering**, **attenuated pulse** and **Optical Parametric Oscillators (OPO)**.

Another technique consists in merging in a single platform several QRNG methods. That's what a Chinese team released in July 2021 on an Alibaba Cloud server, mixing four types of QRNGs: single-photon detection, photon-counting detection, phase-fluctuations and vacuum-fluctuations<sup>1387</sup>. Three of these QRNG sources were off-the-shelf (Quantis-PCIe-16M from ID Quantique, QRG-100E from QuantumCTeck and QRN-16 from MPD).

**Device Independence** deals with the difference between randomness and privacy. A SDI (source device independent) QRNGs ensures private randomness, where the created random numbers can't be known by any adversary. With SDI QRNGs, the randomness source is assumed to be untrusted but the measurement devices are trusted. It's more secured than a trusted device or device dependent QRNG where the device is well characterized and trusted.

These have a high bit rate in the Gbits/s range while SDI QRNGs have a much lower bit rate, in the kbits/s range due to a more complicated setup. SDI QRNG can rely on entanglement and non-locality or be based on quantum computation (this is a variation of the qubit measurement technique mentioned above). SDI QRNG enables real-time estimate of the output entropy which can quantify and certify the QRNG randomness without possessing a detailed knowledge of the entropy source device. The device independence certification comes with loophole free violation of Bell's inequalities. A record rate of 17 GBits/s key generation with a SDI-QRNG was obtained in 2018 in an Italian lab<sup>1388</sup>. It was also experimented in a highly integrated photonic circuits, using a self-tested randomness expansion protocol with multi-dimensional encoding<sup>1389</sup>.

There are also MDI-QRNGs, where the source is trusted and the measurement device is untrusted. It is for example used with time-bin QRNGs with a testing mode used to create a 4-quantum states ( $|0\rangle$ ,  $|1\rangle$ ,  $|+\rangle$  and  $|-\rangle$ ) tomography<sup>1390</sup>.

<sup>1387</sup> See [Quantum random number cloud platform](#) by Leilei Huang, Hongyi Zhou, Kai Feng and Chongjin Xie, Nature, July 2021.

<sup>1388</sup> See [Source-device-independent heterodyne-based quantum random number generator at 17 Gbps](#) by Marco Avesani et al, 2018 (7 pages). It uses a POVM measurement of continuous variable observables.

<sup>1389</sup> See [Multidimensional quantum entanglement with large-scale integrated optics](#) by J. Wang et al, Science, 2018 (24 pages).

<sup>1390</sup> See [Experimental measurement-device-independent quantum random number generation](#) by You-Qi Nie et al, China, 2016 (16 pages).

**Qubits measurement** is a more generic way of generating quantum randomness than photon counting after traversing a polarizing beam splitter. It uses gates-based quantum processing units applied to one or several qubits and creating superposition. The simplest is a single Hadamard gate, but it's not sufficient to create enough randomness. The common practice is to create entangled states, or Bell states, which is done combining Hadamard and CNOT gates<sup>1391</sup>. The useful states are those where there is some correlation or anticorrelation between the qubits from a Bell pair, showing that they were random. CQC (UK) is providing such a solution running on superconducting qubits in the cloud, in partnership with IBM. Still, I don't know how these solutions are certified and we're back at studying the real randomness, non-determinism and weaknesses of qubits preparation sources (microwaves, lasers) as well as qubit readout techniques (microwaves readouts, CCD/CMOS readouts for cold atoms, trapped ions and NV centers, and single photon detectors for photon qubits).

**Quality.** Quantum random numbers generators are not equal. The source may be a true RNG but other components may contain weaknesses and be hacked in some circumstances: the photon source<sup>1392</sup>, the photon measurement system which could deviate or be defective, and at last randomness extractor various other weaknesses. Also, it can be difficult to distinguish classical hardware noise from the quantum randomness coming from the QRNG in evaluation tests.

**Evaluation.** Random series of numbers must be incompressible. This algorithmic randomness can be tested with Borel normality. An infinite sequence of binary numbers is random if every binary string of length  $n$  appearing in the sequence has a frequency of  $2^{-n}$ .

There are various tests of algorithmic randomness like the NIST SP 800-22 1A Test<sup>1393</sup>. It contains 15 tests but other tests suites exist that complement the NIST set, totaling 40 tests<sup>1394</sup>.

Test	Defect detected	Property
Frequency (monobit)	Too many zeroes or ones	Equally likely (global)
Frequency (block)	Too many zeroes or ones	Equally likely (local)
Runs test	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (locally)
Longest run of ones in a block	Oscillation of zeroes and ones too fast or too slow	Sequential dependence (globally)
Binary matrix rank	Deviation from expected rank distribution	Linear dependence
Discrete fourier transform (spectral)	Repetitive patterns	Periodic dependence
Non-overlapping template matching	Irregular occurrences of a prespecified template	Periodic dependence and equally likely
Overlapping template matching	Irregular occurrences of a prespecified template	Periodic dependence and equally likely
Maurer's universal statistical	Sequence is incompressible	Dependence and equally likely
Linear complexity	Linear feedback shift register (LFSR) too short	Dependence
Serial	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Approximate entropy	Non-uniformity in the joint distribution for m-length sequences	Equally likely
Cumulative sums (cusum)	Too many zeroes or ones at either an early or late stage in the sequence	Sequential dependence
Random excursions	Deviation from the distribution of the number of visits of a random walk to a certain state	Sequential dependence
Random excursions variants	Deviation from the distribution of the number of visits (across many random walks) to a certain state	Sequential dependence

Recent TRNG/QRNG benchmarking tools use machine learning techniques and a convolutional network to detect patterns in the generated numbers<sup>1395</sup>. However, while these tests may detect weaknesses in QRNG randomness, it won't ensure real nondeterminism. Other tests are required, like loophole free Bell tests, already mentioned.

<sup>1391</sup> See [Quantum random number generators with entanglement for public randomness testing](#) by Janusz E. Jacak et al, 2020 (9 pages) and [Reference Standard RS-EITCI-QSG-EQRNG-PROTOCOLS-STD-VER-1.0](#), EITCI, 2019 (21 pages).

<sup>1392</sup> See for example [QRNG: Out-of-Band Electromagnetic Injection Attack on a Quantum Random Number Generator](#) by P.R. Smith et al, January 2021 (12 pages).

<sup>1393</sup> See [A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications](#) by Andrew Rukhin et al, NIST, 2010 (131 pages). Then, [Experimentally probing the algorithmic randomness and incomputability of quantum randomness](#) by Alastair Abbott, Cristian Calude and al, UGA/Institut Néel France and University of Auckland, 2018 (17 pages) and [Recommendations and illustrations for the evaluation of photonic random number generators](#) by Joseph D. Hart et al, 2017 (29 pages).

<sup>1394</sup> See [Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators](#) by Charmaine Kenny, April 2005 (107 pages).

<sup>1395</sup> See [Machine Learning Cryptanalysis of a Quantum Random Number Generator](#) by Nhan Duy Truong et al, 2019 (13 pages) and [Benchmarking a Quantum Random Number Generator with Machine Learning](#), 2020 (26 slides).

**KQD or PQC?** We'll describe these two cryptography solutions later on. Which one will make use of QRNGs? Post-quantum cryptography requires large classical random keys, so QRNGs will be very useful, particularly those who have a large throughput. Quantum Key Distribution (QKD) needs randomness to select its active basis choice for each and every detected pairs of photon like their polarization angle. So again, a good and fast QRNG will be mandatory. This QRNG functionality can however be embedded in some specific QKD systems with relying on the randomness of the time between photons detection in the SPCMs (Single Photon Counting Modules)<sup>1396</sup>. But QRNGs have a much broader addressable market: classical cryptography and all the businesses in need of random numbers like casinos, online gaming and lotteries.



Let's now look at the QRNG industry vendors landscape. As said before, this technique has been mastered for a long time by **ID Quantique** (IDQ), a company cofounded by Nicolas Gisin, which belongs to SK Telecom since 2018. Other players abound like **CryptoMathic**, **Crypta Labs**, **Quside**, **InfiniQuant**, **Kets**, **PicoQuant** and **Quantropi**<sup>1397</sup>. **Axon Technologies** (2017, Canada) also created a random number generator competing with the Swiss IDQ.



**CryptoMathic** (1986, Denmark) develops quantum random key generators and various keys generation systems.



**EYL** (2015, USA, \$900K) sells entropy chips of 3mmx3mm and QRNG chips.



**PicoQuant** (1996, Germany) is a Berlin-based SME specialized in photonics and which markets photon counters and diode lasers. But they are here because they also offer a photon arrival time QRNG, the PQRNG 150, with a throughput of 150 Mbits/s. It is much less miniaturized than the random number generator component from IDQ that is integrated in Samsung's Galaxy 5G announced in May 2020.

<sup>1396</sup> This is described in [Practical random number generation protocol for entanglement-based quantum key distribution](#) by G. B. Xavier et al, 2008 (10 pages).

<sup>1397</sup> These companies are described in the [quantum telecommunication and cryptography](#) vendors section since they provide some PQC or QKD solution on top of QRNGs.



**Qrypt** (2018, USA) develops cryptographic solutions using a high speed QRNG powered by multiple entropy sources exclusively licensed from Oak Ridge National Lab and other labs. It will support NIST PQC standards when selected. Qrypt invested in Quside (Spain), which is developing high quality and high speed QRNGs.



**Qnu Labs** (2016, India) sells its Tropos Quantum Random Number Generation, which allows the creation of random numbers of any size and quite quickly, at a rate of up to 1.5 random Mbits/s, or even several tens of Gbits/s.



**Quside** (2017, Spain) proposes a QRNG using phase diffusion, with a 400 Mbits/s key generation rate. It is a spin-off of ICFO, the Institute of Photonics of Barcelona. Quside QRNGs were used in many of the 2015 loophole-free Bell test experiments thanks to their high key rate.



**Quantum Dice** (2019, UK, £2M) is a spin-off from the University of Oxford selling a “true” “self-certified” and fast QRNG device. It uses a patented DISC protocol ensuring that randomness comes only from the quantum process and is protected from external influences.

Their October 2021 £2M investment round was led by French venture capital fund Elaia Partners. They also got a £1M non-dilutive grant from the Quantum Accelerator Group led by IP Group, in partnership with Innovate UK as part of the UK national quantum plan.



**Quantropi** (2018, Canada) sells QEEP, a software generator of “lightweight ultra-high-entropy” random encryption keys. It seems not to be quantum per se.

This allows the creation of quantum safe encryption solutions<sup>1398</sup>. Quantropi positions itself as an alternative to QKD solutions but they brand their solution abusively as a “QKD over the Internet”. It targets in particular applications in the connected objects industry and competes with both QKD and PQC solutions.

## Quantum Key Distribution

The basic quantum cryptography technology is based on "quantum key distribution". It consists in allowing the exchange of symmetrical encryption keys, by optical means (optical fiber, air link or satellite optical link) using a system to protect its transmission against intrusion.

QKD protocols have the particularity of allowing the detection of any intrusion in the transmission chain and to indicate that someone has tried to read its contents or if, disturbances have occurred, "on the line"<sup>1399</sup>.

### QKD principles

One early version was the **BB84** protocol invented by **Charles Bennett** and **Gilles Brassard** in 1984<sup>1400</sup>. They are even the creators in 1982 of the expression "quantum cryptography"<sup>1401</sup>. But it wasn't yet QKD per se.

---

<sup>1398</sup> This leads to some extreme marketing claims as seen on [Startup: Only Quantum Cryptography Can Save The \\$100 Trillion Global Digital Economy](#) by John Koetsier in Forbes, March 2021.

<sup>1399</sup> See the excellent review paper [Advances in Quantum Cryptography](#) by S. Pirandola et al, 2019 (118 pages).

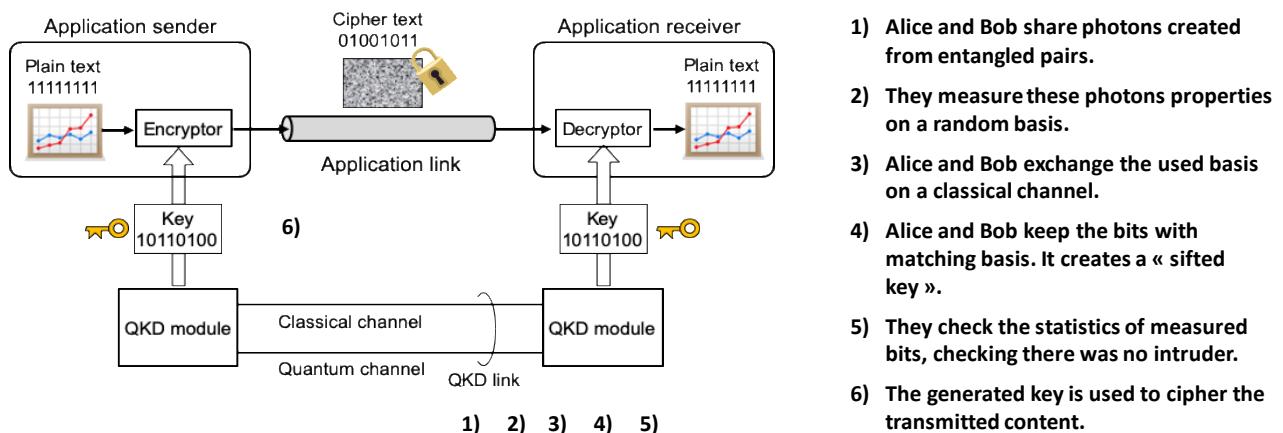
<sup>1400</sup> In [Quantum cryptography : public key distribution and coin tossing](#), 1984 (5 pages).

<sup>1401</sup> Here is a general overview of QKD and PQC: [The Impact of Quantum Computing on Present Cryptography](#), March 2018 (10 pages).

This protocol is about sending photon-based information with four types of rectilinear/diagonal polarizations, *aka* non-orthogonal states:  $0^\circ$ ,  $45^\circ$ ,  $90^\circ$  and  $135^\circ$ . Alice & Bob exchange through a classical channel their polarization basis, used for encoding by Alice and for measurement by Bob, after the photons have been sent to make sure Bob keeps only the relevant bits where his random measurement was done in the same as the polarization basis used by Alice.

The qubits read by an intruder would modify the key, by projecting their polarization at  $0^\circ$  or  $90^\circ$ , or  $45^\circ/135^\circ$  depending on the case and randomly. Any reading intrusion would be detected by Alice and Bob during their classical communication because of the inevitable errors it would cause. If the protocol detects an intruder, it can take this into account and block the communication of sensitive information because the encoding key has been captured and, maybe, chose another quantum channel. And there are solutions to avoid a denial of service in such a case<sup>1402</sup>.

**Artur Ekert** conceived the **E91** protocol in 1991<sup>1403</sup>. He perfected BB84 using quantum entanglement and non-locality, avoiding the explicit transmission of photon information that could be intercepted by an intruder. With E91, Alice and Bob share the photons created from entangled pairs. They can share a randomly generated key with a sequential measurement of these photons. Like with BB84, this measurement has to be done in a random orthogonal polarization basis that has to be shared afterwards between Alice and Bob. They will retain the randomly generated bits when their polarization was synchronized, creating a “sifted key”. If an eavesdropper Eve intercepts the entangled photons, their projections would be different. To make sure there was no eavesdropper, Alice and Bob compute a Bell test statistic which must yield ideally a so-called Bell parameter  $|S| = 2\sqrt{2}$ , called Tsirelson’s bound, otherwise, there was an eavesdropper ([details](#)).



One key difference between BB84 and E91 is the origin of randomness in the shared keys. With BB84, it must be generated by Alice with a random numbers generator, preferably a TRNG (true random numbers generator) and not a PRNG (pseudo-random numbers generator) as described in the earlier section on QRNGs, page 597. With E91, it comes directly from the randomness of the entangled photon pairs readouts. All in all, E91 is both a quantum communication protocol and a quantum random number generator.

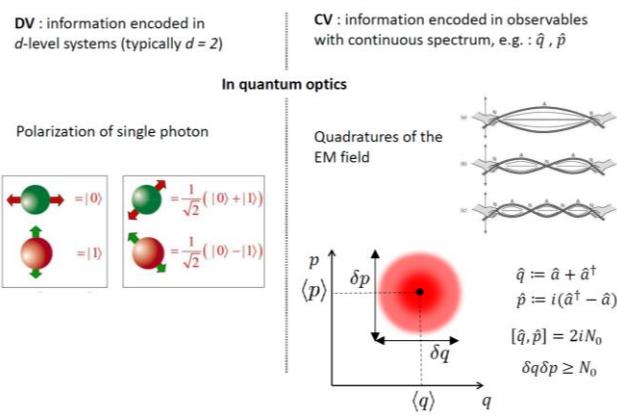
The idea has since made its way. It is at the origin of the creation of the whole field of quantum cryptography, which has now left the exclusive field of research and experimentation to enter actual deployments like in China, even though there are still problems remaining to be fixed such as the creation of safe repeaters.

<sup>1402</sup> See for example [A quantum key distribution protocol for rapid denial of service detection](#) by Alasdair Price et al, from the University of Bristol, in EPJ Quantum Technology, 2020 (20 pages).

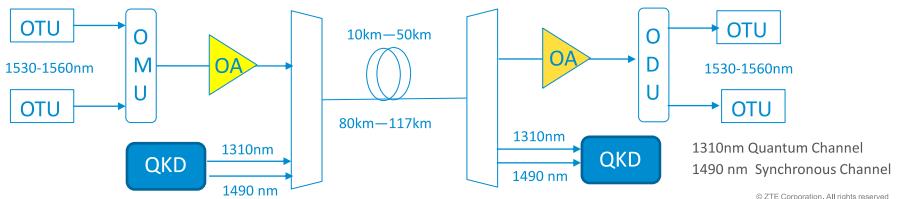
<sup>1403</sup> And published in the article [Quantum Cryptography Based on Bell's Theorem](#) (3 pages). Artur Ekert has been a member of Atos Scientific Council since 2016, along with Alain Aspect, Daniel Esteve, Serge Haroche, Cédric Villani and David DiVincenzo.

QKD was expanded with CV-QKD (continuous variable) which modulates both the phase and the amplitude of the transmitted optical signal. It notably allows multiplexing several communications on the same optical fiber and to exploit the existing infrastructures of telecom operators. **Philippe Grangier** is one of its designers, along with **Frédéric Grosshans** from CNRS-LIP6, in 2002<sup>1404</sup>. CV-QKD complements discrete variables QKD (DV-QKD) as are called the previously mentioned QKD protocols, based on the properties of single photons, which requires cooling on the single-photon detector side.

The integration of a QKD in conventional telecommunication optical fibers is typically done using three methods: by frequency multiplexing (WDM), for instance with a QKD signal on 1310 nm and data sent on 1550 nm, by time sharing (TDM) or by using a dedicated fiber embedded in a sheath (SDM)<sup>1405</sup>.



### Co-Fiber Experiment in China Telecom Laboratory



#### Experiment 1

- High coding rate in co-directional fibers
- Classical optical power reduce the coding rate, so we need control their power to increase coding rate.

#### Experiment 2

- Huge large Capacity Service Datas 8T ( 80x100G )
- Ultra-long transmission distance ( 80km-117km )
- Highj QKD code rate ( 16kbps-1kbps )
- Smooth upgrade, service can be real-time quantum encryption

The initial entanglement done before sending the two bits in the qubits avoids violating the Holevo theorem, already mentioned several times, according to which a set of qubits cannot carry more information than its equivalent number of classical bits. On the other hand, the information encrypted with the transmitted key is usually sent over a traditional channel<sup>1406</sup>. It is still often encrypted using SSL, which protects the relationship between your browser and the websites you visit and supports the secured https protocol.

In practice, keys transmission using a QKD is accompanied by a complex system of "key distillation" that manages the communication imperfections with classical error correction codes (which have nothing to do with the quantum error correction codes seen at the qubit level [elsewhere in this document](#), page 200), an amplification of confidentiality and an authentication system using private keys already shared by the correspondents, making it possible to avoid so-called *man-in-the-middle* attacks by hackers pretending to be one of the interlocutors. Error correction codes and the rest of the protocol generate on-line losses of about 80% of the quantum key communication<sup>1407</sup>.

<sup>1404</sup> Their QKD protocol is baptized accordingly GG02.

<sup>1405</sup> See [QKD Application: Coexistence QKD Network and Optical Networking the same optical fiber network](#) by JiDong Xu, June 2019 (15 slides). It's also described in [Quantum Encrypted Signals on Multiuser Optical Fiber Networks Simulation Analysis of Next Generation Services and Technologies](#) by Rameez Asif, 2017 (6 pages) and [Quantum experiments explore power of light for communications, computing](#) by Elizabeth Rosenthal, January 2020.

<sup>1406</sup> Classical information can take a very different path. For example, a quantum key can be transmitted by satellite and data can be transmitted terrestrially over fiber optics.

<sup>1407</sup> According to the excellent overview by Sheila Cobourne of the University of London [Quantum Key Distribution Protocols and Applications](#), 2011 (95 pages).

Implementing a QKD combines a quantum random key generator such as those from IDQ, an authenticated classical channel to exchange QKD basis information and a QKD channel to share random keys, which can generally be transported on a dark fiber from a B2B telecom operator<sup>1408</sup>.

The useful data is encrypted with the QKD generated key and transmitted over a traditional channel, which may also be a classical optical fiber or other physical communication media, even cellular communications. This is well documented by ETSI<sup>1409</sup>. On arrival, a quantum key receiver and the system for decrypting the signal arriving via the traditional channel is used.

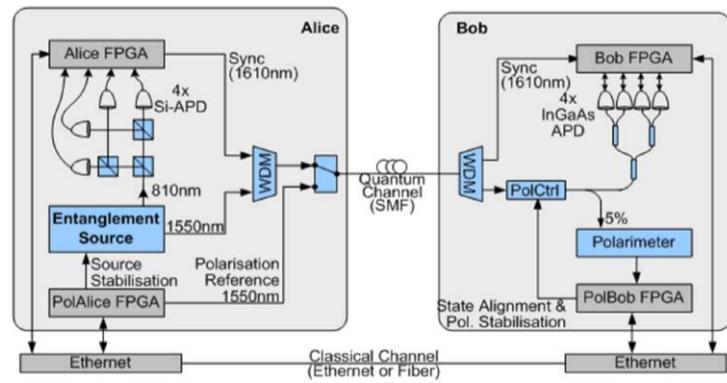
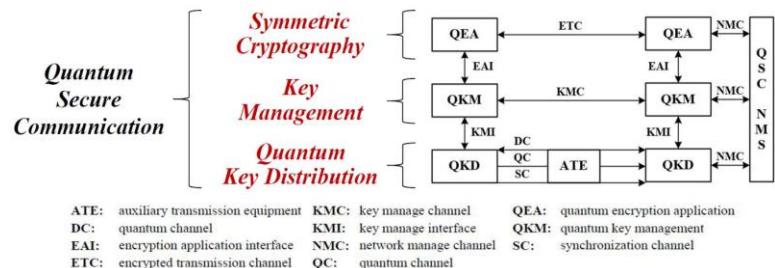


Figure 4.6: Schematic of an entanglement-based QKD system

The secret keys throughput is an important issue and is currently at its maximum in Mbits/s vs. the Tbits/s of the operators' optical links. The quantum keys transfer rate can be much lower than the physical data rate available. There are fundamental bounds on how much secret keys can be generated over a noisy quantum channel.

There are a few other varieties of QKD protocols beyond the DV-QKD and CV-QKD with HD-QKD (multiple key encoding bits per photon) and MDI-QKD<sup>1410</sup>.

QKD is however not the solution-that-fixes-all-problems. It can be subject to jamming and denial of services. Its safety also depends on the security of both ends of telecommunication like with any other solution.

## Experiments and deployments

Many breakthrough symbolic experimental deployments of QKD have been done both in the open air and with optical fibers.

Open-air QKD demonstrations started in 1996 in the USA on a 75m distance, then on 144 km to connect the islands of La Palma and Tenerife in the **Canary Islands** and conducted by Austrians in 2007 and 2010<sup>1411</sup>, and in 2019 in urban areas in Italy with a distance of 145m<sup>1412</sup>.

<sup>1408</sup> Schema source: [Development and evaluation of QKD-based secure communication in China](#) by Wen-yu Zhao, June 2019 (15 slides).

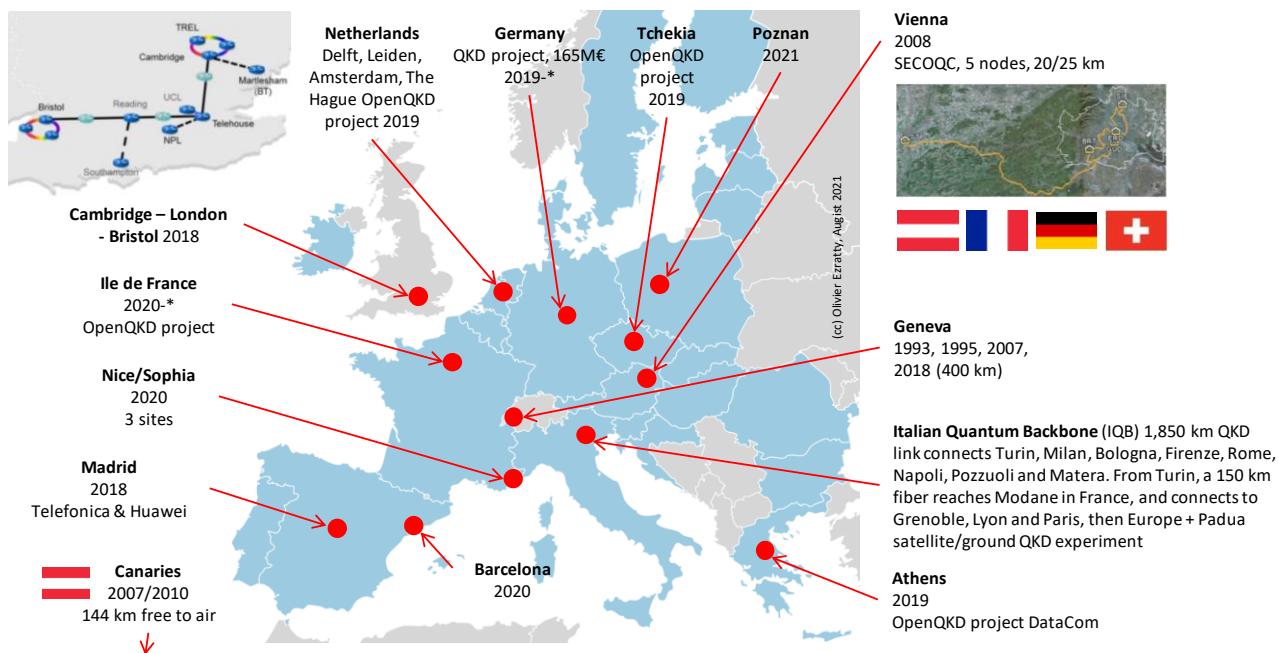
<sup>1409</sup> In [Quantum Key Distribution \(QKD\) Components and Internal Interfaces](#) from ETSI, 2018 (47 pages) which describes the different QKD techniques available to date and where the schema comes from. It also describes very well the photon sources used in QKDs as well as the associated quantitative and qualitative parameters.

<sup>1410</sup> See this good overview of QKD and its technical challenges in [Practical challenges in quantum cryptography](#) by Eleni Diamanti et al, 2016 (25 pages).

<sup>1411</sup> See [Second Generation QKD System over Commercial Fibers](#), 2016 (5 pages) et [Feasibility of 300 km Quantum Key Distribution with Entangled States](#), 2010 (14 pages).

The range of QKD transmission over fiber has improved with only 30 cm in 1989 (IBM with Charles Bennett), 1100 m at the University of Geneva in 1993, then 23 km in 1995 with the BB84 protocol, all via fiber optics. The record at the beginning of 2020 was 509 km of transmission and without repeater, achieved in China<sup>1413</sup>. But with a tiny winy bit rate of a couple bits per hours!

An experiment took place in **Vienna** in 2008 as part of the European **SECOQC** (*SECure COnmunication based on Quantum Cryptography*) project launched in 2004 and involving some 40 research laboratories and vendors, using a "mesh" architecture<sup>1414</sup>.



This went on in Switzerland with **IDQ** with local banks. In 2007 they also set up an election vote counting system based on a QKD.

In 2018, the United Kingdom deployed its UK Quantum Communications hub between Bristol, London, Cambridge and Ipswich<sup>1415</sup>.

In France, **Orange** announced in May 2019 the launch of tests of a QKD protected communication with the University Côte d'Azur (UCA) which provides the solution via the InPhyNi laboratory. It connects the Valrose and Inria campuses in Sophia Antipolis with an access point on the Plaine du Var IMREDD campus in Nice, using dark fibers provided by the telecom operator<sup>1416</sup>.

<sup>1412</sup> See [Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics](#) by Matteo Schiavon et al, July 2019 (7 pages). QKD key transmission over the 145m air link took place at 1550 nm in the infrared band that is commonly used in fiber optic transmissions and therefore compatible with many existing telecommunication equipment. They used a silicon chipset doing all the work with an error rate of only 0.5% and a data rate of 30 kbit/s. Their QCosOne ("Quantum Communication for Space-One") used telescopes with 120 and 315 mm optics for transmission and reception. It worked during daytime, but there were still problems in case of turbulence and depending on the time of day and the side effects coming from the sun. Performance was better in the evening. They used triple photon encoding: temporal, spatial and spectral.

<sup>1413</sup> See [Study achieves a new record fiber QKD transmission distance of over 509 km](#) by Ingrid Fadelli, March 2020.

<sup>1414</sup> See [The SECOQC quantum key distribution network in Vienna](#) by Romain Alléaume, Eleni Diamanti et al, 2016 (39 pages).

<sup>1415</sup> Seen in [IDQ: Quantum-Safe Security relevance for Central Banks](#), 2018 (27 slides). The network was extended in Cambridge in 2019 as seen in [Cambridge quantum network](#) by J. F. Dynes et al, 2019 (8 pages).

<sup>1416</sup> See [Université Côte d'Azur and Orange are collaborating to set up an experiment in quantum cryptography](#), May 2019. And for Orange's QKD projects in general: [Orange and quantum technologies for secure data exchange](#), June 2020.

The test network was operational in September 2021.

In particular, Orange is studying the reliability of trusted optical network nodes in such a configuration.

The operator is also looking to combine QKD solutions to protect physical links and PQC solutions that could be used as a method of encrypting data transmitted in association with a QKD.



## OPEN QKD

The European consortium **OpenQKD** is experimenting a terrestrial QKD network. It prepares the ground for the launch of the **EuroQCI** network which would be an operational implementation of a terrestrial and satellite European QKD network<sup>1417</sup>. This involves in particular France, Germany, Austria, Italy, Spain, the Netherlands, Greece, Switzerland and Poland and vendors like Thales Alenia Space (satellite communication), Orange and Mellanox (a subsidiary of Nvidia). From a practical point of view, it's about deploying a large interoperable experimental QKD network on a European scale, exploited by applications in various fields (healthcare, energy grids, transportation, finance, government, education and the likes). The consortium also intends to influence QKD standardization. And at last, as far as possible, it's also about contributing to the development of a European industry offering in QKD and associated technologies.

In France, the test area will be the Paris region and its major research laboratories with the Institut d'Optique, Telecom Paris, LIP6 in Jussieu and Nokia labs in Villarceau. The project has received €15M in European funding from Horizon 2020, independently of Quantum Flagship.

Moving now to the USA, the first experiments were conducted in Boston by **DARPA** between 2004 and 2007. A QKD network piloted by **Batelle** was tested in Ohio in 2013<sup>1418</sup>. Tests were also conducted in 2015 at **MIT**, linking two sites 43 km apart. A commercial deployment of QKD on an unused 800 km fiber optic network connecting Boston to Washington DC is also being deployed by **Quantum Xchange** and **Zayo**, to connect Wall Street finance businesses with their backoffices in New Jersey. It uses some trusted node technology<sup>1419</sup>.

An 85 km facility was also deployed in Chicago in 2019<sup>1420</sup>. In July 2020, the Department of Energy announced the expansion of the QKD network to link all of its research laboratory sites<sup>1421</sup>.

In **Canada** launched in November 2020 its Canada Quantum Network through a partnership between Xanadu, the Creative Destruction Lab and the startups service company MaRS around Toronto.

---

<sup>1417</sup> See [Nine more countries join initiative to explore quantum communication for Europe](#), December 2019.

<sup>1418</sup> See [Batelle Installs First Commercial Quantum Key Distribution Protected Network in U.S.](#), 2013.

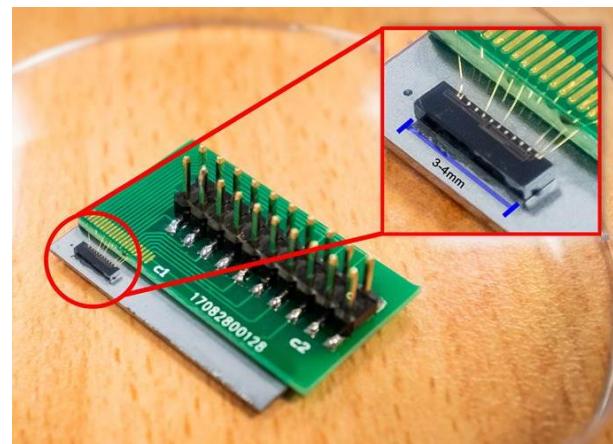
<sup>1419</sup> See [New plans aim to deploy the first US quantum network from Boston to Washington, DC](#), October 2018. Schema source: [From MIT : Semiconductor Quantum Technologies for Communications and Computing](#), 2017, 32 slides).

<sup>1420</sup> See [Argonne and UChicago scientists take important step in developing national quantum internet](#) by Louise Lerner, February 2020.

<sup>1421</sup> See [Department of Energy \(DOE\) Unveils Blueprint for a U.S. Quantum Internet](#) by Doug Finke, July 2020.

In Japan, **Toshiba** announced in September 2018 that a QKD solution co-developed with the Tohoku Medical Megabank Organization (ToMMo) at Tohoku University had achieved a QKD throughput of more than 10 Mbps during one month.

One of the challenges in deploying QKD is the miniaturization of its components. Whereas initially a complete rack of hardware was needed for quantum key transmitting/receiving stations, the goal is to fit everything in a photonics component a few mm long. This is what **NTU** researchers in Singapore did in 2019 to manage a CV-QKD supporting existing telecom operators' fiber infrastructures<sup>1422</sup>. But this miniaturization concerns here only the photonics part. These photonic circuits have to be completed by classical electronic components.



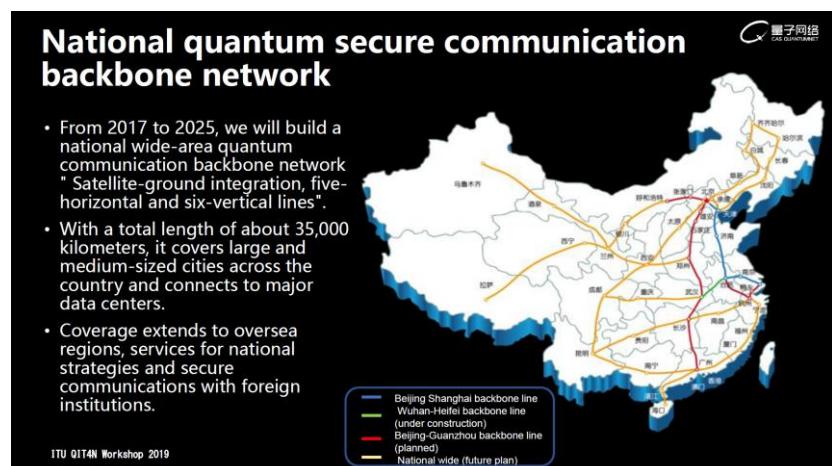
The development of such integrated photonics components will also be supported in the framework of European Horizon Europe projects that follows Europe 2020 projects over the 2021-2027 period.

## QKD in China

China stands out since 2016 with impressive QKD experiments and deployments. The country invests heavily in QKD with a now classical multi-pronged strategy: to protect its sensitive communications against any attacker and to develop an industry in a promising emerging technology field. A first deployment was carried out in 2012 in the Hefei area to link various Chinese government entities<sup>1423</sup>.

It was then expanded with an installation of a QKD-secured fiber optic link between Shanghai and Beijing, covering 2,000 km. The line installed between 2013 and 2016 was deployed by a local startup, **QuantumCTek**.

The network relies on 32 transponders with secured physical access<sup>1424</sup>. Indeed, the signal attenuation was then too strong beyond about 50 km on one optical fiber.



The entities using this line are government agencies, including various financial sector regulatory agencies and banks. The country also plans to protect its energy grid infrastructure with this network<sup>1425</sup>.

<sup>1422</sup> See [Researchers create quantum chip 1,000 times smaller than current setups](#), October 2019 which references [An integrated silicon photonic chip platform for continuous-variable quantum key distribution](#) by G. Zhang et al, December 2019 (5 pages).

<sup>1423</sup> See [Unhackable Chinese Communication Network Launches Soon](#) by Rechelle Ann Fuentes, 2017.

<sup>1424</sup> Source: [Security assessment and key management in a quantum key distribution network](#) by Xiongfeng Ma, June 2019 (21 slides).

<sup>1425</sup> See [Application In Power Industry Promotes the Development of Quantum Cryptography Technology](#) by Yonghe Guo, June 2019 (13 slides).

China then launched in 2017 a deployment of an additional 33,000 km of the **National Quantum Secure Communication Backbone Network**, to be completed by 2025. It had started with the creation of a Hefei-Wuhan link<sup>1426</sup>. Hefei is the city where Jian-Wei-Pan's main quantum technologies laboratory is located<sup>1427</sup>.

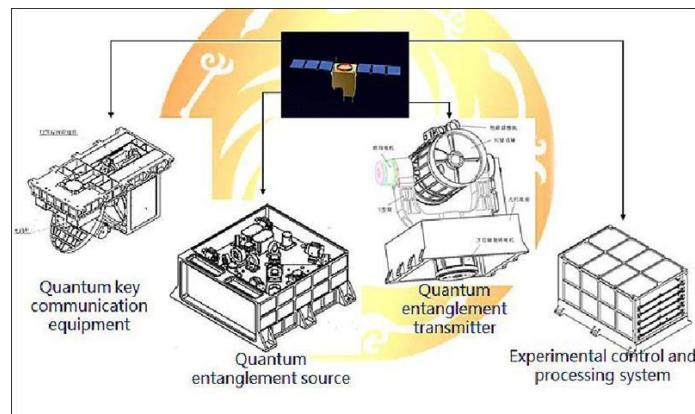
### **QKD by satellite and with UAVs**

The second Chinese performance deals with the use of the **Micius** satellite also named **Mozi** for a western/Chinese pronunciation and **QUESS** (Quantum Experiments at Space Scale) to teleport photon quantum states by optical means in 2017, at a distance of 1,400 km between the satellite and Earth, at an altitude of 5,100 m in the Ngari prefecture in Chinese Tibet<sup>1428</sup>. The satellite weighs 640 kg and consumes 560W. This kind of experiment had already been done on Earth with distances of up to 100 km corresponding to the maximum length of an optical fiber without a repeater.

The experience was renewed in 2018 with the organization of a videoconference between China and Austria using a quantum key sent every minute<sup>1429</sup>. Why with Austria? Because Jian-Wei Pan did his PhD thesis in Austria under the supervision of Anton Zeilinger, who piloted the European part of the experiment.

China is in fact planning to launch a cloud of satellites in low orbit by 2030 dedicated to sending quantum keys by repeating this process<sup>1430</sup>. Finally, a 2000 km quantum key protected fiber optic link has been deployed between Shanghai and Beijing. In any case, we can see that China is taking this issue of secure communications very seriously.

If they are bundling on QKD for symmetric key management, it seems that they are also investing in post-quantum cryptography but in a quieter way.



<sup>1426</sup> See [Towards large-scale quantum key distribution network and its applications](#) by Hao Qin, 2019 (17 slides).

<sup>1427</sup> The extended BB84 based QKD network is documented in [Implementation of a 46-node quantum metropolitan area network](#) by Teng-Yun Chen et al, September 2021 (14 pages). It describes the intra-metropolitan network infrastructure deployed in Hefei, with 46 nodes.

<sup>1428</sup> Details in [Ground-to-satellite quantum teleportation](#), 2017 (16 pages). The principle was first described in 1993 in [Teleporting an Unknown Quantum State via Dual Classical and EPR Channels](#) by Charles Bennett, Gilles Brassard (from Montreal), Claude Crépeau, Richard Jozsa, Asher Peres and William Wootters. See also [Quantum Communication at 7,600km and Beyond](#) by Chao-Yang Lu and Cheng-Zhi Peng, Jian-Wei Pan, November 2018.

<sup>1429</sup> See [Real-world intercontinental quantum communications enabled by the Micius satellite](#), USTC, January 2018. Experiments or equivalent experiences have been launched by European teams. See [Quantum Photonics Technologies for Space](#), October 2018 (22 pages) and [Nanobob CubeSat mission](#), 2018 (31 pages). This is also being done in the UK, where an experimental Cubesat micro-satellite project is planned to cover the country. See [QUARC: Quantum Research Cubesat - A Constellation for Quantum Communication](#) by Luca Mazzarella et al, 2020 (27 pages).

<sup>1430</sup> See some details on the satellite QKD deployment architecture in [Approaches to scheduling satellite-based quantum key distribution for the quantum network](#) by Xingyu Wang et al, 2021 (11 pages).

But this satellite experiment had limitations: it could handle 5.9 million pairs of entangled photons per second, but due to error corrections, only one useful photon pair was exploitable per second<sup>1431</sup>. As a result, Chinese scientists are studying scheduling approaches to load balance key distribution over time<sup>1432</sup>.

At the beginning of 2020, China announced that it had miniaturized its ground receiving station for quantum key communication with the Micius satellite from 10 tons to 80 kg. The key bitrate was reduced, from 40Kbits/s to 4-10Kbits/s. The experiment took place on the Earth side in Jinan and Shanghai, so it seems at sea level<sup>1433</sup>. The Bank of China would already secure transactions by sending keys via the Micius/Mozi Beijing satellite and remote provinces.

In June 2019, Chinese researchers announced that they had demonstrated the use of optical QKD aerial links established within a network of 35 kg octocopter UAVs spaced 200 m apart during a 40-minute flight at an altitude of 100 m<sup>1434</sup>. The payload handling quantum communication weighted 11.8 kg. It can still be miniaturized, since the Chinese are aiming to integrate it into mass-market UAVs.

At last, China was proud to announce in 2021 that they had created the world's first integrated quantum communication network, combining 700 terrestrial optical fibers with two ground-to-satellite links, achieving quantum key distribution over a distance of 4,600 km<sup>1435</sup>.

## QKD repeaters

So what about repeaters, which are essential for distributing quantum keys over long distances, beyond 80 km<sup>1436</sup>? One can make a distinction between trusted nodes/repeaters where keys have to be revealed in the intermediate stations or with some untrusted ones, like when entanglement-based or MDI protocols are used.

Chinese researchers created a 404 km QKD fiber connection without a repeater in 2016<sup>1437</sup>, then extended this record in 2020 to 511 km using the TF-QKD protocol<sup>1438</sup>. The technique was improved in 2020 by a mix of British and American researchers to reach 600 km<sup>1439</sup>.

At these large distances, the error rates are so high that it becomes impractical. The key rates are very low, getting under  $10^{-7}$  for distances larger than 400 km. There is even a higher bound for these key rates,  $-\log_2(1-\eta)$  with  $\eta$  being the transmissivity of the lossy quantum channel, whatever the protocol<sup>1440</sup>.

---

<sup>1431</sup> See [A step closer to secure global communication](#) by Eleni Diamanti, Nature, June 2020, which describes the practical conditions and limitations of these satellite key transmission experiments. And in particular the most recent one described in [Entanglement-based secure quantum cryptography over 1,120 kilometers](#) by Juan Yin et al, Nature, June 2020. The actual key bitrate was 0.12 bits per second!

<sup>1432</sup> See [Approaches to scheduling satellite-based quantum key distribution for the quantum network](#) by Xingyu Wang et al, 2021 (11 pages).

<sup>1433</sup> See [China has developed the world's first mobile quantum satellite station](#) by Donna Lu, January 2020..

<sup>1434</sup> See [Drone-based all-weather entanglement distribution](#) by Hua-Ying Liu et al, May 2019 (16 pages) and [World's First "Quantum Drone" for Impenetrable Air-to-Ground Data Links Takes Off](#) by Charles Q. Choi, IEEE Spectrum.

<sup>1435</sup> See [Chinese Scientists Report World's First Integrated Quantum Communication Network](#) by Matt Swayne, 2021.

<sup>1436</sup> Knowing that the record distance for quantum telecommunication without repeaters is 509 km as we have already seen. See also [Viewpoint: Record Distance for Quantum Cryptography](#) by Marco Lucamarini, Toshiba & Cambridge, November 2018 and [Recent progress on Measurement-Device-Independent \(MDI\) Quantum Key Distribution \(QKD\)](#) by Marco Lucamarini, 2018 (71 slides).

<sup>1437</sup> Documented in [Measurement device independent quantum key distribution over 404 km optical fiber](#), 2016 (15 pages).

<sup>1438</sup> See [Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans](#) by Jiu-Peng Chen, Jian-Wei Pan et al, January 2021 (32 pages). This is the source of the graph below.

<sup>1439</sup> See [600-km repeater-like quantum communications with dual-band stabilization](#) by Mirko Pittalugal et al, 2020 (14 pages).

<sup>1440</sup> See [Fundamental Limits of Repeaterless Quantum Communications](#) by Stefano Pirandola et al, 2017 (61 pages).

Quantum channels used for QKD are subject to noise and leaks. Transmitting a useful photon requires several trials and its number grows exponentially with distance. And when the photon arrives at destination, its state fidelity also decreases exponentially with distance.

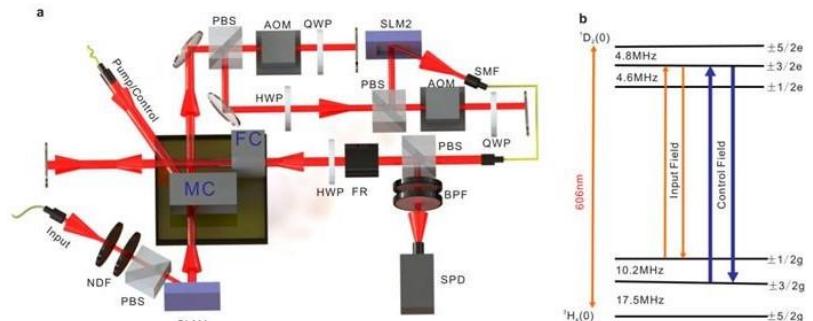
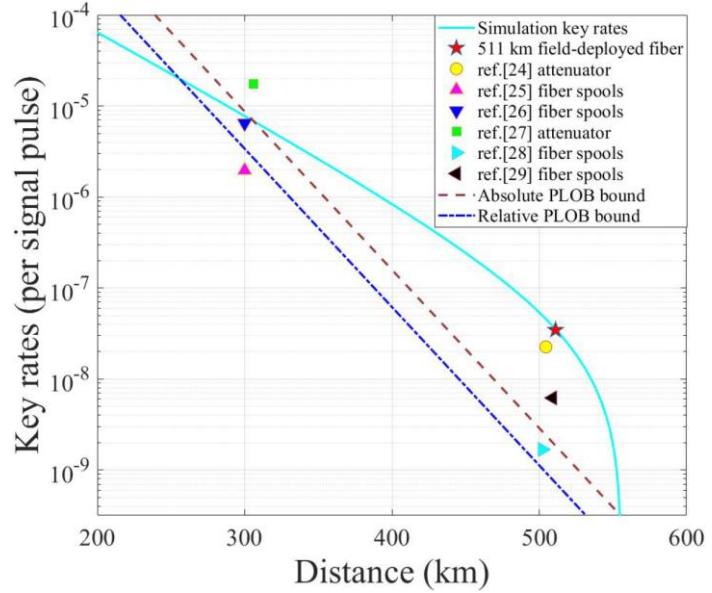
As a result, for large distances, we need repeaters. These must guarantee a good key rate and fidelity and be tolerant to errors. They implement quantum states purification which consists in keeping trusted entangled pairs selected out of many imperfect pairs, and entanglement exchange.

Quantum repeater technologies are still at basic research stage and with some limitations<sup>1441</sup>. We are already in the third generation of these repeaters. These repeaters must usually be equipped with some quantum memory to propagate the state of the photons to be transmitted through entanglement swapping. This quantum memory can be based on cold atoms, rare earth doped crystals, trapped ions of NV centers with long lasting qubits lives and connectivity (qubit exchanges) with telecom fiber photons<sup>1442</sup>.

The **DLCZ protocol** created by Harvard, Austria and China scientists in 2001 made it possible to improve entanglement sharing on lossy communication channels and has been continuously improved since then<sup>1443</sup>. It is based on using clouds of identical atoms instead of individual atoms, beam splitters and single-photon detectors with moderate efficiencies with a communication efficiency that scales polynomially with distance.

Among others, **Nicolas Gisin's** team at the University of Geneva (and with ID Quantique) with a CNRS team in France are also working on quantum repeaters<sup>1444</sup>.

Researchers from the **Key Laboratory of Quantum Information** of the Chinese Academy of Sciences published in August 2018 a study on the creation of quantum memories based on rare earth ions (praseodymium) doped with three degrees of freedom, controllable by sending photons<sup>1445</sup>.



<sup>1441</sup> See [Tutorial on quantum repeaters](#) by Rodney Van Meter and Tracy Northup, 2019 (178 slides), [Overcoming the rate-distance limit of quantum key distribution without quantum repeaters](#), 2018 (5 pages) et [An Information-Theoretic Framework for Quantum Repeaters](#) by Roberto Ferrara, 2018 (144 pages).

<sup>1442</sup> See [Quantum Nodes for Quantum Repeaters](#) by Hugues de Riedmatten, ICFO, January 2021 (60 slides).

<sup>1443</sup> See [Long-distance quantum communication with atomic ensembles and linear optics](#) by Lu-Ming Duan, Mikhail Lukin, Ignacio Cirac and Peter Zoller, Nature, May 2001 (11 pages).

<sup>1444</sup> According to [Ytterbium: The quantum memory of tomorrow](#), July 2018.

<sup>1445</sup> See [Multiplexed storage and real-time manipulation based on a multiple-degree-of-freedom quantum memory](#), by Tian-Shu Yang et al, China CAS, 2018 (9 pages).

This technique could be used both to create repeaters for QKD networks and to create quantum memories for photon-qubits quantum accelerators. In July 2019, Chinese researchers finally announced that they succeeded using a photonic repeater technology based on 12-photon interferometers without any quantum memory<sup>1446</sup>.

In mid-2019, other Chinese researchers experimented the teleportation of qutrits, allowing a transmission of more information per photons<sup>1447</sup>. This could be used to increase the rate of QKD key transmission.

## Securing QKD

Securing a chain depends on its weakest links and here it is the transmitters and receivers before they even exchange via a QKD. Furthermore, QKDs are not a panacea because they depend on a point-to-point link and not on a routing technique that allows several paths to be used. This could lead to a form of denial of service by blocking the used physical communication but rerouting techniques are investigated<sup>1448</sup>. This table lists a whole bunch of vulnerabilities in the QKD, some of which have since been fixed<sup>1449</sup>.

Attack	Target component	Tested system
<b>Distinguishability of decoy states</b> A. Huang <i>et al.</i> , Phys. Rev. A 98, 012330 (2018)	laser in Alice	3 research systems
<b>Intersymbol interference</b> K. Yoshino <i>et al.</i> , poster at QCrypt (2016)	intensity modulator in Alice	research system
<b>Laser damage</b> V. Makarov <i>et al.</i> , Phys. Rev. A 94, 030302 (2016); A. Huang <i>et al.</i> , poster at QCrypt (2018)	any receiver optics	5 commercial & 1 research systems
<b>Spatial efficiency mismatch</b> M. Rau <i>et al.</i> , IEEE J. Sel. Top. Quantum Electron. 21, 6600905 (2015); S. Saeed <i>et al.</i> , Phys. Rev. A 91, 062301 (2015)	classical watchdog detector	2 research systems
<b>Pulse energy calibration</b> S. Saeed <i>et al.</i> , Phys. Rev. A 91, 032326 (2015)	phase modulator in Alice	ID Quantique
<b>Trojan-horse</b> I. Khan <i>et al.</i> , presentation at QCrypt (2014)	phase modulator in Bob	SeQureNet
<b>Trojan-horse</b> N. Jain <i>et al.</i> , New J. Phys. 16, 123030 (2014); S. Saeed <i>et al.</i> , Sci. Rep. 7, 8403 (2017)	homodyne detector	ID Quantique
<b>Detector saturation</b> H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 88990N (2013)	classical sync detector	SeQureNet
<b>Shot-noise calibration</b> P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A 87, 062313 (2013)	intensity modulator	(theory)
<b>Wavelength-selected PNS</b> M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A 86, 032310 (2012)	beamsplitter	research system
<b>Multi-wavelength</b> H.-W. Li <i>et al.</i> , Phys. Rev. A 84, 062308 (2011)	single-photon detector	research system
<b>Deadtime</b> H. Weier <i>et al.</i> , New J. Phys. 13, 073024 (2011)	single-photon detector	ID Quantique
<b>Channel calibration</b> N. Jain <i>et al.</i> , Phys. Rev. Lett. 107, 110501 (2011)	Faraday mirror	(theory)
<b>Faraday-mirror</b> S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A 83, 062331 (2011)	single-photon detector	ID Quantique, MagiQ, research systems
<b>Detector control</b> I. Gerhardt <i>et al.</i> , Nat. Commun. 2, 349 (2011); L. Lydersen <i>et al.</i> , Nat. Photonics 4, 686 (2010)		

All the side-channel attacks from the table above that can be typically fixed with countermeasures. But the more fundamental issue of device independence, linked to the need of loophole free Bell test will be very difficult to implement practically.

Cryptography is fascinating for the speed at which security devices can be broken by researchers before they are deployed en masse. Thus QKDs would be vulnerable due to an implementation vulnerability associated with Bell's theorem that can be handled with better quality detectors<sup>1450</sup>. It's a never-ending race!

## QKD and Blockchain

Another example is this project to use QKD to secure a Blockchain. This is obviously delicate to deploy end-to-end on a large scale. Indeed, Blockchain users don't have a satellite link in the mountains or a secured fiber on hand, even when they are mobile.

---

<sup>1446</sup> See [Scientists Firstly Realize All-photonic Quantum Repeater](#), July 2019 and [Experimental quantum repeater without quantum memory](#) by Zheng-Da Li et al, 2019 (12 pages).

<sup>1447</sup> See [Qutrits experiments are a first in quantum teleportation](#) by Daniel Garisto in Scientific American, August 2019, which refers to [Experimental multi-level quantum teleportation](#) by Xiao-Min Hu et al, April 2019 (12 pages) and [Quantum teleportation in high dimensions](#) by Yi-Han Luo, June 2019 (23 pages).

<sup>1448</sup> On QKD vulnerabilities and methods to avoid them, see [QKD Measurement Devices Independent](#) by Joshua Slater, 2014 (83 slides).

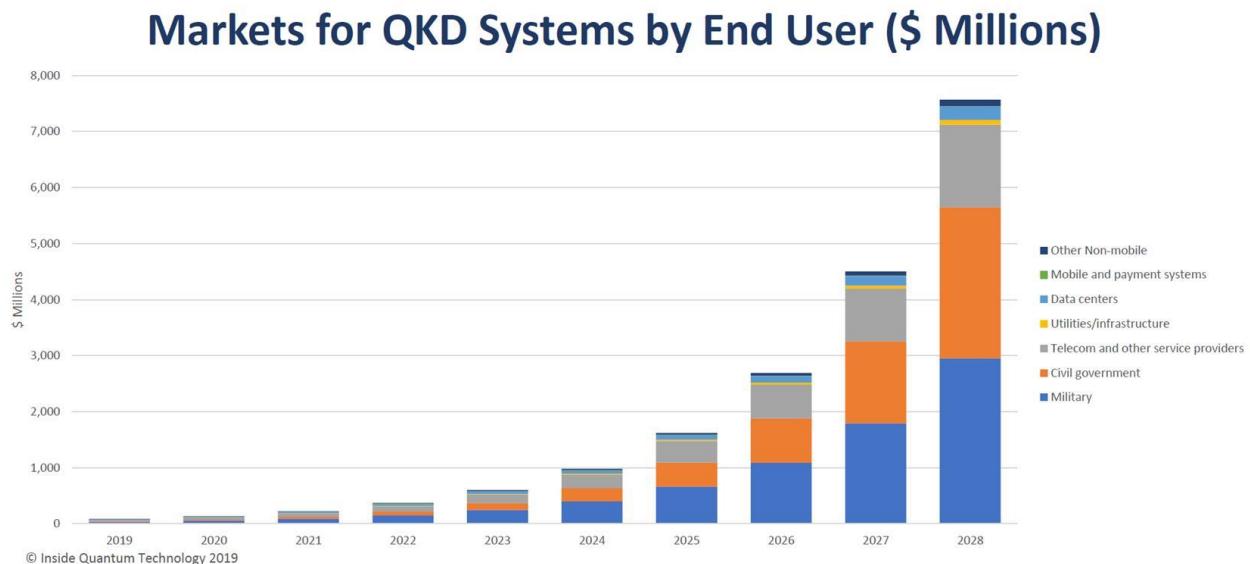
<sup>1449</sup> See [Certification of cryptographic tools](#) by Vadim Makarov from Quantum Hacking Lab in Moscow, 2019 (15 slides).

<sup>1450</sup> It is documented by Jonathan Jogenfors in [Breaking the Unbreakable Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography](#), 2017 (254 pages).

But so be it. This is the proposal of Evgeny Kiktenko of the Russian Quantum Center in Moscow<sup>1451</sup> and Del Rajan and Matt Visser of Victoria University of Wellington in New Zealand<sup>1452</sup>. Why exactly is not all data transmitted protected in the same way as the QKD? It seems at least to be limited by the low bitrate of existing QKDs.

## Market and standards

What about the size of the QKD market? **Inside Quantum Technology** (a UK analyst company) made an estimate with a first \$1B dollars reached in 2024, then an exponential growth leading to \$7B in 2028<sup>1453</sup>. These are simplistic exponential growth curves, as usual. We'll see.



China is very active in defining a set of QKD standards<sup>1454</sup>. The ITU is also working on QKD standards<sup>1455</sup>. Europe is represented in the standardization work carried out at ISO, IEEE, ETSI and CEN-CENELEC, the European Committee for Standardization in Electronics and Electrotechnology.

## Post-quantum cryptography

A physical protection of symmetric key transmission is not easily applicable in a generalized way, if only because it requires some optical link (direct free to air or by optical fiber) between transmitters and receivers. This, for example, does not work with radio links like with smartphones.

So, cybersecurity also requires the creation of cryptography systems capable of resisting the onslaught of quantum computers whether coming from Shor's or Grover's algorithms. Breaking encrypted messages - without private keys - should be an NP-Complete or NP-Hard problem to withstand future quantum assaults.

<sup>1451</sup> Documented in [First Quantum-Secured Blockchain Technology Tested in Moscow](#), June 2017.

<sup>1452</sup> In [Quantum Blockchain using entanglement in time](#), 2018 (5 pages).

<sup>1453</sup> See [The Future of the Quantum Internet A Commercialization Perspective](#) by Lawrence Gasman, June 2019 (11 slides) and [The Future of the Quantum Internet A Commercialization Perspective](#) by Lawrence Gasman from Inside Quantum Technology, June 2019 (11 slides). Seen in [ITU Workshop on Quantum Information Technology for Networks](#).

<sup>1454</sup> See [Introduction of Quantum secured Communication Standardization in CCSA](#) by Zhangchao Ma, June 2019 (16 slides) and [An overview of current quantum information technology \(QIT\) standardization](#) by Wei Qi, June 2019 (13 slides).

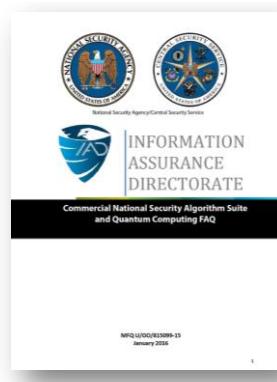
<sup>1455</sup> See [ITU-T Focus Group on Quantum Information Technology for Networks \(FG-QIT4N\)](#), 2019.

Post-Quantum Cryptography (PQC) complements Quantum Key Distribution (QKD) for this respect. It is certainly easier to deploy on a large scale because it is independent from the telecommunications infrastructures.

However, it can be combined by sending PQC public keys over physical QKD links or with using some PQC for authenticating the classical link used for the exchange of the photons measurement basis<sup>1456</sup>. Different PQC systems differ in many parameters and have different trade-offs between signature size, processing speed for encryption and decryption, and public key size.

Let's look at the PQC timeline<sup>1457</sup>:

- **1978:** the first algorithm resistant to quantum computers is created by **Robert McEliece** (details below) even before Richard Feynman even mentioned the idea of creating quantum computers and the creation of both Shor and Grover's algorithms!
- **2003:** the term "post quantum cryptography" (PQC) is created by **Daniel Bernstein**<sup>1458</sup>.
- **2006:** the first international **PQCrypto** workshop is held in Belgium to study ways to circumvent quantum computer attacks at a time when you can barely assemble two qubits. The program consists in finding successors to the quantum-resistant public key cryptography algorithms RSA and ECC<sup>1459</sup>. The 12-person program committee includes among others Louis Goubin from the University of Versailles and Phong Nguyen and Christopher Wolf from the ENS. From this first edition, four of the five pillars of the PQC are established with the code-based crypto, lattice codes, hash Lamport signature and multivariate cryptography. The isogenies will arrive later. Two French researchers propose two of these four tracks: Nicolas Sendrier, from Inria, with "Post-quantum code-based cryptography" and Jacques Stern from ENS with "Post-quantum multivariate-quadratic public key schemes"<sup>1460</sup>. These workshops have since been held every one to two years around the world. The [2013 edition took place](#) in Limoges, France.
- **2012:** the NIST (National Institute for Standards & Technologies) launches its first projects and a team on PQC.



<sup>1456</sup> See [Experimental authentication of quantum key distribution with post-quantum cryptography](#) by Liu-Jun Wang et al, May 2021 (7 pages).

<sup>1457</sup> I extracted a piece of it from [Quantum cryptanalysis - the catastrophe we know and don't know](#) by Tanja Lange, a researcher from the Netherlands, 2017 (33 slides).

<sup>1458</sup> Daniel Bernstein is the author with Johannes Buchmann and Erik Dahmen of the impressive book [Post-Quantum Cryptography](#), 2009 (254 pages) which describes well the challenges of PQC.

<sup>1459</sup> The proceedings are in [PQCrypto 2006 International Workshop on Post-Quantum Cryptography](#), May 2006 (254 pages).

<sup>1460</sup> Source: [Quantum Computing and Cryptography Today](#) by Travis L. Swaim, University of Maryland University College (22 pages).

- **2014:** the **European Union** launches a Horizon 2020 call for projects on PQC. At the same time, ETSI, the European Telecoms Standardization Body, also launches its working group on PQC.
- **2015:** NIST organizes its first PQC workshop. ETSI published a reference document on QC<sup>1461</sup>. The NSA woke up and declared that the transition to PQC would become a priority<sup>1462</sup>. The NSA is playing two roles each time: it wants to protect itself and the sensitive communications of the U.S. government with good encryption systems but at the same time maintain the ability to break the codes of standard commercial communications and those from other countries. This relies on the brute force of giant supercomputers and a highly asymmetrical technical resources. In 2015, the European project PQCrypto coordinated by Tanja Lange is launched<sup>1463</sup>.
- **2016:** NIST publishes [QCP Progress Report](#) (15 pages) and an associated standardization roadmap. It also marks the launch of the [RISQ](#) (Regroupement de l'Industrie française pour la Sécurité Post-Quantique) investment program for the future, which, in addition to various laboratories (CEA, CNRS, INRIA, UMPC), includes private companies such as CryptoExperts, Secure-IC and Thales. They made submissions of proposed standards to NIST in 2017. RISQ is piloted by Secure-IC.
- **2017:** marks the end of the PQC standardization proposal submissions to NIST. By the end of 2017, 69 applicants are accepted out of 82, mainly with Euclidean networks (lattice codes) and error correction codes (code based PQC). In the same year, the 8th PQCrypto workshop was held in Utrecht, The Netherlands.
- **2019:** 26 candidates were selected by NIST in February to move to the second stage, including 17 candidates for public key encryption solutions and 9 for signatures<sup>1464</sup>. These include three projects involving Worldline, which until 2019 was part of the Atos Group. For its part, Inria (France) was involved in 7 of the 26 selected projects.

**2019 second round candidates,  
2020 finalists and 2020 alternate candidates**

<a href="#">BIKE</a>	<a href="#">LEDAcrypt</a>	<a href="#">Rainbow</a>
<a href="#">Classic McEliece</a>	<a href="#">LUOV</a>	<a href="#">ROLLO</a>
<a href="#">CRYSTALS-DILITHIUM</a>	<a href="#">MQDSS</a>	<a href="#">Round5</a>
<a href="#">CRYSTALS-KYBER</a>	<a href="#">NewHope</a>	<a href="#">RQC</a>
<a href="#">FALCON</a>	<a href="#">NTRU</a>	<a href="#">SABER</a>
<a href="#">FrodoKEM</a>	<a href="#">NTRU Prime</a>	<a href="#">SIKE</a>
<a href="#">GeMSS</a>	<a href="#">NTS-KEM</a>	<a href="#">SPHINCS+</a>
<a href="#">HQC</a>	<a href="#">Picnic</a>	<a href="#">Three Bears</a>
<a href="#">LAC</a>	<a href="#">qTESLA</a>	

- **2020:** results of the third round of NIST candidate selection in July, which kept 15 out of the 26 candidates from the previous round<sup>1465</sup>. This selection includes 7 teams that were finalists for this stage and 8 teams that propose lower quality solutions that need to be further evaluated (aka “alternate candidates”). NIST planned to hold a fourth round of selection in 2021. See their list in the above table<sup>1466</sup>.

Here are the participants countries, research teams and vendor organizations per project.

<sup>1461</sup> See [Quantum Safe Cryptography and Security](#) (64 pages).

<sup>1462</sup> See [Commercial national security algorithm suite and quantum computing FAQ IAD](#) (11 pages).

<sup>1463</sup> It is documented in [Post-Quantum Cryptography for Long-Term Security](#) (10 pages).

<sup>1464</sup> See [NIST Post-Quantum Cryptography - A Hardware Evaluation Study](#), 2019 (16 pages), [Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process](#), 2019 (27 pages) and [Recent Developments in Post Quantum Cryptography](#) by Tsuyoshi Takagi, November 2018 (38 slides).

<sup>1465</sup> See [PQC Standardization Process: Third Round Candidate Announcement](#), July 2020.

<sup>1466</sup> The Bit-flipping Key Encapsulation (BIKE) was codeveloped by Intel. It's a public key based encryption. Decoding can be done with 1.3 million operations at 110 MHz on an Intel Arria 10 FPGA in 12 ms.

	finalists	research teams	vendors teams
Public-Key Encryption/KEMs	Classic McEliece	UK: U. London, U. Plymouth. Switzerland: ETH Zurich. USA: U. Illinois & Chicago, U. Florida, Yale. Europe: U.Ruhr Bochum, U. Eindhoven, U. Southern, Denmark, MPI, Inria (France). Taiwan: Academia Sinica.	Google PQ Solutions
	CRYSTALS-KYBER	USA: SRI. Canada: U. Waterloo. Europe: Radboud U. Netherlands, Ruhr U. Bochum, ENS Lyon.	IBM Research Europe Arm NXP Semiconductors
	NTRU	Europe: Radboud U Netherlands, Eindhoven U. USA: Brown U. Canada: U. Waterloo.	Qualcomm NTT Algorand
	SABER	Europe: KU Leuven (Belgium). UK: Birmingham U.	
Digital Signatures	CRYSTALS-DILITHIUM	USA: Florida Atlantic U. Switzerland: ETH Zurich. Europe: CWI Netherlands, Ruhr U. Bochum, MPI, ENS Lyon.	IBM Research Europe Google
	FALCON	Europe: ENS Paris, U. Rennes (France). USA: Brown U.	IBM Research PQShield, Qualcomm Ethereum Foundation Thales
	Rainbow	Europe: FAU Erlangen Nuremberg, U. Versailles. USA: Cincinnati U. Taiwan: Academia Sinica, National Taiwan U.	

(cc) compilation Olivier Ezratty, June 2021

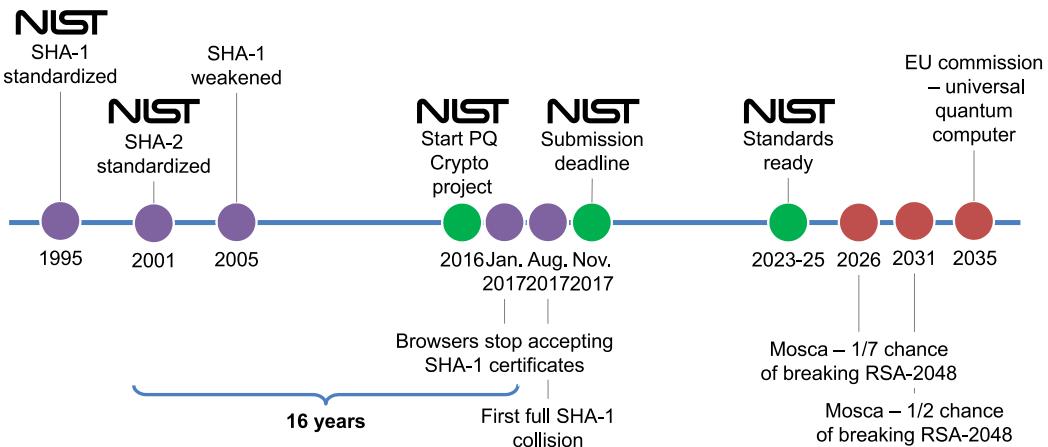
And the alternate candidates:

	finalists	research teams	vendors teams
Public-Key Encryption/KEMs	BIKE	USA: U.Washington, Florida U. Europe: U. Limoges, ENAC & U. Toulouse, Inria, U. Bordeaux (France), U. Ruhr Bochum (Germany). Israel: U. Haifa.	Intel Google IBM Worldline France
	FrodoKEM	USA: U. Michigan, Stanford U. Netherlands: CWI. Canada: U. Waterloo. Middle-East: Ege University (Turkey).	NXP Microsoft Research
	HQC	France: ISAE-Supaero, Limoges U., ENAC, U. Toulouse, Toulon U., Bordeaux U. USA: Florida U.	Worldline France and Netherlands
	NTRU Prime	Taiwan: Academia Sinica, National Taiwan U. Australia: U. Adelaide. Europe: Eindhoven U (Netherlands), Hamburg U. (Germany), Tampere U. (Finland). USA: Illinois U.	NXP
Digital Signatures	SIKE	USA: Florida U. Canada: Waterloo U., Toronto U. Europe: Radboud U. Netherlands, U. Versailles (France).	evolutionQ Amazon Microsoft Research Infosec Global Texas Instruments
	GeMSS	France: Inria, University of Versailles and Sorbonne Université.	CryptoNext Orange
	Picnic	USA: Northwestern U., GeorgiaTech, U. Maryland., Princeton U. Europe: Austrian Institute of Technology, TU Graz (Austria), Aarhus U. (Denmark), DTU (Denmark).	Microsoft Research Dfinity
	SPINCS+	Europe: U.Ruhr Bochum, KU Leuven, TU Graz, Eindhoven U, Radboud U.	Cisco, Infineon Infosec Global Genua, Taurus

(cc) compilation Olivier Ezratty, June 2021

- **2022/2024:** planned publication of PQC standards drafts by NIST. It must be noted that the NIST challenge embedded some constraints on intellectual property. Strictly said, NIST doesn't object to the contestants having some patents related to their submitted protocols. But they favor royalty-free ones and IP licensing without compensation, under reasonable terms (RAND) and conditions that are demonstrably free of unfair discrimination. While this could certainly accelerate their adoptions, this may indirectly favor large cybersecurity vendors who already have an existing customer base.

- **2025:** NIST's target date for finalizing PQC standards. Deployments of these standards would begin with the rapid deployment of commercial solutions supporting these standards. Fast, for the simple reason that the candidates are often in the standardization consortia. Some of them are already testing their solutions.



source: [Introduction to post-quantum cryptography and learning with errors](#), Douglas Stebila, 2018 (106 slides).

There are five distinct categories of PQC standards, as follows. I will not be able to technically describe them all except for the first category<sup>1467</sup>. In the last part of this section on cryptography, we will mention the case of some startups that are positioned in this market.

**Table 2 - Comparison on encryption schemes (RSA decryption = 1, size in bits, k security strength)**

Algorithm	KeyGen (time compared to RSA decrypt)	Decryption (time compared to RSA decrypt)	Encryption (time compared to RSA decrypt)	PubKey (key size in bits to achieve 128 bits of security)	PrivateKey (key size in bits to achieve 128 bits of security)	Cipher text (size of resulting cipher text)	Time Scaling	Key Scaling
NTRU	5	0.05	0.05	4939	1398	4939	$k^2$	$k$
McEliece	2	0.5	0.01	1537536	64861	2860	$k^2$	$k^2$
Quasi-Cyclic MDPC McEliece	5	0.5	0.1	9857	19714	19714	$k^2$	$k$
RSA	50	1	0.01	3072	24,576	3072	$k^6$	$k^3$
DH	0.2	0.2	0.2	3072	3238	3072	$k^4$	$k^3$
ECDH	0.05	0.05	0.05	256	256	512	$k^2$	$k$

Note: in key scaling, the factor  $\log k$  is omitted.

source : [Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges](#), ETSI, 2015 (64 pages).

<sup>1467</sup> See in particular [A Guide to Post-Quantum Cryptography](#) by Ben Perez, October 2018.

Established companies are not left out. **IBM** announced in August 2019 a system for archiving information on magnetic bank that integrates post-quantum cryptography<sup>1468</sup>. They use encryption based on Euclidean networks. As it is usually long-term storage, it is necessary to keep the decryption software for the same length of time to avoid ending up with a pile of data that cannot be reused. IBM is also involved in the three consortia that responded to the NIST call for proposals. **Kudelski Security** (Switzerland) is also interested in PQC.

**IBM** is part of three consortium submissions to the NIST call for post-quantum standards

- CRYSTALS** (Cryptographic Suite for Algebraic Lattices)
  - Kyber** is a CCA-secure key encapsulation mechanism, whose security relies on the hardness of the module-LWE problem.
  - Dilithium** is a digital signature scheme whose security is based on the module-LWE and module-SIS problems.
- FALCON**
  - FALCON** is a digital signature scheme using Fast-Fourier lattice-based compact signatures over NTRU.

What crypto vulnerability took more than 800 days to identify, cost more than \$500 million to fix, and years later, nearly 200,000 websites are still at risk

(CVE-2014-0160) OpenSSL Heartbleed Vulnerability

Jan 2017: (<https://thehackernews.com/2017/01/heartbleed-openssl-vulnerability.html>).

**Atos** and **Thales** are interested in France. The **ANSSI** published an information note in May 2020 in which it expressed certain reserves about the QKD<sup>1469</sup>. It highlighted the fact that it does not address a common problem, cannot guarantee perfect inviolability and requires dedicated optical infrastructures. Instead, it recommends to focus on PQC. This followed a memo of equivalent content from their British NCSC counterparts published in April 2020<sup>1470</sup>. A similar publication from the **NSA** was published in October 2020 ([source](#)).

## Code-based cryptography

This cryptographic system invented in 1978 by **Robert McEliece**, long before Shor's algorithm, has since resisted all cryptanalysis attacks, either classical or designed with quantum algorithms. It is the oldest of the PQC codes which was even a PQC before its time. The method consists in multiplying the data to be encrypted, represented as binary vectors (of length k), by a public and static matrix with more columns than rows (k x n), aka a "binary Goppa code".

This multiplication generates a vector larger than the original vector (with n bits). We then add a binary vector which adds random errors to the result but of constant value (vector z in schema with a given number of 1s). It is described as a "*uniformly random word of weight t*". It is a series of random bits containing a fixed number "t" of 1s called a Hamming weight. The public key sent by the receiver to the transmitter is the matrix  $\hat{G}$  and this number of errors t.

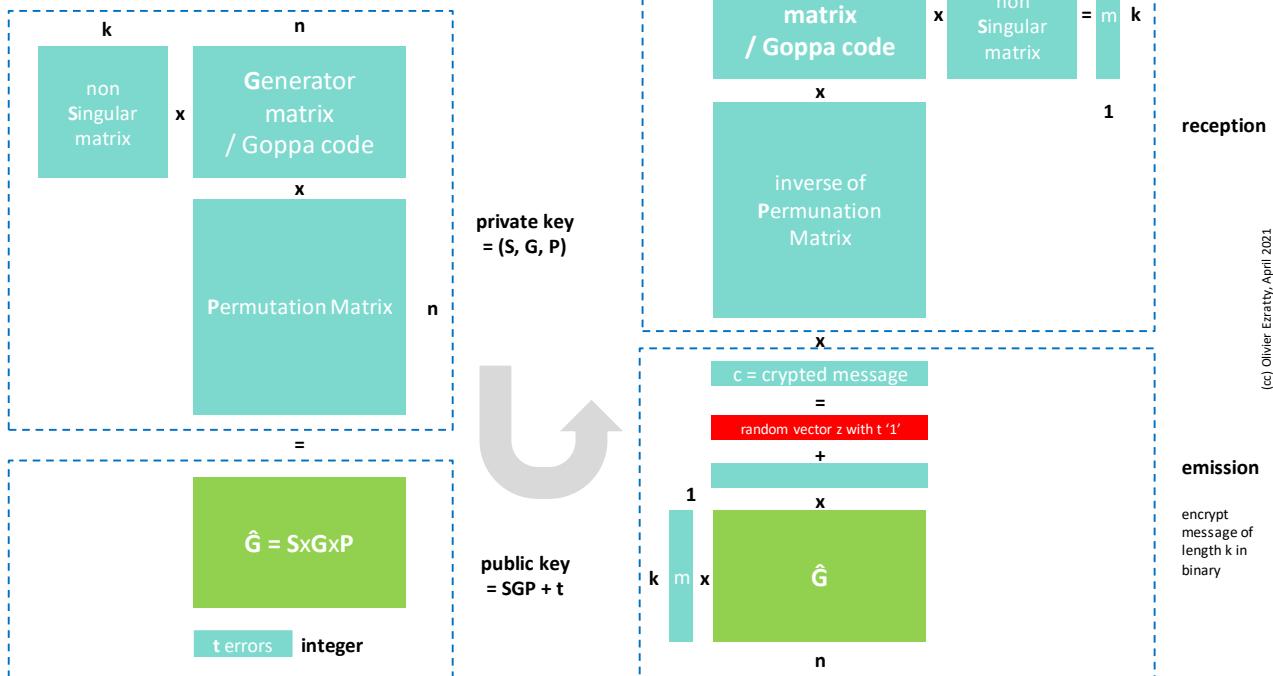
The three matrices having created  $\hat{G}$  constitute the private key. This matrix  $\hat{G}$  is the multiplication of three matrices called SGP for "non Singular", "generator matrix / Goppa code" and "Permutation matrix". The message decoding uses inverses of matrix S, P and G. This is explained in this diagram. The G matrix is designed to remove the "t" errors introduced in the encryption phase.

<sup>1468</sup> See [IBM's quantum-resistant magnetic tape storage is not actually snake oil](#) by Kevin Coldewey in TechCrunch, August 2019.

<sup>1469</sup> See [L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés?](#) by ANSSI, May 2020 (6 pages).

<sup>1470</sup> See [Quantum Security Technologies](#), NCSC, March 2020 (4 pages) and a detailed response in [Quantum safe cryptography - the big picture - Fact Based Insight](#) by David Shaw, 2020.

# code-based cryptography



This system generates public keys one hundred times larger than with RSA, of the order of 80 KB. It generates new vulnerabilities if you reduce their size.

The advantage of the PQC category is its good encryption and decryption speed. It can even be accelerated by using a dedicated FPGA chipset<sup>1471</sup>.

Breaking this kind of encryption is an NP-Hard problem that is currently inaccessible to quantum computing, even though to resist quantum computing it would still require a fairly large key of at least 1 MB<sup>1472</sup>.

## Lattice-based cryptography or Euclidean networks

The technique was proposed in 1996 by Miklos Ajtai, a researcher at IBM, and implemented in a public key system in 2005 by Oded Regev with its LWE (Learning With Errors) system and improved since then by many researchers.

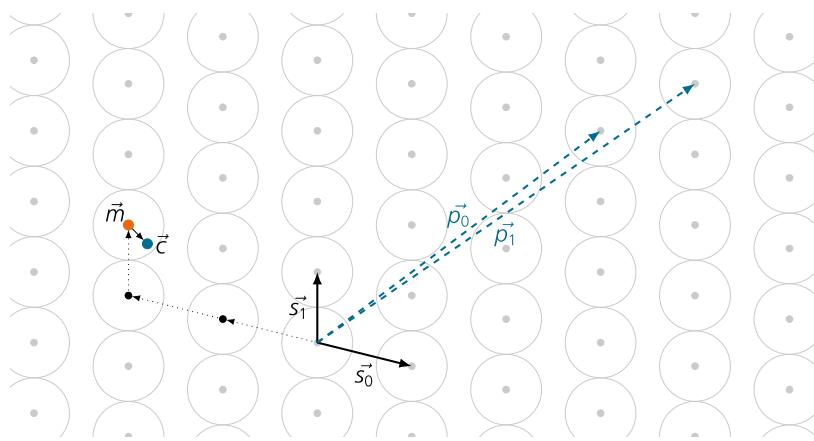
The associated literature is inaccessible for non-specialists. It is not easy to understand how this encryption method works despite the elegance of the diagrams that present the notion of Euclidean network like the one *below*<sup>1473</sup>. Basically, it is a matrix of dots that allows to locate points according to their coordinates according to a mark of different vectors between the public and private keys.

<sup>1471</sup> As seen in [Code-Based Cryptography for FPGAs](#) by Ruben Niederhagen, 2018 (73 slides).

<sup>1472</sup> The resistance of this method to attacks is documented in [Code-Based Cryptography](#) by Tanja Lange, 2016 (38 slides). For more information, see also [Code Based Cryptography](#) by Alain Couvreur, 2018 (122 slides) and [Some Notes on Code-Based Cryptography](#), a thesis by Carl Löndahl, 2014 (192 pages).

<sup>1473</sup> See [Practical Post-Quantum Cryptography](#) by Ruben Niederhagen and Michael Waidner, 2017 (31 pages).

An error is added to the coordinates generated with the public key vector. Only the coordinate vectors of the private key can be used to retrieve the coordinate of the encrypted value. Initially, it suffered from performance problems, but effective solutions appeared such as [NTRU](#), created in 1998 by Jeffrey Hoffstein, Jill Pipher and Joseph Silverman. The method advantage is to use small public keys. Its decryption is an NP-complete problem inaccessible to quantum computing. On the other hand, it is a method protected by many patents, so it is proprietary and potentially expensive<sup>1474</sup>.



**Figure 3.2:** Example for lattice-based encryption in a two-dimensional lattice: The secret, well-formed base is  $\{\vec{s}_0, \vec{s}_1\}$ ; the public, "scrambled" base is  $\{\vec{p}_0, \vec{p}_1\}$ . The sender uses  $\{\vec{p}_0, \vec{p}_1\}$  to map the message to a lattice point  $\vec{m}$  and adds an error vector to obtain the point  $\vec{c}$ . The point  $\vec{c}$  is closer to  $\vec{m}$  than to any other lattice point. Therefore, the receiver can use the well-formed secret base  $\{\vec{s}_0, \vec{s}_1\}$  to easily recover  $\vec{m}$  (dotted vectors); this is a hard computation for an attacker who only has the scrambled base  $\{\vec{p}_0, \vec{p}_1\}$ . For a secure scheme, the dimension of the lattice must be much higher than 2 as in this example.

The PQC **New Hope** solution (CECPQ1) which was tested in 2016 for a few months by [Google](#) in Chrome and is based on Ring-LWE is in this class of methods. Since 2019, they have moved to CECPO2 which includes a variant of the HRSS key exchange system that is among the bidders in the NIST competition and the selected in the last wave in the NTRU project<sup>1475</sup>.

In France, a team from the IRISA-EMSEC laboratory is developing a cryptographic solution based on these Lattice base systems, also named Euclidean networks.

Damien Stehlé is another specialist of the domain, doing research at ENS Lyon. He participated to the creation of CRYSTALS - Kyber, a finalist in 2020 of NIST's PQC competition.

## Isogeny-based cryptography

This variant of elliptic curves is even less easy to grasp than all of the above. It is a "*morphism of superimposed group and finite kernel between two elliptic curves*". Piece of cake! The system was proposed in 2006 by Alexander Rostovtsev and Anton Stolbunov and then broken by quantum cryptanalysis by Andrew Childs, David Jao and Vladimir Soukharev. This led David Jao and Luca De Feo (Inria) to propose in 2011 the use of "super-singular" curves to correct this flaw<sup>1476</sup>.

Software publisher **Cloudflare** has released an open-source security solution based on isogenies, CIRCL (Cloudflare Interoperable Reusable Cryptographic Library). It is published on GitHub. Their SIKE key encapsulation solution has been submitted to NIST. In January 2019, they were among the 17 finalist candidates for public key encryption or key creation solutions<sup>1477</sup>.

<sup>1474</sup> For more information, see the thesis [Lattice-based cryptography: a practical implementation](#) by Michael Rose, 2011 (103 pages), [Lattice-based Cryptography](#) by Daniele Micciancio and Oded Regev, 2008 (33 pages) and the slightly more pedagogical but still incomprehensible [Overview of Lattice based Cryptography from Geometric](#) by Leo Ducas, 2017 (53 slides).

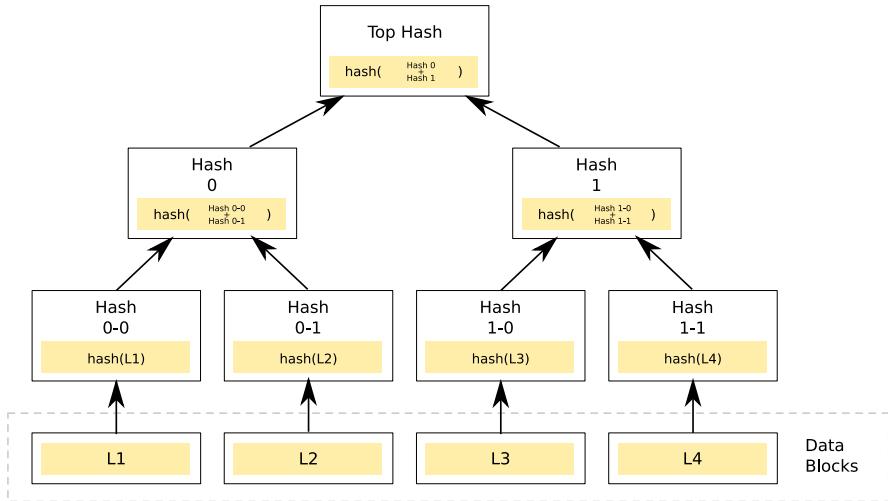
<sup>1475</sup> See [Experimenting with Post-Quantum Cryptography](#) by Matt Braithwaite, July 2016 and then [Google starts CECPO2, a new postquantum key exchange for TLS](#), January 2019.

<sup>1476</sup> More on this with [20 years of isogeny-based cryptography](#) by Luca De Feo, 2017 (84 slides), [An introduction to supersingular isogeny-based cryptography](#) by Craig Costello (Microsoft Research), 2017 (78 slides), [Isogeny Graphs in Cryptography](#) by Luca De Feo, 2018 (73 slides) and [An introduction to isogeny-based crypto](#) by Chloe Martindale, 2017 (78 slides).

<sup>1477</sup> See [Cloudflare wants to protect the internet from quantum computing](#), June 2019 and [Introducing CIRCL: An Advanced Cryptographic Library](#), June 2019.

## Hash-based signatures

This post-quantum cryptography other method also predates the very notion of quantum computer imagined by Richard Feynman in 1982. It is based on the work of **Leslie Lamport** of the SRI in 1979 and her single-use hash-based "signatures". The method was then improved by using hash trees also called Merkle trees to sign several messages. It is based on public keys of reduced size, down to 1 kbits



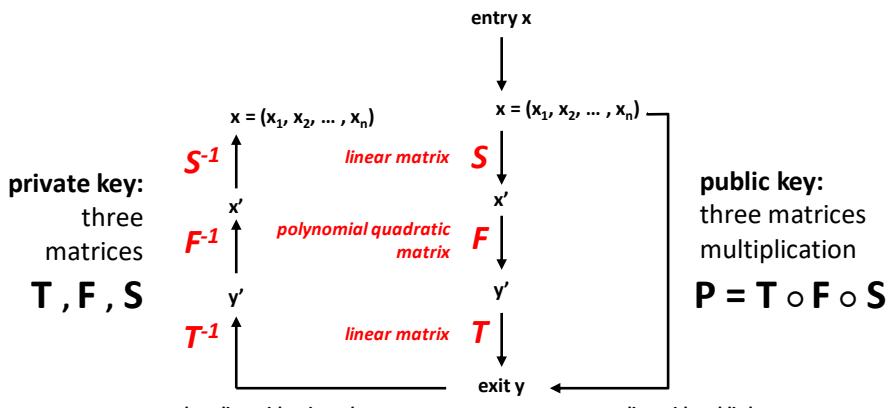
source: [Merkle Tree](#), Wikipedia.

This method is mainly used for electronic signature<sup>1478</sup>.

## Multivariate polynomial cryptography

This last group of methods is reminiscent of error correction codes. The public key is a multiplication of several matrices, two of which are linear and one quadratic (with squared values), the three separate matrices constituting the private key used to reconstruct the encrypted message.

Code breaking these keys is an NP-Hard problem, out of reach of quantum computing. The method dates from 2009 and was obviously then declined in several variants. The public keys are quite large, up to 130 KB (with the HFEBoost variant)<sup>1479</sup>. This encryption method is also rather used for electronic signatures.



We could imagine that QKD (physical protection of key distribution) could be combined with PQC (logical protection of encryption against quantum computer decryption). Actually, not really. QKD is rather dedicated to symmetric keys that assume protection of physical communication between correspondents, whereas PQC relies on public keys that do not need to be protected by QKD because their interception (without QKD) would already be useless to hackers.

<sup>1478</sup> If you are well versed in mathematics and cryptography, see [Hash-based Signatures: An Outline for a New Standard](#) (12 pages), [Design and implementation of a post-quantum hash-based cryptographic signature scheme](#) by Guillaume Endignoux, 2017 (102 pages) and [SPHINCS: practical stateless hash-based signatures](#), 2015 (30 pages).

<sup>1479</sup> Note the contribution of Jacques Stern from the ENS "Post-quantum multivariate-quadratic public key schemes" at PQCRYPTO 2006.

However, QKD for key exchange can be combined with PQC for authentication and data encryption. QKD requires authentication, which can be provided upstream by PQC. On the other hand, QKD can be redundant with PQC used for key exchange<sup>1480</sup>.

## Quantum homomorphic cryptography

Homomorphic cryptography consists in encrypting data that can then pass through a conventional processing in encrypted mode and give an encrypted result that will be decipherable at the end of the processing.

In machine learning and deep learning, this mode of encryption makes it possible to distribute training and inference processing of learning machine models in the cloud without the hacking of the transmitted data revealing the data content that feeds the model or inferences. The disadvantage of this method is that it does not work with all learning machine models and is very expensive in terms of machine time for data encryption and decryption.

Quantum homomorphic encryption is a similar approach for encoding data that will feed a quantum computer in the cloud and then decode the result of the processing. It is one of the tools for implementing so-called "blind computing" in the cloud, where servers cannot understand and interpret the data they process.

Various algorithms for encrypting quantum gate control programs have been proposed but are not yet commonly used<sup>1481</sup>. Some of the keys can be quantum-transmitted like a QKD. This is one of the conditions to be sure that the server part cannot interpret the processing it performs<sup>1482</sup>.

## Quantum telecommunications

As indicated at the beginning of this long section, QKD-based quantum cryptography is not the only application of quantum telecommunications<sup>1483</sup>. It is one of its applications. And, as we have already seen earlier in this book, quantum telecommunications are not about transmitting information faster than light<sup>1484</sup>.

One application area is the creation of quantum networks linking quantum "endpoints" that are themselves quantum, which could be quantum computers and even quantum sensors<sup>1485</sup>. In the first case, links between quantum computers would make it possible to create distributed computing architectures, following the example of classical distributed computing architectures that exist on the Internet, in data centers and within supercomputers.

---

<sup>1480</sup> To learn more about PQC, see in particular [Post-quantum cryptography - dealing with the fallout of physics success](#) by Daniel Bernstein and Tanja Lange, 2017 (20 pages).

<sup>1481</sup> See [Classical Homomorphic Encryption for Quantum Circuits](#) by Urmila Mahadev, 2018 (7 pages), [Quantum Fully Homomorphic Encryption With Verification](#), 2017 (30 pages and [slides](#), 28 slides), [Quantum Homomorphic Encryption: A Survey](#), 2017 (11 pages) et [Quantum homomorphic encryption for circuits of low T-gate complexity](#) by Anne Broadbent et Stacey Jeffery, 2015 (35 pages).

<sup>1482</sup> As indicated in [On the implausibility of classical client blind quantum computing](#) by Scott Aaronson, Elham Kashefi et al, 2017 (43 pages).

<sup>1483</sup> See the excellent [Quantum internet: A vision for the road ahead](#) by Stephanie Wehner et al, October 2018 (11 pages).

<sup>1484</sup> Let's remind at least two key explanations: first, entanglement and non-locality is about having a correlation between two distant quantum objects values when measured sequentially, but this value is random by essence. You can't set one quantum value at one end (Alice) and then measure it at the other location (Bob's). You just decide to measure random values at both end that happen to be correlated. On a more practical reason, the teleportation algorithm that can send a qubit state to another location with using entanglement needs two classical communications links. So, we're stuck with the speed of light. See [No, We Still Can't Use Quantum Entanglement To Communicate Faster Than Light](#) by Ethan Siegel, February 2020.

<sup>1485</sup> See [Repeater-enhanced distributed quantum sensing based on continuous-variable multipartite entanglement](#) by Yi Xia et al, 2018 (9 pages).

A direct link between quantum computers and quantum telecommunications would have enormous advantages for implementing secured processing. This is part of the concept of "blind computing" with the BFK protocol created in 2009 by Anne Broadbent, Joe Fitzsimons and Elham Kashefi<sup>1486</sup>. The principle consists in preparing computation in a quantum way at the starting point and sending it by a quantum link by teleportation to the remote quantum computer.

It is a bit the quantum equivalent of the homomorphic encryption used in the learning machine. One way to manage the confidentiality of the processing is to partition the processing on several quantum computers.

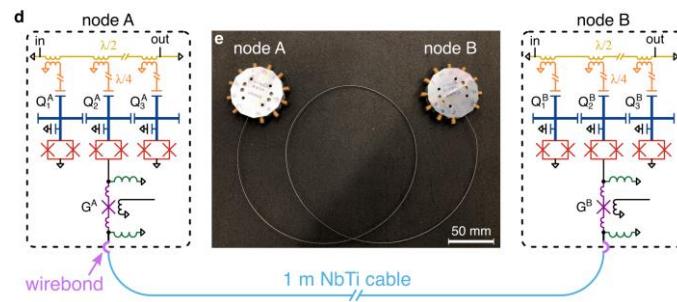
However, communication between quantum computers is not an easy task. It should indeed be possible to convert the qubit state of these machines into quantum states of photons - usually in the infrared range at 1550 nm - for optical transmission. Apart from the photon-based systems case, qubits are most often electrons spins or atoms energy states. Hence the numerous efforts to make conversions between these qubits states and qubits encoded in transmissible photons.

In superconducting qubits, we know how to convert the state of a qubit into microwaves. These are in the 6-8 GHz range, not in the infrared range. These microwaves can be used for short distance communication between processing units as was realized by an international team led by the University of Chicago.

They connected two nodes of three superconducting qubits, each arranged as an entangled GHZ state, and managed this entanglement transmission with microwaves on a distance of one meter on a niobium-titanium coax cable. The entanglement transmission was done with a fidelity of 65% and 91% for a single qubit transmission. It's a first promising step<sup>1487</sup>.

Others, from ETH Zurich and the University of Sherbrooke in Canada are even connecting several superconducting units using connected cryogenic systems. This enables the connection between these units with microwave waveguides<sup>1488</sup>. The two processing units were separated by a 5 meters cryogenic link where the microwaves are transmitted.

Other efforts are undertaken to connect heterogeneous quantum networks with hybrid entanglement swapping between DV and CV photonic systems<sup>1489</sup>. More classically, qubits can be distantly connected through a photonic link, as MPQ researchers in Germany did show in 2021<sup>1490</sup>.



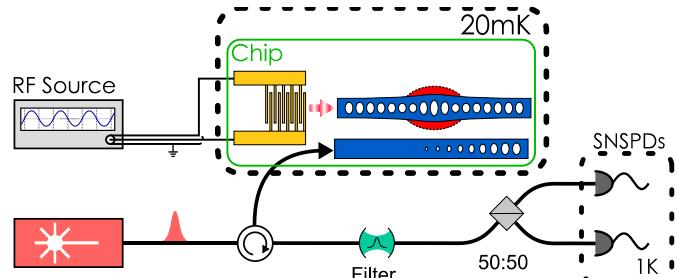
<sup>1486</sup> See [Universal blind quantum computation](#) by Anne Broadbent, Joseph Fitzsimons and Elham Kashefi, 2008 (20 pages) and the [associated presentation](#) (25 slides), [Blind quantum computing can always be made verifiable](#) by Tomoyuki Morimae, 2018 (5 pages), [Experimental Blind Quantum Computing for a Classical Client](#), 2017 (5 pages) and [Blind Quantum Computation](#) by Charles Herder (5 pages).

<sup>1487</sup> See [Deterministic multi-qubit entanglement in a quantum network](#) by Youpeng Zhong, Audrey Bienfait (ENS Lyon), et al, November 2020 on Arxiv and February 2021 in Nature (38 pages).

<sup>1488</sup> See [Microwave Quantum Link between Superconducting Circuits Housed in Spatially Separated Cryogenic Systems](#) by P. Magnard et al, PRL, December 2020 (13 pages).

<sup>1489</sup> See [Quantum Networking Demonstrated for First Time](#) par Dhananjay Khadilkar, November 2018, referencing [Connecting heterogeneous quantum networks by hybrid entanglement swapping](#) by Giovanni Guccione, Tom Darras et al, May 2020 (7 pages).

For longer distance, microwaves are converted to another frequency range while keeping the quantum state. This conversion can be done with opto-electromechanical systems<sup>1491</sup>. Delft researchers led by Simon Gröblacher experimentally achieved this in 2018, at 20 mK, close to superconducting qubits operating temperature<sup>1492</sup>.



It led to the creation in 2021 of **QPhox** (2021, Netherlands, 2.4M€) by Simon Gröblacher, a startup financed by Quantonation. The research project turned into a quantum modem for the quantum Internet<sup>1493</sup>.

Trapped ions and cold atoms are controlled by lasers, but converting their quantum state into a photon is no small matter either. Silicon qubits use the spin of one or two electrons. Spin-to-charge and charge-to-photon conversions can then be performed.

In 2021, another team from Qutech and TU Delft made another progress with connecting three qubits quantumly in an entangled GHZ state, beyond the traditional two nodes existing experiments<sup>1494</sup>.

Photons may also need their own conversion, between the wavelength used in quantum memories and in dark fibers quantum telecommunications (from 606 nm to 1552 nm)<sup>1495</sup>.

**Next Generation Quantum** (2019, USA) is CUNY university spin-off created by German Kolmakov (CTO) and Shaina Raklyar (CEO) developing commercial quantum computing applications and a hardware and software solution interconnecting multiple quantum computers to create quantum computer clusters. They plan to manage this connection with photons and to use cavity polaritons, photons dressed with charges in a semiconductor optical microcavity that are sensitive to electric fields.

Other researchers are looking for ways to encode quantum information differently in transmitted photons. Instead of using a classical polarization encoding, researchers from Caltech experimented quantum teleportation of time-bin qubits (with “time of arrival” encoding) using a standard telecommunication wavelength of 1536.5 nm with an average success superior to 90%<sup>1496</sup>. There are also experiments of qubit transmission with entanglement resources between atom-based quantum memories<sup>1497</sup>.

<sup>1490</sup> See [Quantum systems learn joint computing - MPQ researchers realize the first quantum-logic computer operation between two separate quantum modules in different laboratories](#), February 2021.

<sup>1491</sup> See also [A quantum microwave-to-optical transducer](#) by Thibaut Jacqmin of LKB, 2019 (17 slides) which describes opto-electromechanical mechanisms for state conversion of superconducting qubits into transportable photons on optical fibers.

<sup>1492</sup> See [New horizons for connecting future quantum computers into a quantum network](#), October 2019 which references [Microwave-to-optics conversion using a mechanical oscillator in its quantum ground state](#) by Moritz Forsch et al, 2019 (11 pages).

<sup>1493</sup> See [The widely anticipated quantum internet breakthrough is finally here](#) by Maija Palmer, May 2021 and [A perspective on hybrid quantum opto- and electromechanical systems](#) by Yiwen Chua and Simon Gröblacher, 2020 (7 pages). Simon Gröblacher also created Nenso Solutions, a quantum technology consulting company.

<sup>1494</sup> See [Realization of a multi-node quantum network of remote solid-state qubits](#) by Matteo Pompil, Sophie Hermans, Stephanie Wehner et al, February 2021 (28 pages).

<sup>1495</sup> See [Quantum frequency conversion of memory-compatible single photons from 606 nm to the telecom C-band](#) by Nicolas Maring, Dario Lago-Rivera et al, IFCO, 2021 (7 pages).

<sup>1496</sup> See [Teleportation Systems Toward a Quantum Internet](#) by Raju Valivarthi et al, Caltech, 2020 (16 pages).

<sup>1497</sup> See [Efficient reversible entanglement transfer between light and quantum memories](#) by Mingtao Cao, Julien Laurat et al, LKB ENS Paris, 2020 (6 pages).

In August 2021, AMD published a patent designed to handle a local scale-out capacity for quantum computers, with a teleportation-based multi-SIMD architecture. SIMD stands for “Single Instruction Multiple Data” and is heavily used in parallel classical hardware architectures like vector processors or tensor processors and GPUs. Here, teleportation would be used to handle coordination between several quantum processing units and reduce both the number of qubits and quantum gates needed to run an algorithm. Unfortunately, this patent doesn’t describe in any way a real quantum process, contains no physics, no maths, no compiling trick, no timing analysis and nothing about teleportation implementation and about any quantum algorithm parallelization. It also mentions a “global memory” like if creating qubits memory was some standard off-the-shelf technology. On top of that, none of the patent holders seem to have a quantum computing background and they never published any quantum-related paper visible on Arxiv<sup>1498</sup>. This has the flavor of a PR-driven approach that only a few scientists can fact-check, if not of a patent-troll. And it unfortunately worked<sup>1499</sup>!

Research in these areas is progressing step by step, and revolves essentially around photonics and light-matter interactions<sup>1500</sup>, and up to entangling different quantum objects<sup>1501</sup>.

Three other areas must make progress to enable the deployment of quantum telecommunications networks: repeaters<sup>1502</sup>, switches<sup>1503</sup> and quantum memory<sup>1504</sup>. In that later case, Chinese researchers succeeded in 2019 to entangle two rubidium atoms-based quantum memories via entangled photons at a distance of 50 km<sup>1505</sup>.

In the network layout domain, a team led by British and Austrian researchers established an any-to-any quantum communication link with 8 network nodes using dense wavelength division multiplexers (DWDM) and a single source of polarization-entangled photon pairs<sup>1506</sup>.

---

<sup>1498</sup> See [New AMD Patent Proposes Teleportation to Make Quantum Computing More Efficient](#) by Francisco Pires, August 2021.

<sup>1499</sup> See for example [AMD patent reveals revolutionary teleportation-based quantum computer](#) by Bogdan Solca, Notebook Check, August 2021.

<sup>1500</sup> See for example [First chip-to-chip quantum teleportation harnessing silicon photonic chip fabrication](#) by the University of Bristol, December 2019 which refers to [Chip-to-chip quantum teleportation and multi-photon entanglement in silicon](#) by Daniel Llewellyn et al, 2019 (48 pages). And the exaggerated version in [The first "quantum teleportation" between two computer chips](#) by Valentin Cimino, December 2019.

<sup>1501</sup> See [Entanglement between Distant Macroscopic Mechanical and Spin Systems](#) by Rodrigo A. Thomas et al, March 2020 (24 pages).

<sup>1502</sup> See [Adaptive bandwidth management for entanglement distribution in quantum networks](#) by Navin B. Lingaraju et al, 2021 (5 pages).

See [Telecom-heralded entanglement between multimode solid-state quantum memories](#) by Dario Lago-Rivera et al, Nature, IFCO, June 2021 (7 pages).

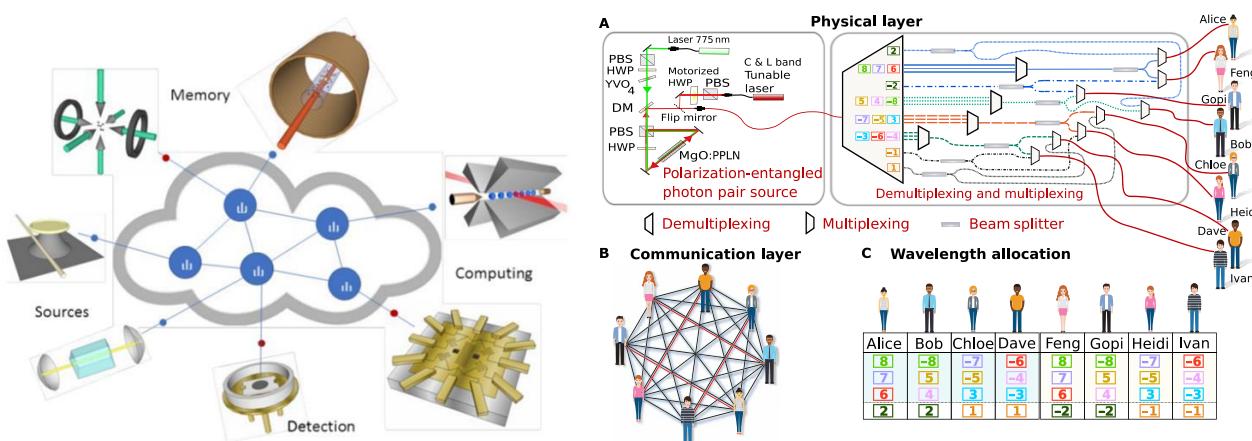
<sup>1503</sup> See [Development of Quantum InterConnects \(QuICs\) for Next-Generation Information Technologies](#) by David Awschalom et al, 2019 (31 pages) and [Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels](#), 2020 (14 pages).

<sup>1504</sup> See this general overview of quantum memories used in quantum networks: [Optical Quantum Memory and its Applications in Quantum Communication Systems](#) by Lijun Ma et al of NIST, 2020 (13 pages). The schema of this page on the Quantum Internet is derived from it.

<sup>1505</sup> See [New Record: Researchers have entangled quantum memory over 50 kilometers](#) by Stéphanie Schmidt, February 2020. The feat comes from Hefei's Jian-Wei Pan laboratory in China. This refers to the article published in Nature: [Entanglement of two quantum memories via fibers over dozens of kilometers](#) by Jian-Wei Pan et al, February 2020 and previously on Arxiv in March 2019: [Entanglement of two quantum memories via metropolitan-scale fibers](#) (19 pages).

<sup>1506</sup> See [A trusted node-free eight-user metropolitan quantum communication network](#) by Siddarth Koduru Joshi et al, September 2020 (9 pages) and the subsequent work [Flexible entanglement-distribution network with an AlGaAs chip for secure communications](#) by Félicien Appas, Eleni Diamanti, Sara Ducci et al, NPJ Quantum Information, July 2021 (12 pages).

Is this a “quantum Internet”? It’s still a marketing buzzword since many-nodes technologies are not really available and quantum entanglement distribution is an additional feature and not a replacement for existing classical networks.



Other applications of quantum telecommunications should be mentioned in addition to distributed computing:

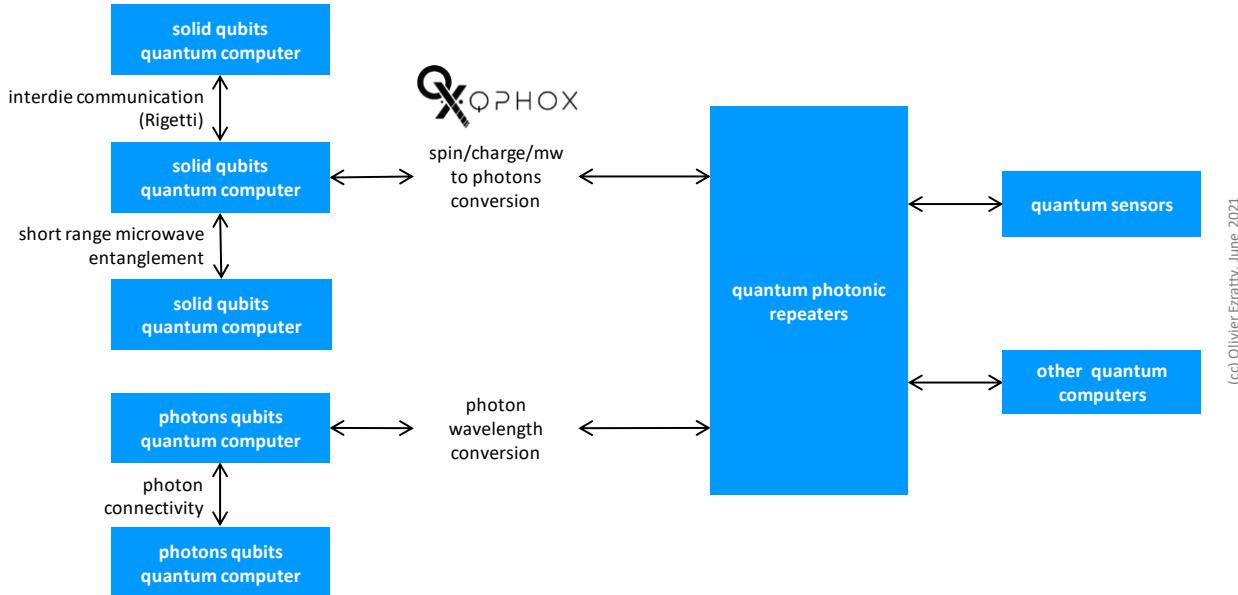
- **Quantum electronic signatures** that authenticate classic messages. They are transferable to third parties, non-repudiable and non-forgeable.
- **Connecting quantum sensors** which could be useful when it makes sense to consolidate quantum states from various quantum sensors and also protect their content.
- **Transmission of anonymous data**. It allows two nodes in a quantum network to communicate with each other without one node being able to identify the other node and also without the other nodes not involved in the protocol being able to identify the sender and the recipient. The communications leave no trace and are therefore not auditible. This replaces traditional anonymization proxies. It can be used as a basis for distributed processing, coupling this with classical or quantum data encryption. It is a means of ensuring the anonymization of the transmission of data such as survey or health data.
- **Quantum money** that applies a concept of Stephen Wiesner (1942-2021, Israeli) from 1970, and improved in 1983. It is based on tokens of verifiable integrity that can only be used once.
- **Clock synchronization** which has been tested in the early 2000s and is useful for telecommunication networks and GPS operations<sup>1507</sup>.
- **Detecting Extra-Terrestrial life**. Well, sort of. That’s the plan from SETI who wants to analyze “quantum communications” coming from exoplanets, which would bear some differentiated signature. One can wonder how such communications could be sorted out from the planet’s star random photon streams, but who knows<sup>1508</sup>.

At last, let’s mention the **Quantum Protocol Zoo** initiative launched by LIP6 and VeriQloud which inventories about 56 quantum telecommunication and cryptography protocols<sup>1509</sup>.

<sup>1507</sup> See [Distant clock synchronization using entangled photon pairs](#) by Alejandra Valencia et al, 2004 (10 pages).

<sup>1508</sup> See [We could detect alien civilizations through their interstellar quantum communication](#) by Matt Williams, April 2021 referring to [Searching for interstellar quantum communications](#) by Michael Hippke, April 2021 (14 pages).

<sup>1509</sup> See [Protocol Library](#).



(cc) Olivier Ezratty, June 2021

## Quantum Physical Unclonable Functions

qPUF are the not most talked about quantum technologies. It is at the crossroads of quantum cryptography, QRNGs and embedded systems and sensors.

Generically, Physical Unclonable Functions (PUF) are systems containing a piece of classical hardware that contain some unique signature related to the random aspect of matter and physical disorder<sup>1510</sup>. This unique signature can't be reproduced. It can also be dynamically generated and always be different.

A PUF is implemented as a unique function and is hard to physically and logically clone. They operate on a challenge/response basis: a challenge is fed into the PUF, which generates a unique binary response coming from the hardware module, which is based on its unique material imperfections.

The physical imperfections used in PUF are manyfold: reflection of optical materials, random scattering of light, ring oscillators, coating materials capacitance up to some random characteristics of electronic components like SRAM and DRAM memories. The most common PUFs are using silicon IC and their various defects and variations that are even greater as their integration nodes become smaller, now down to 5 nm.

The generated binary strings are used in as keys or identifiers in cryptography systems and as anti-counterfeiting systems. These can also serve as generic true random number generators, either standalone or combined with other entropy sources. But these security systems are not perfect and are prone to various attacks<sup>1511</sup>, done with various methods including machine learning, side attacks and even, potentially, quantum computing<sup>1512</sup>.

<sup>1510</sup> See [Physical One-Way Functions](#) by Papu Srinivasa Ravikanth, 2001 (154 pages) and [Physically Unclonable Functions - a Study on the State of the Art and Future Research Directions](#) by Roel Maes and Ingrid Verbauwhede, 2010 (36 pages).

<sup>1511</sup> A side-channel attack collects information from a security system or influence its execution in an indirect manner, by collecting in a stealth way some data on hardware operations (quantity of data processed in a computer, heating, amount of gas in a car tank). Side-channels may be power dissipation, operations timing, system temperature, acoustic, radio or optical emissions or a mix of these.

<sup>1512</sup> Samsung Galaxy S10 launched in 2019 contains an Exynos 9820 chipset with PUF technology, for crypto wallets, associated with Samsung Knox, a built-in storage hardware for security keys used with Blockchain services and cryptocurrencies like Ethereum. According to Samsung, the Exynos "PUF generates an unclonable key for data encryption by using the unique physical characteristics of each chip" but this characteristic is not specified. Looks like this PUF was replaced in some subsequent Samsung smartphones by a QRNG coming from IDQ.

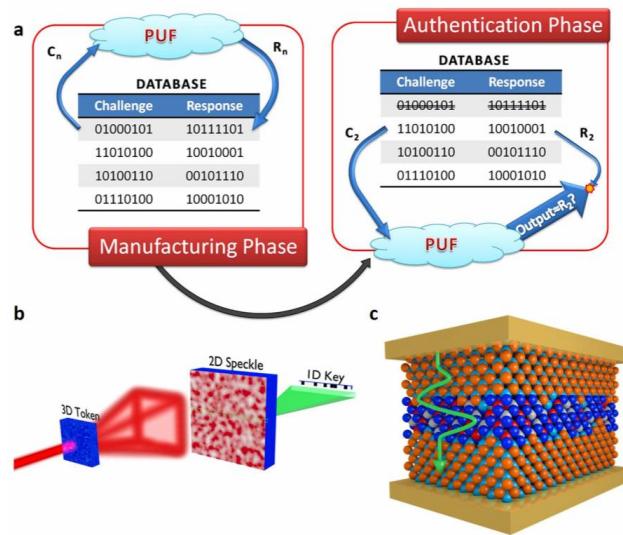
qPUFs are quantum equivalents of PUF that are based on quantum states and their physical unclonability. There's even a variation with Quantum read-out of PUF (QR-PUF) which reads-out quantumly a non-quantum physical disorder in a physical device. These qPUFs are better than classical PUFs but their resistance to forgery depends on their detailed level of unforgeability, which can be "existential" and "selective"<sup>1513</sup>.

What is the physical form of qPUFs? It can be based on photonic features and polarized prepared devices and multiple scattering medium.



**Quantum Base** (2014, UK, \$1.1M) offers various quantum product authentication solutions such as the Q-ID Optical, an optically readable "atomic" finger-print solution that uses Physically Unclonable Functions (PUFs) in the form of physical tags that cannot be copied at the atomic scale level<sup>1514</sup>.

The tag exploits a thin 2D layer of graphene that contains unique irregularities at the atomic scale that cannot be cloned. These irregularities would be amplified by unspecified quantum phenomena. Moreover, these tags can be dynamically activated and deactivated. The project stems from the work of Lancaster University of Robert Young who is the co-founder of the startup. The whole is integrated in a home-made random number generator (Q-RAND) based on a semiconductor diode, which can be integrated in a chipset ([video](#))<sup>1515</sup>. They also propose the Q-ID Electronic, a unique identifier generator.



## Quantum telecommunications and cryptography vendors

Let's now review the startups in this vast sector of activity of quantum and post-quantum cryptography, trying to describe the nature of their offer and their differentiation when the information is publicly available! I have only kept here startups offering technology solutions and not integrated consulting and integration companies.

Note that on the market size side, the market for quantum and post-quantum cryptography is modest for the moment. A 2017 report estimated it at \$2.5B by 2022<sup>1516</sup>.

However, it is expected to gain momentum from this period onward, following the finalization of standardization by NIST and ETSI.

<sup>1513</sup> See [Quantum Physical Unclonable Functions: Possibilities and Impossibilities](#) by Myrto Arapinis, Elham Kashefi et al, June 2021 (32 pages) and [A Unified Framework For Quantum Unforgeability](#) by Mina Doosti, Mahshid Delavar, Elham Kashefi and Myrto Arapinis, March 2021 (47 pages), all from the University of Edinburgh and CNRS LIP6 Paris.

<sup>1514</sup> This is documented in the USPTO patent US10148435B2 [Quantum Physical Unclonable Function](#) filed in 2015 (11 pages) and validated in 2018. It evokes a semiconductor component based on gallium arsenide, aluminum and antimony that generates a random spectral response that differs from one component to another. The process is described in [Using Quantum Confinement to Uniquely Identify Devices](#) by Robert Young et al, 2015 (8 pages).

<sup>1515</sup> The resonant-tunnelling diode (RTD) process is documented in [Resonant-Tunnelling Diodes as PUF Building Blocks](#), 2018 (6 pages).

<sup>1516</sup> See [New CIR Report States Quantum Encryption Market To Reach \\$2.5 Billion Revenues By 2022: Mobile Systems Will Ultimately Dominate](#), 2017.

## cryptography QKD/PQC



(cc) Olivier Ezratty, September 2021

In addition to startups, commercial offers in quantum and post-quantum cryptography are also proposed or about to be proposed by various large IT players such as **Batelle**, **Infineon**, **Raytheon**, **IBM**, **Cisco<sup>1517</sup>**, **Atos**, **Gemalto** (part of Thales group), **Microsoft<sup>1518</sup>**, **NEC**, **Toshiba**, **Huawei<sup>1519</sup>**, **KT** and **Samsung**.

**IBM** created a set of PQC protocols and participated to the NIST PQC competition. They were finalists of round 3 of the NIST selection in July 2020 for both lattice-based CRYSTALS-KYBER (secure key encapsulation mechanism) and CRYSTALS-DILITHIUM (secure digital signature). These were developed in partnership with **ENS Lyon** (France), **Ruhr-Universität Bochum** and **Radboud University** (Germany). These PQC solutions are embedded in an IBM TS1160 tape drive system with a modified firmware in combination with symmetric AES-256 encryption. It enables a secured long-term data storage. In November 2020, IBM also announced it would integrate these protocols in its cloud offering.

**Microsoft** also works on PQC algorithms. It includes FrodoKEM and SIKE which are PQC based key exchanges protocols. Then, qTesla and Picnic, PQC based signatures protocols.

Let's also mention **Toshiba**'s ambitions in QKD deployments, announced in October 2020. They are deploying a QKD based network for **ICT** (National Institute of Information and Communications Technology) in Japan, on top of a similar deployment undertaken with BT and their Openreach network in the UK in 2020 and demonstrations done with **Verizon** and **Quantum Exchange**. Their hardware offer includes the "Multiplexed QKD system" which can transmit QKDs at a key rate of 40 kb/s over 70 km, and high-speed data on the same fiber. The "Long Distance QKD System" has similar features with a key rate of 300 kb/s and a range of up to 120 km but requiring two fibers. These solutions using the (quite old) BB84 protocol are manufactured in Cambridge, UK and fit in a 3U 19" rack format.

<sup>1517</sup> Cisco's Quantum Research is led by Alireza Shabani.

<sup>1518</sup> See the [Microsoft site](#) that describes their activity in the PQC.

<sup>1519</sup> See [Continuous-Variable Quantum Key Distribution with Gaussian Modulation, the Theory of Practical Implementations](#), 2018 (71 pages). The Huawei team working on the QKD is partly located in their research center in Dusseldorf.

**ABCMintFoundation** (2017, Switzerland) created by Jin Liu and Jintai Ding is tasked with creating a quantum resistant Blockchain using a Rainbow Multivariable Polynomial Signature Scheme. It is a community driven open-source project. It uses keys that can be as large as 1.7MB.



**AegiQ** (2019, UK, \$1,8M) is developing quantum cryptography systems based on III-V photonic semiconductors. It was created by Max Sich as a spin-off of the University of Sheffield. They plan to equip telecommunication data centers for their fiber optical infrastructures upgrades to QKD.



**AgilePQ** (2014, USA) provides a software platform for "post-quantum" security of communication between connected objects and the cloud, such as drones.

It includes AgilePQ C-code, a piece of software that runs on connected object microcontrollers and consumes little power, and AgilePQ DEFEND, an adaptive size-based key generation system. DEFEND generates codes that are harder to break than AES 256 and with 429 orders of magnitude difference. Specifically, we go from a key space of 10 to the power of 77 to  $8 \times 10$  to the power of 506 (factor of 256)<sup>1520</sup>. The system that is patented seems to be a variant of linear random codes but with keys of reasonable size. It has been standardized at NIST and interfaces with SCADA (Supervisory control and data acquisition) control and supervision systems. The company is a Microsoft Azure partner.



**American Binary or Ambit** (2019, USA) sells PQC solutions to governments, enterprise customers and consumer products companies, including a VPN.



**Anametric** (2017, USA, \$1.9M), formerly bra-ket science, is a startup that wants to create information storage systems in qubits operating at room temperature. It seems they are focused on quantum telecommunication systems.



**Agnostiq** (2018, Canada, \$2.5M) is a startup coming out of the Creative Destruction Lab accelerator in Toronto. They develop workflow management tools to submit and scale jobs on hybrid quantum computers, cloud privacy and quantum obfuscation tools and pre-built applications in the finance sector for portfolio optimization and options pricing.



**Alternatio** (2016, Poland) develops a post-quantum cryptography IP core to be integrated in chipsets for the industry and connected objects.



**ArQit** (2016, UK, \$470M) is developing QuantumCloud, a cloud-distributed symmetric keys mixing keys generation in local agents and key distribution via low earth orbit satellites and QKD. In May 2021, it announced a funding round of \$400M using an IPO through a special purpose acquisition company like IonQ, this time with Centricus Acquisition Corp.

---

<sup>1520</sup> See [AgilePQ DEFEND Cryptographic Tests](#) (11 pages).



# ciena

Although they do not yet have a structured QKD offering, they are very interested in standardizing it. In particular, they are participating in the Quantum Alliance Initiative launched in 2018 in the USA by the Hudson Institute, a conservative think tank, which is working towards this goal and creating proposed standards for QKD and QRNG (quantum random number generation).



## CRYPTO4A

It includes a 19-inch QAOS format appliance server for generating entropy random numbers (without specifying the technology used) and another that generates quantum safe PQC encryption, the QxEdge Hardware Security Module (HSM). The PQC generation module is called QASM (Quantum Assured Security Module), which duplicates the quantum development language of the same name.

It is based on quantum safe hash-based signatures (HBS). These appliances are equipped with four Intel Core i7 chipsets, 16 GB of memory and 256 GB of SSD and run on a hardened version of Linux. They support algorithms certified by the NSA in the USA ("suite B") and future NIST PQC standards.

## CRYPTO EXPERTS

## CRYPTONEXT SECURITY

**BLAKFX** (2017, USA) develop quantum resistant software solutions around their Helix22 SDK that provides five layers of symmetric keys protections for end-user to end-user communications (AES1, TwoFish, AES2, ThreeFish, Snow3G). With sufficiently long keys, symmetric keys are quantum resistant.

**Ciena** (1992, USA) is an equipment manufacturer in the field of optical telecommunications. They integrate IDQ's offers in their solutions, and in particular, their optical random key generators.

**Crypta Labs** (2013, UK, \$300K) develops post-quantum encryption solutions adapted to connected objects. In particular, they propose quantum random number generators that can be integrated into a cell phone (such as IDQ) and also work in space. The QRNG uses a LED or laser light source and a camera sensor. They are working with the University of Bristol.

**Crypto4A Technologies** (2016, Canada) offers an encryption solution based on a random number generation.



**CryptoExperts** (2008, France) develops homomorphic encryption and post-quantum cryptography, and also offers services based on these technologies.

**CryptoNext Security** (2019, France) is a startup that develops a post-quantum cryptography solution. They were founded by Ludovic Perret (CPO, ex Inria) and Jean-Charles Faugères (CTO, ex LIP6 Sorbonne) with Florent Grosmaitre as CEO.

Their software solution is developed in C language and assembler for performance reasons. It combines multivariate polynomials and hashing. Their solution can be integrated into RSA/ECC schemes by hybridization. CryptoNext is also one of the French teams who submitted a PQC proposal to the NIST which has been selected as an alternative candidate in 2020's round 2, GeMSS, which consolidates contributions from CryptoNext, Inria, Orange, University of Versailles and Sorbonne Université.

PQC standardization processors are used in practice by many organizations such as ISO, ITU (X509), IETF (TLS) and ETSI (algorithms). Their PQC should be integrated into R3's CORDA

blockchain solution for banks. Note that China is also organizing a competition with a faster selection schedule than the NIST one. CryptoNext equips French special forces with their PQC, running on secure mobiles using Android.



**Crypto Quantique** (2016, UK, \$8M) is a startup offering a cryptography solution to secure communication with connected objects targeting various markets ranging from automotive to finance. It uses a chipset that is installed in the object. It is a "quantum processor" in silicon technology that is used to generate a unique identification key for the object, which is tamper-proof and tamper-proof. It probably exploits photonics with a random number generator similar to the Swiss IDQ technologies.

Their technology is called Quantum Driven Physically Unclonable Function (QD-PUF) but they do not explain how it works or what encryption model is used<sup>1521</sup>. The founders are of Iranian, Italian and Greek origins, a beautiful patchwork.



**Cyphe** (2014, USA, \$1M) sells PQC solutions. The company was created by Ryan Lester and Joshua Boehm, two engineers from SpaceX. Mars not interesting anymore?



**Dencrypt** (2013, Denmark) is a cybersecurity software provider protecting smartphone communications. They are working on creating PQC based solutions in partnership with the Technical University of Denmark (DTU).



**evolutionQ** (2015, Canada) is a startup that stands out especially for the pedigree of its creator, Michele Mosca, an Italian specialist in post-quantum cryptography.

He is also the founder of the Institute for Quantum Computing at the University of Waterloo in Canada. The company provides what is known as "service equipped" to support companies in the adoption of post-quantum and quantum cryptography. It begins with a six-phase Quantum Risk Assessment product, documented in [A Methodology for Quantum Risk Assessment](#), published in 2017. Is it really a product? It looks more like a methodology to be implemented with consultants. The rest is of the same cream with integration and training services to evolve the company's cryptographic systems.



**Flipscloud** (2013, Taiwan) creates "quantum level" encryption software targeting IoT, cloud services and the big data market. It seems it is using some unspecified PQC and AES 256 bits keys. Software runs on embedded systems using Arm cores and Imagination CPUs.



**fragmentiX** (2018, Austria) offers a secure data storage management system that uses the technique of fragmentation and distribution of data on different physical media. All this is supplied in the form of appliances.

The distributed data is of course encrypted, but in a classical way. This is another way to create data protection that is resistant to Shor's algorithm. It is not the only company positioned in this niche.

---

<sup>1521</sup> See [Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions](#) by Roel Maes and Ingrid Verbauwhede (36 pages) and [Quantum readout of Physical Unclonable Functions](#) by B. Skoric (21 pages).

They combined their appliances with QKD equipment from IDQ and Toshiba that was available at AIT. The theoretical proposal comes from researchers of TU Darmstadt in Germany and it has already been implemented a couple of years ago in Tokyo.

GO QUANTUM



**GoQuantum** (2018, Chile) is willing to provide “*a post-quantum secure data transmission solutions through quantum-based hardware and radio link layer encryption.*”. Translation: it’s using PQC encryption algorithms with a photonic based QRNG for key generation.

**HaQien** (2019, India) designs post-quantum cryptography (PQC) solutions. But it is not quite clear because they also seem to use a random number generator to create classical keys.

**Hub Security** (2017, Israel, \$55M) sells quantum secure FPGA based Hardware Security Module (HSM). These HSM modules contain QRNGs and support quantum-resistant algorithms acceleration in hardware (PQC).

**IDQ (ID Quantique)** (2001, Switzerland, \$74.6M, acquired by SK Telecom in 2018 for \$65M) is one of the oldest companies in the sector, created by Swiss researcher Nicolas Gisin, a specialist in photonics and quantum entanglement.

The company offers a complete range of random number generators and QKD management systems as well as a high-efficiency (>95%) superconducting nanowire single photon detector (SNSPDs). Its Quantis random number generator, already described at the beginning of this section, is complemented by Cerberis, a QKD solution to protect the circulation of encryption keys in a 6U rack and Centauris, a range of encryption servers supporting 100 GBits/s optical links. This FPGA-based server currently supports elliptic curve-based systems as well as AES-256, pending the standardization of PQC (post-quantum-crypto) protocols.

Since the beginning of 2018, the company belongs to the Korean group SKT Invest which is the Corporate Venture branch of **SK Telecom**. The fund invested \$65M in what was modestly [presented as a partnership](#) while it's actually a full takeover.

IDQ's QKD offer is notably deployed in Korea to protect the 5G backbone of the operator SK Telecom. They are also partnering with Toshiba in Cambridge and in the OpenQKD project.



KEEQUANT

**Keequant** (2017, Germany, \$1.7M), formerly InfiniQuant, is a spin-off from the Max Planck Institute for the Science of Light. They are developing a CV-QKD for use over fiber optics and satellite links.

This technique uses amplitude modulation in addition to phase modulation to transmit quantum keys. The startup is also working on a quantum random number generator.



**Infotechs** (1991, Russia) is a cybersecurity specialist historically specialized in VPN creation. It has developed a PQC solution in 2016, with an awkward communication that could make it look like QKD<sup>1522</sup>.

But they develop many QKD solutions. In 2018, they launched their "ViPNet Quantum Phone", using their ViPNet VPN (ViPNet Client and ViPNet Connect) and a hardware QKD solution developed at Moscow University. What they call a "phone" is in fact a PC with an external box with a fiber optic link connecting it to a QKD key server<sup>1523</sup>.



**ISARA** (2015, Canada, \$27M) develops post-quantum encryption software solutions and PQC implementation consulting with "ISARA Radiate Security Solution Suite" which provides public keys and encryption algorithms.

They are visibly based on hash trees and combine PQC (post-quantum crypto) and traditional PKI (public-key infrastructure)<sup>1524</sup>. One of their investors is the [Quantum Valley Investments fund](#), managed by Mike Lazaridis, co-founder of BlackBerry RIM. He reinvested his BlackBerry-related fortune in the development of the Canadian scientific and entrepreneurial ecosystem, particularly in quantum, where he has invested a total of \$450M ([source](#)).



**KETS Quantum Security** (2016, UK, £5.1M) develops a quantum random number generator (QRNG) and a QKD quantum key generator, all integrated in a single component miniaturized photonic and packaged in PCI cards.

All this is combined with a consulting activity for the deployment of the solutions. The company was founded by photonics researchers from the University of Bristol. They target the financial and public sector markets. They are prototyping UAVs with Airbus for QKD implementation in military or public security applications, with Airbus Defense. Their QKD chipset can also equip Cubesat-type micro-satellites.

**Knot Communications / Artedys** (France) wants to launch a network of satellites to operate some sort of quantum blockchain satellite phone. They plan to launch a satellite between 2024 and 2027. This looks a little farfetched.



**MagiQ** (1999, USA, \$7.5M) is a startup that initially started in 2003 with the creation of a QKD system. For about ten years, this company seems to have repositioned itself in the US service and defense industry. They have developed the Agile Interference Mitigation System (AIMS), a system for reducing electromagnetic communication interference.



**MtPellerin** (2018, Switzerland) is a startup specialized in the management of crypto-assets via a dedicated mobile application ("Bridge Wallet"). They have created a quantum safe with IDQ, "The Quantum Vault", which is based on IDQ's random number generator and QKD system.

<sup>1522</sup> See [Infotechs At The Forefront Of Quantum Cryptography](#), 2017.

<sup>1523</sup> See [Infotechs has presented its ViPNet Quantum Phone](#), January 2018.

<sup>1524</sup> This is documented in the white paper [Enabling Quantum-Safe Migration with Crypto-Agile Certificates](#), 2018 (7 pages).



**NuCrypt** (2003, USA) develops optical technologies for quantum communications and metrology, including entangled photon sources, optical pulse generators, single photon detectors, polarization analyzers and associated software.



**Nu Quantum** (2018, UK, £4.3M) is a spin-off from the University of Cambridge developing QKD optical links and satellite systems using proprietary single-photon components. They also created their own source of single photons and have some ambition to create a photon-based quantum computer of their own. The startup is co-founded and directed by Carmen Palacios-Berraquero.



**Origone** (2014, UK) develops cryptography solutions based on D-Wave computers. It targets in particular the defense market as well as the railway industry. Their quantitative/post-quantum cryptography activity is an evolution of a traditional cybersecurity business.



**Post-Quantum** or **PQ Solutions** (2009, UK, \$10.4M) is a startup initially created under the name SRD Wireless that created the secure PQ Chat messaging using the random linear codes invented by Robert McEliece.

The company was renamed as Post-Quantum or PQ Solutions Limited in 2014. They offer a line of security products integrating post-quantum crypto algorithms. One of the co-founders, Martin Tomlinson, has developed the Tomlinson-Harashima pre-encoding, which corrects interference in telecommunication signals and various error correction codes. Their products also include PQ Guard, a post-quantum encryption system.



**PQSecure Technologies** (2017, USA) is a provider of isogeny-based PQC solutions. It is a spin-off from the University of Florida Atlantic launched by Reza Azarderakhsh. Their SIKE algorithm is a finalist in the NIST PQC call for proposals.



**PQShield** (2018, UK, \$6.9M) is Oxford University spin-off that develops PQC solutions. They collaborate with finalist teams in the PQC solutions competition launched by NIST. They have developed a licensed SoC (system on chip) that integrates their in-house Euclidian networks based PQC. Bosch is one of their first customers.



**Qaisec** (2019, Bulgaria) develops cryptographic solutions targeting the AI, finance and telecommunications sectors. They seem to offer first a security audit service and then cryptography solutions that use quantum random number generators for keys. They are also creating a PQC-based blockchain.



**QEYnet** (2016, Canada, \$7M) is developing a QKD quantum cryptography satellite network. Funding for the startup comes from the Canadian government.



**QuantLR** (2018, Israel) is a developer of an affordable QKD software solution that is supposed to reduce the cost of QKD deployment by 90% with “*no specific hardware*”.

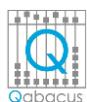
The startup was cofounded by Hagai Eisenberg, a professor at Hebrew University of Jerusalem. When looking at a recent paper he coauthored<sup>1525</sup>, you get an idea of what they may be doing.

It consists in using an high-dimensional QKD architecture that can work on existing binary QKD hardware on distances of up to 40 km, thanks to using some time-bin encoding programmed on a FPGA component. They also partner with a telecom equipment manufacturer, **PacketLight Networks** (2000, \$18M), also based in Israel, which provides optical fiber WDM (wavelength-division multiplexing) equipment.



**QuantumCTek** (2009, China) is a provider of end-to-end quantum cryptography solutions: QKD, QKD repeaters, optical routers. The company is a spin-off of Hefei National Laboratory for Physical Science at Micro-scale (HFNL) and the University of Science and Technology of China (USTC).

They are behind the creation in 2014 of the "Quantum-Safe Security Working Group" with ID Quantique and Battelle, which promotes PQC. As we saw above, they have deployed the 2000 km QKD-protected link between Shanghai and Beijing. They ran an IPO (Initial Public Offering) in China in July 2020.



**Qabacus** (2019, USA) is developing quantum computing and cryptography technologies and a complete cyber-security software stack.



**Qasky** (2016, China) commercializes research coming out of the Chinese Academy of Sciences. Funding comes from Wuhu Construction and Investment Ltd and the China University of Science and Technology.

They offer solutions for post-quantum crypto, QKD and photonics components. Their name is derived from CAS Key laboratory, CAS = China Academy of Sciences.



**QRATE Quantum Communications** (2015, Russia) sells QRATE Key Distributor, a BB84 protocol-based QKD quantum key distribution solution in a 4U rack with a range of up to 100 km.

They also market a single-photon avalanche diode detector (SPAD) operating at 1550 nm and a quantum random number generator (QRNG).



**QuantiCor Security** (2017, Germany) develops PQC solutions, particularly for Blockchain applications and connected objects, via offerings with Quantum-Multisign and Quantum IDEncrypt.

That they are supposed to be cheaper than traditional PKIs. They come from TU Darmstadt and target the healthcare market in particular.



**Quantum Blockchains** (2018, Poland) wants to create a quantum resilient blockchain based on QKD. That's an interesting long-term bet given the infrastructure required to make it happen at a large scale.

**QuDoor** (2016, China, \$7,8M) aka **Qike Quantum**, aka **Quantum Door**, aka **Guokai Quantum Technology** designs various products for QKD distribution, a trapped ion quantum processor supposed to reach someday 100 qubits (Tiansuan 1) and a laser-based vibration quantum sensor.

<sup>1525</sup> See [Fast and Simple One-Way High-Dimensional Quantum Key Distribution](#) by Kfir Sulimany, Hagai Eisenberg, Michael Ben-Or et al, May 2021 (7 pages).

QuDoor's cofounder and R&D track record include a commercial QKD system (2003), a waveform generator (2007), ion trapping (2012), quantum computing sensing (2015) and ion-phonon-photon entanglement function (2018).

## QUANTUM IMPENETRABLE



**Quantum Impenetrable** (2018, UK) is a Scottish startup that develops a security module (HSM) using a quantum random number generator and resistant to quantum key-breaking algorithms.

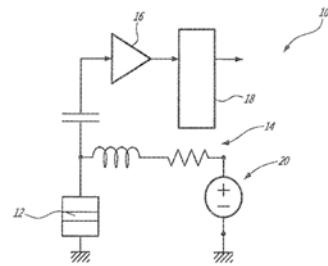
**Quantum Xchange** (2016, USA, \$23.5M) distributes Phio Trusted Xchange, a key distribution system supporting both PQC and QKD.

They partner with the telecom infrastructure operator Zayo Group, from which they operate their dark fibers and use ID Quantique's QKD solutions. They began by deploying a 1,000-kilometer QKD network from Boston to Washington via New York and New Jersey<sup>1526</sup>. Since 2021, they also partner with **Cisco** for the support of the Cisco Secure Key Integration Protocol implemented in enterprise routers, for the non-quantum part of their hybrid key distribution architecture.



**Quantum eMotion** (2007, Canada), formerly Quantum Numbers Corp, develops a cryptographic system based on a quantum random number generator and targets in particular mobile uses. It mainly communicates on the filing of an associated patent.

Let's hope it won't be a patent troller! The company seems to be licensing its technology to electronic component designers. It exploits research work from the Department of Physics at the University of Sherbrooke in Quebec. One of the patents relates to the generation of random numbers based on the random noise generated by some electron tunneling effect through a potential barrier<sup>1527</sup>. The QRNG speed reaches 1 Gbits/s and fits in USB key form factor. The company is listed on the Canadian Venture Exchange (CVE).



**Quantum Trilogy** (2016, USA) created a secure communications solution based on applications (including for mail and voice communication) protected by an unspecified encryption, a QRNG to create real entropy in generated keys and servers that are protected at some level by a QKD.



**QuBalt** (2015, Germany) is a startup established between Germany and Latvia that develops solutions for post-quantum cryptography (PQC) and quantum algorithms.



**Qubit Reset** (2018, USA) develops quantum repeaters for QKD arrays. The company was founded by two Argentinians based in Miami. It is not listed in the Crunchbase and does not seem to have raised any funds, which seems to be a bad omen.

<sup>1526</sup> See [Quantum Xchange Breaks Final Barriers to Make Quantum Key Distribution \(QKD\) Commercially Viable with the Launch of Phio TX](#), September 2019.

<sup>1527</sup> I found the complete PDF of USPTO patent 10437559 on <https://www.pat2pdf.org/>.



**Quintessence  
Labs**

**Quintessence Labs** (2006, Australia, \$49.3M) proposes a quantum random number generator and a QKD system. They use the CV-QKD technique which allows the use of existing fiber optic infrastructures of very high-speed telecom operators.



**Qunnect**

**Qunnect** (2017, USA, \$2.3M) is a spin-off from Stony Brook University of Long Island that offers components to upgrade existing telecom facilities with QKD and PQC, including photon sources, including a quantum memory operating at room temperature that can be used to set up quantum repeaters.



The Quantonation fund is one of the investors in this startup led by Mehdi Namazi, Eden Figueroa, Noel Goddard and Mael Flament<sup>1528</sup>.

**Q → N U**

**QNu Labs** (2016, India, \$5.3M) develops QKD-based solutions. They also offer their own quantum random number generator and are also working on the creation of a QKD solution operating on Li-Fi, W-Fi that uses the frequencies of visible light.

**QuSecure**

**QuSecure** (2019, USA, \$1.7M) develops a secure blockchain solution that is resilient to quantum code breaking. It seems that they are also developing a Blockchain that would be secured via QKD, and Blockchain security testing protocols. The startup is also doing cybersecurity consulting and, in particular, audits for the deployment of PQC. It was founded by Rebecca Krauthamer, who also founded the **Quantum Thought** startup mentioned above.

**ravel**

**Ravel Technologies** (2018, France) offers Ravel Homomorphic Encryption, a post-quantum and homomorphic encryption solution. The company was founded by Mehdi Sabeg.

**SECURE-IC**  
THE SECURITY SCIENCE COMPANY

**Secure-IC** (2010, France) is the leader of the RISQ project, which aims to create a French post-quantum crypto solution.

The company develops security hardware and software solutions that are used to evaluate the robustness of security solutions. The company is a spin-off from the Institut Mines-Télécom.



**SeQURENET** (2008-2017, France) was a spin-off of Telecom ParisTech specialized in the distribution of long distance CV-QKDs ([source](#)).

It had been funded within the framework of the European research project SECOQC (secure communication based on quantum cryptography). The startup was based on work done by Philippe Grangier's team at the Institute of Optics and the Thales TRT laboratory in Palaiseau. The company closed down in 2017! It had been launched a little too early compared to the maturity of the market.



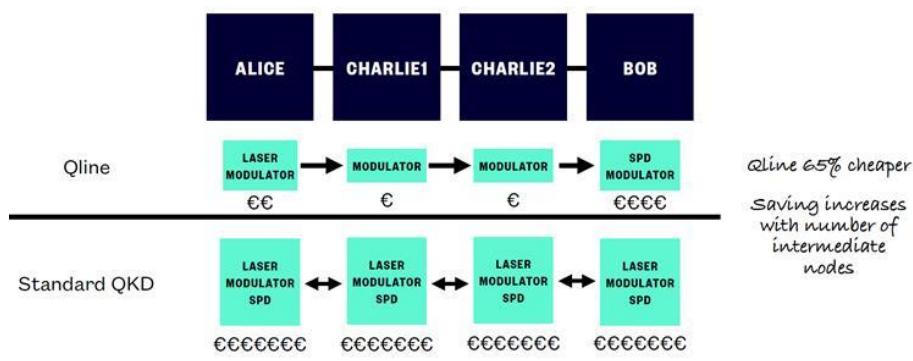
**Smarts Quanttelecom** (1991, Russia) proposes a quantum cryptography solution based on CV-QKD which exploits standard fibers of telecom operators.

<sup>1528</sup> They received \$1.5 million of funding in April 2020 from the US Department of Energy under the Small Business Innovation Research Awards (SBIR) program. See [Qunnect receives \\$1.5M award from the DoE - Swiss Quantum Hub](#), April 2020. This will allow them to test their equipment with specialized telecommunication operators and in New York City.

Smarts was until 2015 a Russian mobile telecom operator. It has since become a telecom services operator with an offer of secure telecom links and data center and cloud services. Their QKD solution comes from Quanttelecom, a subsidiary of Smarts, developed jointly with the ITMO University of Saint Petersburg.



Their offer is based on the Qline, a software solution that enables the deployment of a multi-point quantum network with a lower cost in hardware infrastructure. With this architecture, nodes that are very expensive can be replaced by simple modulators that are much more affordable. The operation is based on a kind of "time-sharing" of the line. This lowers the hardware addition by about two thirds on a typical installation below with two intermediate stations in the network. At both ends of the line there is on one side a laser and modulator-based photon generator and on the other side a single photon detector, the most expensive part of the equipment ranging from 20K€ to 100K€. The solution is deployable on networks totaling 100 to 200 km.



The first application is QKD quantum key distribution. They can interoperate with classical QKD networks. Initially, secure file transfer and instant messaging are targeted as applications associated with QKD. The system can also be used to gener-

ate disposable masks<sup>1529</sup>.



**XT Quantech** (2017, China) specializes in CV-QKD distribution equipment after initially focusing on DV-QKD solutions. The CV-QKD is essential because it can coexist in the fiber links of telecom operators.

They offer server appliances for QKD key encoding and decoding gateways. Its full name is Shanghai Xuntai Information Technology Co.



**ZY4** (2014, Canada) develops post-quantum cryptography solutions based on their in-house concept of the Shannon Event Horizon which would be a new class of PKI and random number generation<sup>1530</sup>.

### Quantum telecommunications and cryptography key takeaways

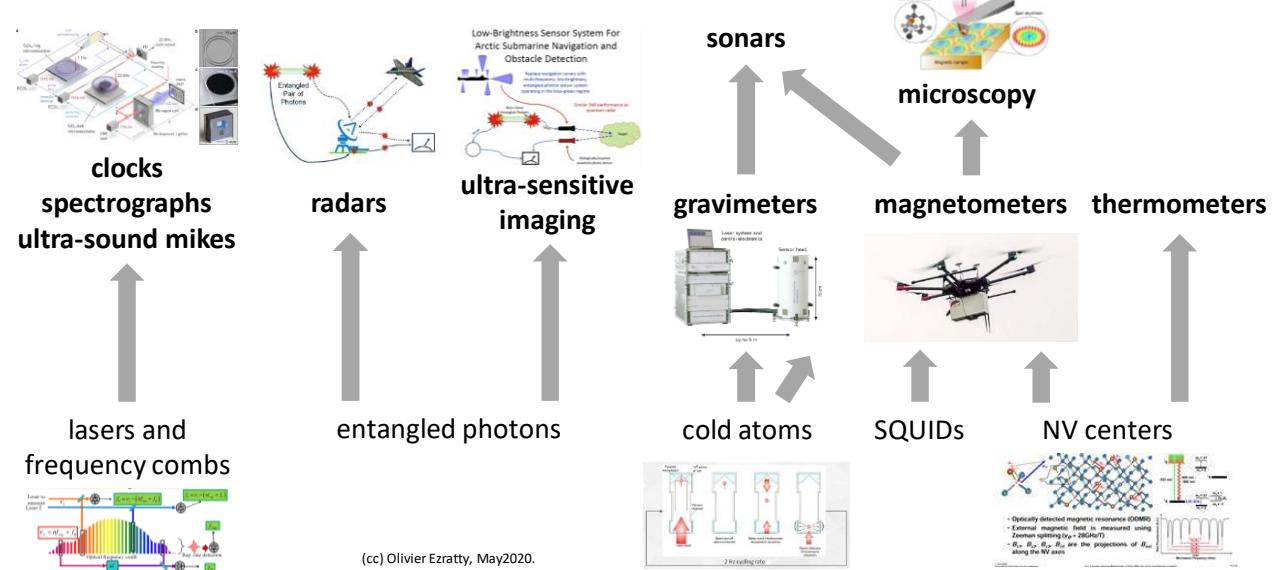
- Quantum computing poses a theoretical threat to many existing cryptography systems, particularly those using public key distribution. This is due to Peter Shor's algorithm. But other algorithm are creating various threats, including for symmetric key distributions.
- As a result, two breeds of solutions have been elaborated. The first one is based on quantum key distribution, requiring a photonic transmission channel (airborne or fiber based), and using most of the time quantum entanglement.
- The second option is to create cryptographic protocols that are not breakable by quantum computers. The USA NIST has launched in 2016 an international competition to standardize a set of post-quantum cryptography (PQC) protocols. The process should end by 2023. Solutions deployments should happen next and be done way before the quantum computing menace will materialize, if it does.
- Quantum random numbers generation is/will be used for classical cryptography. It provides sources of both random and non-deterministic numbers used in cryptography systems. It has other used cases when randomness is mandatory like with lotteries and simulation tools.
- Quantum telecommunications can also use quantum entanglement to enable communications between quantum computers and/or quantum sensors. Distributed quantum computing has two potential benefits: scale quantum computing beyond the capacity of individual quantum computers and enable safe communications between quantum computers.
- Quantum Physical Unclonable Functions are cryptographic solutions used to authenticate physical objects in an unfalsifiable quantum way. It is however still an unmature technology.
- There are already many startups in the QKD and PQC scene. Deployments have already started worldwide, particularly in China.

<sup>1529</sup> See [How to build quantum communication networks at a small scale](#) by Marc Kaplan from VeriQloud, May 2020.

<sup>1530</sup> See their white paper [Introducing the Shannon Event Horizon](#), 2019 (20 pages).

# Quantum sensing

Quantum sensing is about the various precision measurement solutions that rely on second generation quantum technologies and go beyond the limits of classical measurements systems. It also often allows non-invasive measurements to be carried out on various solid or organic materials. The main physical values measured are time, distances, gravity, magnetism, temperature and electromagnetic spectrum analysis. Many applications use these technologies like radars, sonars, very high sensitivity microphones or the field of imaging in general and in medical imaging in particular.

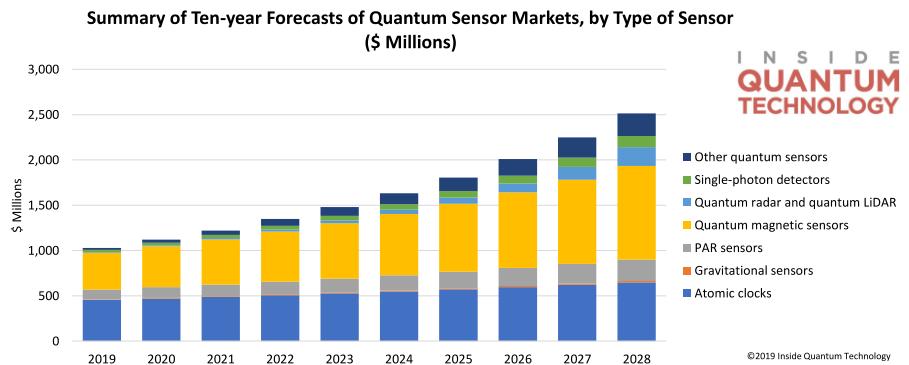


Some of these technologies have commonalities with the various qubits types we have already explored in detail. This is particularly the case for cold atoms, NV centers and superconducting qubits. Precision magnetometers use NV centers as well as SQUIDs (Superconducting Quantum Interference Device), which also measure the direction of current in superconducting flux-type qubits and are used in particular by D-Wave in quantum annealers.

Many of these quantum measurement technologies make extensive use of photonic tools, either directly based on photons (lasers, frequency combs, entangled photons) or exploiting cold atoms and even NV centers, whose state is then evaluated by measuring their fluorescence.

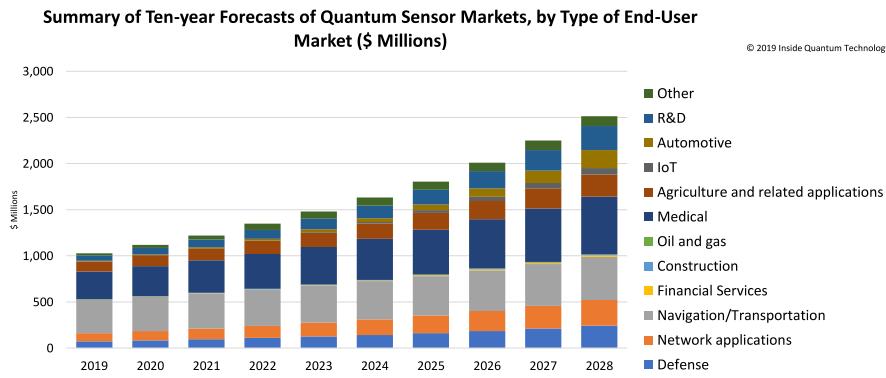
Many of these technologies are already commercially viable and continue to progress steadily.

It is still a niche market made of many sub-niche markets, evaluated at around \$1B and expected to double in a decade<sup>1531</sup>.



<sup>1531</sup> Data source: [Quantum Sensors: Ten Year Market Projections](#) by Lawrence Gasman, 2019 (7 slides).

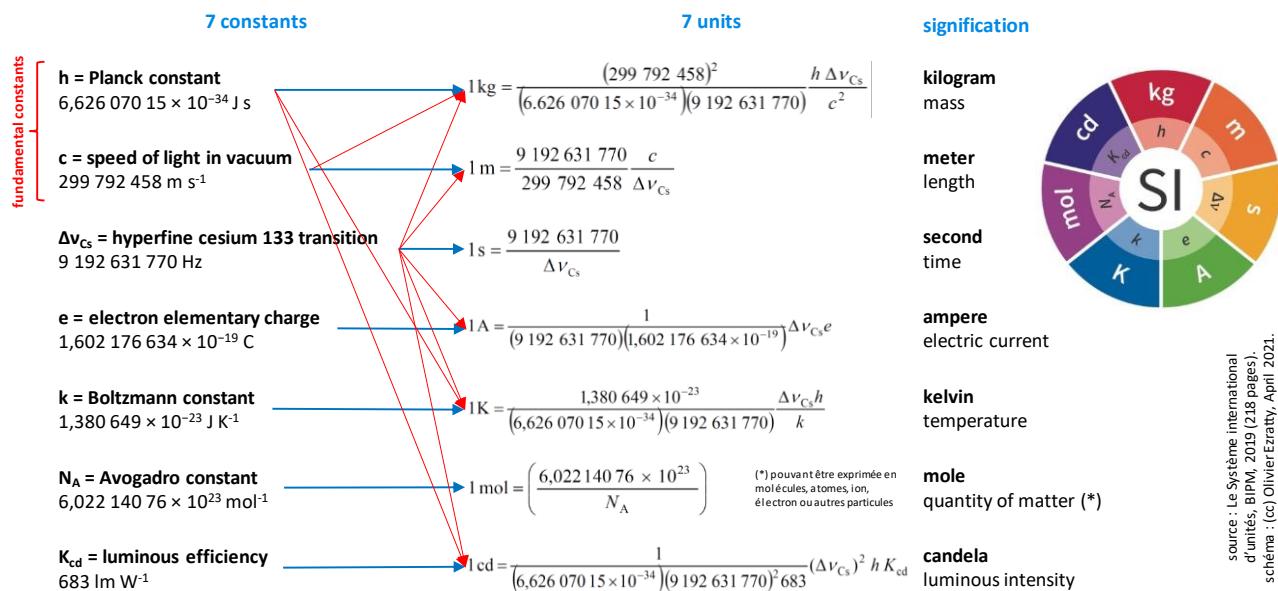
The two largest applications markets are transportation and medical imaging. But these forecasts may become wrong since some use cases might at some point become mainstream and drive more market growth. This is the case of GPS without satellite links using micro-magnetometers.



It could someday equip all autonomous vehicles!

Sensing cannot be discussed without being connected to the **International System for Measurement** (or International System of Units, aka SI). It was recast after a unanimous vote on the Versailles Metre Treaty signed at the 26th General Conference on Weights and Measures (CGPM) in November 2018<sup>1532</sup>. Its implementation started on May 20, 2019.

The new 2019 SI updates the definition of the kilogram, ampere, kelvin and mole. It is built around seven fixed constants: a number of hyperfine transitions of cesium 133, the speed of light in vacuum<sup>1533</sup>, the Planck constant, the elementary charge of an electron, the Boltzmann constant, the Avogadro number or constant and the luminous efficiency. From these constants are derived the seven basic units of the system: kilogram, meter, second<sup>1534</sup>, ampere, kelvin, mole and candela. It no longer relies on materials that are degrading over time, such as the standard kilogram kept at the BIPM in Saint-Cloud, or on the triple point of water (gel) which defined the kelvin, and which depended on its isotopic composition.

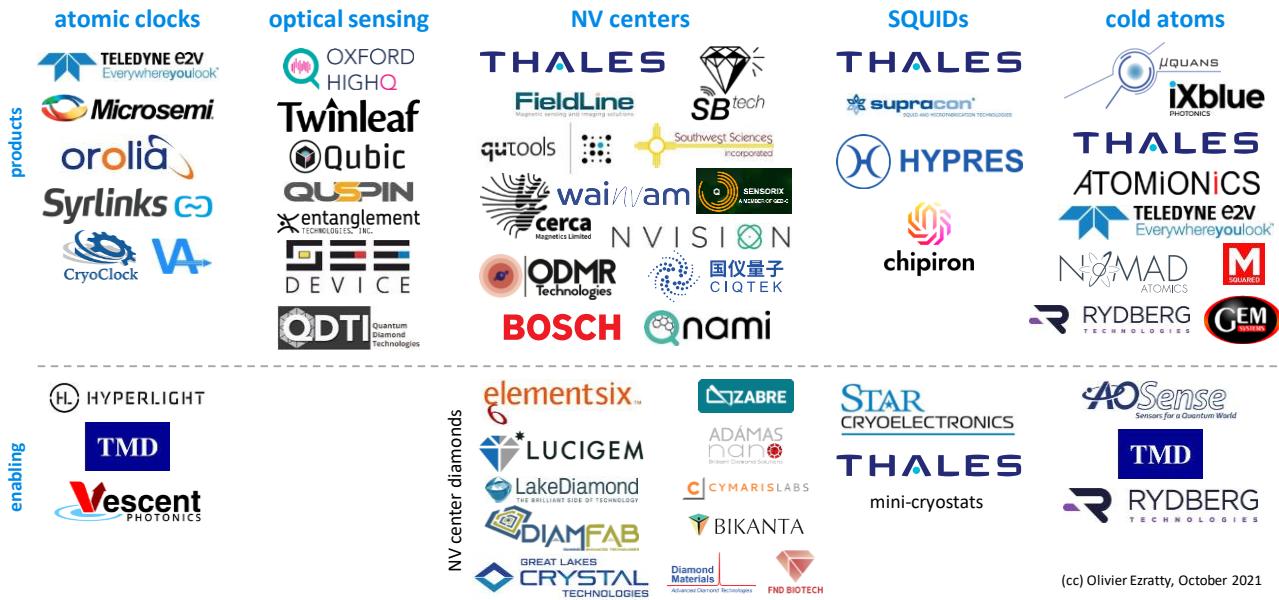


<sup>1532</sup> See [The International System of Units \(SI\)](#), NIST, 2019 (13 pages) and [The International System of Units](#), BIPM, 2019 (218 pages).

<sup>1533</sup> The definition of the speed of light at 299 792 458 m s<sup>-1</sup> dates from 1983.

<sup>1534</sup> The second was defined from the hyperfine transition frequency of cesium 133 since the 13th CGPM of 1967. Previously, it was a fraction of the solar day, which was not stable.

The mole was previously defined on the basis of 0.012 kg of  $^{12}\text{C}$ <sup>1535</sup>. The standard meter, which is kept in the Archives in Paris, was no longer the reference since 1960. All other units of measurement such as hertz, joule, coulomb, lumen or watt are derived from constants and base units. This measurement system is branded as being "quantum" because it is based on the measurement of fundamental phenomena that bring us back to quanta, in particular for the definition of the second, which uses quantized energy transitions in the cesium atom, and that of the kilogram, which uses the Planck constant, itself a foundation of quantum physics. Numerous quantum physics works related to these evolutions of the international measurement system, notably at NIST, have a link with the commercial devices discussed in this section.



(cc) Olivier Ezratty, October 2021

## Quantum gravimeters

Quantum gravimeters measure gravity with a very high accuracy. These are useful in many scenarios: in seismic detectors, for the measurement and definition of the reference kilogram, for precision autonomous navigation complementing GPS in airplanes, ships, submarines and drones, for gravity field mapping, for detecting subterranean holes before undergoing constructions, for detecting groundwater, for oil and mineral exploration and for the detection of gravitational waves in astronomy.

The measurement of gravity is generally performed with cold atom interferometers, taking advantage of the wave-particle duality that also applies to atoms. The technique has been developed since 1991 and perfected since then<sup>1536</sup>. In France, ONERA and LNE-SYRTE have been pioneers in the field, launching experiments in 2009 (GIRAFE project) and in 2014-2016 (GIRAFE2)<sup>1537</sup>.

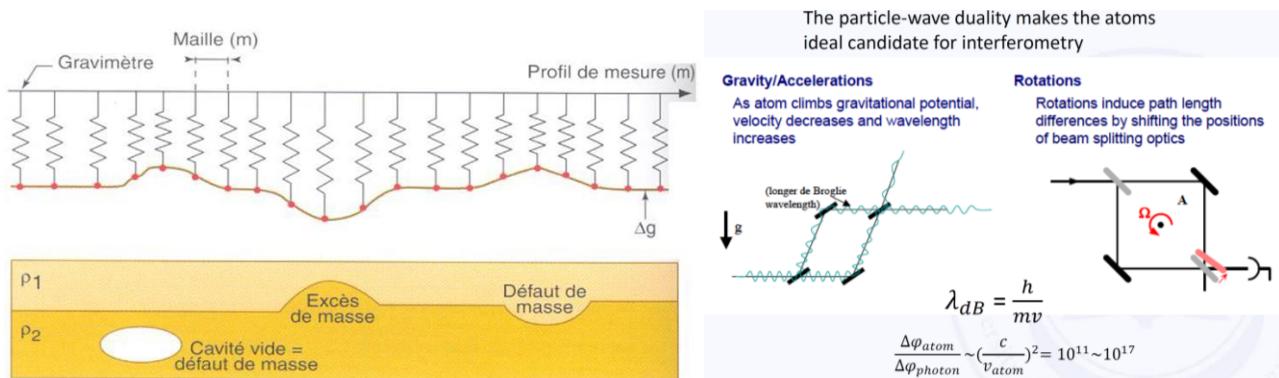
<sup>1535</sup> With the new SI, one gram of matter contains  $N_A$  multiplied by the number of nucleons (protons and neutrons) of the element in question (atom, molecule). This comes from the fact that in an atom, the majority of the weight is in the nucleus. Electrons have a mass equivalent to 1/1836 times that of a nucleon.

<sup>1536</sup> See [Young double-slit experiment with atoms: A simple atom interferometer](#), from O. Carnal, J. Mlynek, 1991 (6 pages) which describes a Young's double-slit interferometry experiment with helium atoms. See also [Experimental gravitation and geophysics with matter wave sensors](#), LP2N, 2018 (234 slides).

<sup>1537</sup> See ["Embedded" applications of atomic gravimetry](#) by N. Zahzam et al, April 2019 (24 slides) and [ONERA invents with SHOM the "atomic" precision gravity mapping](#), February 2016. SHOM is the Hydrographic and Oceanographic Service of the French Navy.

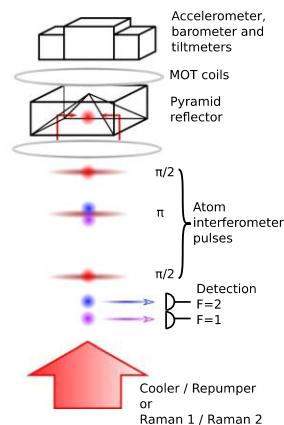
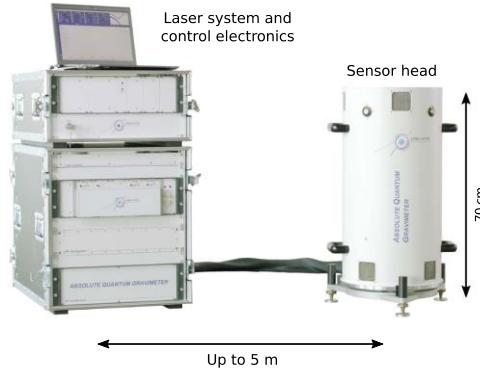
The principle consists in creating a source of cold atoms in suspension, generally rubidium, preparing their state with lasers, then passing them through an interferometer and then analyzing the results. This can be used to measure gravity, but also magnetism, temperature, acceleration and rotation<sup>1538</sup>.

The technique has been perfected and made transportable by the **Muquans** (2011, France, part of iXblue since 2021), based at the Institut d'Optique in Bordeaux. They use joint research work done with the CNRS.



Their quantum gravimeter targets, for example, the detection of cavities in construction, oil exploration and the monitoring of volcanoes such as Etna in Italy<sup>1539</sup>.

The product is called "Absolute Quantum Gravimeter"<sup>1540</sup>. They use a small cloud of about 100 rubidium atoms cooled to  $1\mu\text{K}$  by lasers in 6 directions and magnetically trapped in a vacuum. These atoms are stimulated by Raman transitions based on double photons with different durations and polarizations ( $\pi/2, -\pi, -\pi/2$ )<sup>1541</sup>.



<sup>1538</sup> Schema source: [Compact and Portable Atom Gravimeter](#) by Shuai Chen, University of Science and Technology of China, June 2019 (22 slides). Cold atoms sensing using atoms-light interactions is mostly based on spontaneous/stimulated photon emissions with atoms state detection with fluorescence, and atoms preparation using optical pumping with circularly polarized photons aligning electron spins for atoms preparation and laser cooling using Doppler and Raman effects.

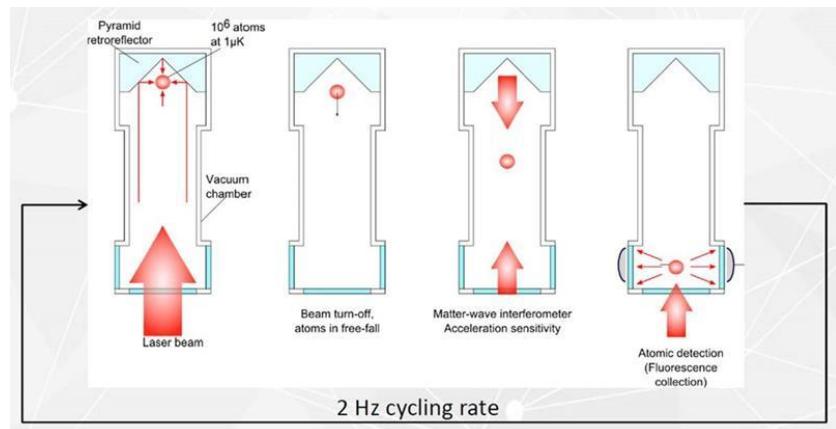
<sup>1539</sup> The Muquans startup employed 29 people in May 2019 and made €2.9M in 2018. They are developing a quantum gravimeter that is used for example to detect cavities for the construction industry, oil exploration and monitoring of volcanoes such as Etna in Italy. The product is called Absolute Quantum Gravimeter. The system uses cold atoms (rubidium) illuminated and cooled to  $1\mu\text{K}$  by laser in 6 directions and magnetically trapped in a vacuum. The system measures the gravitational fall of the atom cloud with high accuracy. A fluorescence and laser-based system measures the velocity of the fall and does so over time to evaluate its temporal variation. They are participating in projects of the European Quantum Internet Alliance flagship to create hardware to extend the reach of QKD and Pasquans systems in cold atom quantum simulation. The company was created in 2011.

<sup>1540</sup> The Muquans process is documented in [Gravity measurements below  \$10^{-9}\text{g}\$  with a transportable absolute quantum gravimeter](#), 2018 (12 pages) and highlighted in [Digging Into Quantum Sensors](#) by Stewart Wills in Optics & Photonics, September 2019.

<sup>1541</sup> Double-photon Raman cooling uses two lasers. One excites the atoms to reach a high excited state and the other de-excites the atom to bring it down to a higher excited state than the initial state. This technique allows to lower the temperature below a micro-Kelvin.

The system then measures the gravitational fall of the atom cloud which is different depending on the atoms preparation.

A fluorescence-based system and diodes measure the fall speed and does it in time to evaluate its time variation. The diodes measure the proportion of atoms in each interferometer output.



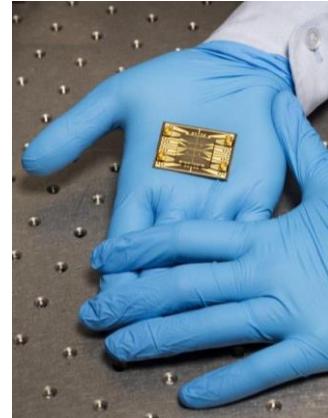
The source of the atoms also contains an accelerometer that corrects the phase of the lasers in real time.

The control of cold atoms has other applications<sup>1542</sup>. For example, Muquans participates in the European flagship project **Quantum Internet Alliance** to create hardware to extend the reach of QKD systems and with the French startup **Pasqal** which creates quantum processors based on cold atoms.

Other companies are also positioned in this market:



**Thales** Research & Technology (France) is developing miniaturized cold atom accelerometer, gyrometer and clock designed to be embedded. The whole with a "BEC on chip" component (for "Bose Einstein condensates on chip") in collaboration with the Charles Fabry laboratory of the Institut d'Optique (LCFIO). Atoms are vaporized in a glass cage glued to the chip, in which a good vacuum has been created. They are laser-cooled and trapped by a magnetic field and controlled by electromagnetic fields. This research project started around 2014.



*Photo credit: Ecliptique - Laurent Thion.*



**Atomionics** (2018, Singapore, \$2.5M) is developing Gravio, a cold atoms interferometry based sensor measuring acceleration, rotations and gravity variations.

It can be used for navigation and resource exploration. It can also be used as an underground GPS.

Other laboratories are working on the same technology, such as the **Leibniz University** of Hannover<sup>1543</sup>. **Aquark Technologies** (2020, UK) is a spin-off from the University of Southampton which is in the same niche as Muquans. **AtomSensors** (2015, Italy) is a spin-off of the University of Florence which also develops cold atoms-based quantum sensors, including gravimeters. They also provide laser sources for spectroscopy and laser cooling of atoms. The Chinese are also in this field, but without having gone so far in miniaturization<sup>1544</sup>.

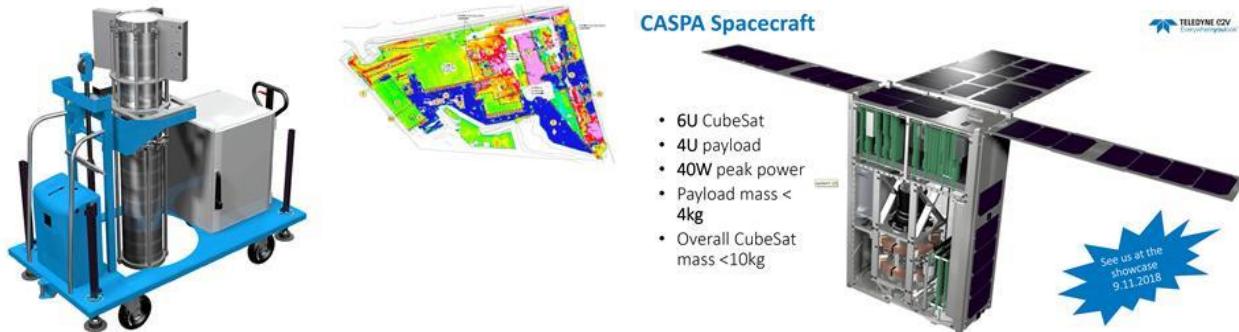
<sup>1542</sup> See [Fifteen years of cold matter on the atom chip promise, realizations, and prospects](#) by Mark Keil et al, 2019 (46 pages) which makes a good inventory of scientific applications of cold atoms.

<sup>1543</sup> See [Gravity measured using a Bose-Einstein condensate on a chip](#) by Hamish Johnston, 2016 mentioning the work of Ernst Rasel of the Leibniz University of Hannover who refers to [Atom interferometry and its applications](#) by S. Abend et al, 2020 (48 pages). See also [Fifteen years of cold matter on the atom chip: promise, realizations, and prospects](#) by Mark Keil et al, 2019 (46 pages).

<sup>1544</sup> See [Compact and Portable Atom Gravimeter](#) by Shuai Chen, 2019 (22 slides).

**Teledyne e2v** (UK, a subsidiary of Teledyne US) maintains infrastructures with the detection of underground obstacles or cavities before construction works, and also do geothermal energy and groundwater reserves searches.

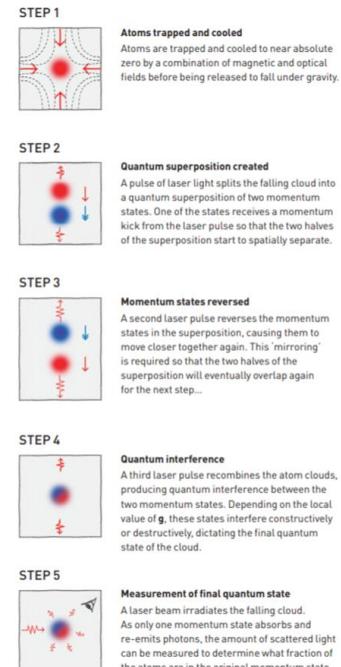
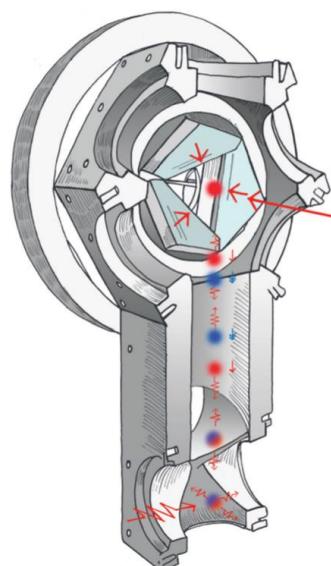
They are also involved in the creation of **CASPA** (Cold Atom Space PAyload), a small satellite weighing 14 kg and containing 6 CubeSat in a volume of 30x20 x10cm, including a cold atom gravimeter, which would be the first to operate in space. It was to be launched by ESA in 2020.



**M Squared** (2006, UK, \$56M) created a cold atom quantum gravimeter using a process similar to Muquans<sup>1545</sup>, in partnership with the University of Birmingham and Imperial College London (UCL).

The project was funded under the UK government's Quantum Initiative launched in 2013. The original business of the Scotland startup is their range of SolsTiS lasers covering the spectrum from 200 nm to 4000 nm. These lasers are used in industry and in optical clocks.

#### HOW THE QUANTUM GRAVIMETER WORKS



**Nomad Atomics** (2018, Australia) develops compact cold atom-based quantum gravimeters and accelerometers. The company was launched by Kyle Hardman, Christian Freier and Paul Wigley, respectively researcher and post-docs at the Australian National University.



**iXblue Photonics** (2000, France) is the photonics branch of iXblue, which specializes in the design and manufacture of inertial and sonar power plants, with 700 employees.

<sup>1545</sup> Illustration source: [M Squared quantum gravimetry](#) (4 pages).

It is specialized in the creation of lithium niobate optical modulators, microwave amplifiers and modulator bias controllers for the control of Mach-Zehnder interferometers. Their components are manufactured at their site in Lannion, Brittany. They are in particular involved with the LP2N of Bordeaux in the creation of iXatom, a quantum inertial sensor based on cold rubidium atoms<sup>1546</sup>. iXblue Photonics is the result of the acquisition of two companies: iXFiber in 2011, a specialist in passive optical components (FBG fiber grating filters, Fiber Bragg Gratings). Then Photline Technologies in 2013, a spin-off of the Femto-ST laboratory created in 2000 in Besançon. In May 2021, iXblue acquired **Muquans** and **Kylia** (a photonic equipment specialist, with its polarizers, delay line interferometers and multiplexers/multiplexers).



**AOSense** (2004, USA) creates quantum gyroscopes, a quantum gravimeter and commercial optical clocks. It also provides instrumentation equipment with cold atom generators and laser frequency comb generators

They collaborate with IonQ for their quantum computers based on trapped ions.



**Innoseis** (2020, Netherlands) was created by Mark Beker and Johannes van den Brand (who worked on gravitational waves detections instruments like those from LIGO), from Maastricht University. They develop MEMS based quantum gravimeters targeting seismic surveying.

**Microg LaCoste** (1939, USA) develops absolute quantum gravimeters based on interferometry and free fall dropped mirrors, using a rubidium based atomic clock.

Finally, let's also mention a very special category of microgravimeters: the LIGO microgravimeters that are used to evaluate gravitational waves. They are based on optical interferometers of very high precision but of a size incompatible with all other imaginable uses<sup>1547</sup>.

**Draper Labs** (1932, USA) also designs cold atoms sensors, mostly, gravimeters and accelerometers for navigation systems.

**Wideblue** (2006, UK) creates MEMS gravimeters. It's a consulting and engineering company.

## Quantum clocks

Time measurement steadily progressed since the first mechanical clocks used between the 14th and 19th centuries. Quartz clocks appeared between the two World Wars. They were based on the piezoelectric effect demonstrated by Pierre and Jacques Curie in 1880. With a frequency of  $2^{15}$  Hz, time is counted with using frequency dividers, with a drift of a few hundred microseconds per day.

The first cesium atomic clocks dates from the 1950s. They have a frequency of the order of 9 GHz and provide a frequency accuracy of  $10^{-13}$ . The second is defined since 1967 as the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two "hyperfine" levels of the fundamental electronic state of cesium 133.

The recent variants of these clocks are "fountain clocks". They operate at very low temperature, with laser cooling bringing the atoms at 1  $\mu$ K, way much colder than superconducting qubits are at 15 mK, but is however easier to obtain than with a dilution refrigerator. A frequency oscillator generates a transition between two levels of cesium energy. The frequency is locked with a servo loop.

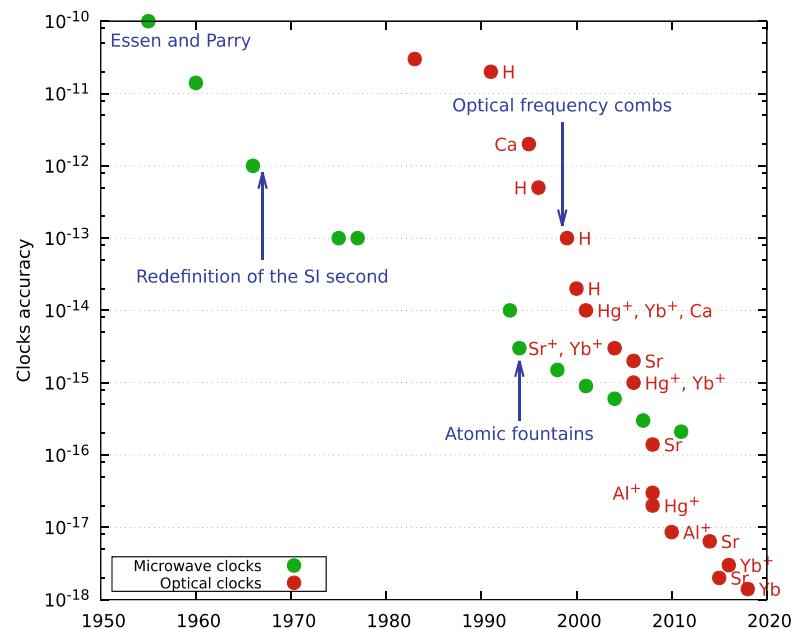
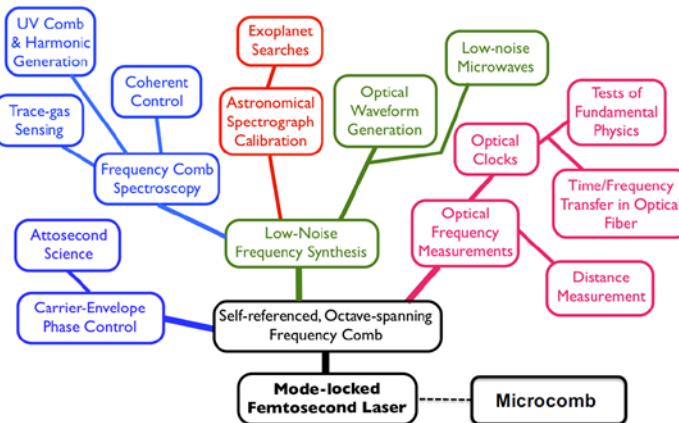
<sup>1546</sup> See [iXAtom - LP2N and iXblue Cold Atoms joint laboratory](#).

<sup>1547</sup> See [Advanced LIGO Just Got More Advanced Thanks To An All-New Quantum Enhancement](#) by Ethan Siegel, December 2019. And a description of the quantum squeezing technique used in the latest version of LIGO: [NIST Team Supersizes 'Quantum Squeezing' to Measure Ultrasmall Motion](#), 2019.

The precise measurement of frequencies has many applications: time measurement, synchronization of various devices on the Internet, even if only servers or scientific instruments, synchronization of moving objects to measure their position, astronomy (like with exoplanets and gravitational waves detection<sup>1548</sup>), absorption or emission precision spectroscopy, fiber optic transmissions and the generation of radio waves of arbitrary shape.

However, a better accuracy is needed. For about twenty years, it has been obtained through optical measurement of frequencies and time. The measurement of atomic vibrations has been replaced by the measurement of light waves generated by lasers and at  $10^{15}$  Hz.

It has allowed a gain in accuracy of five orders of magnitude ( $10^5$ ). It was demonstrated in 2000 to generate an accuracy of a femtosecond. This earned the Nobel Prize in Physics in 2005 to **Theodor Hänsch** (1941, German) and **John Hall** (1934, American).



Frequency combs were discovered with the first mode-locked lasers by Logan Hargrove in 1964<sup>1549</sup>. Before optical combs, light frequency harmonic generators were used with a combination of several lasers in complicated setups. To measure light high frequencies, these clocks use optical frequency combs, which subdivided optical (high) frequencies into microwave (lower) frequencies for frequency measurement and timekeeping. It uses blocked-mode lasers that generate very short pulses, which can be as short as a few femtoseconds.

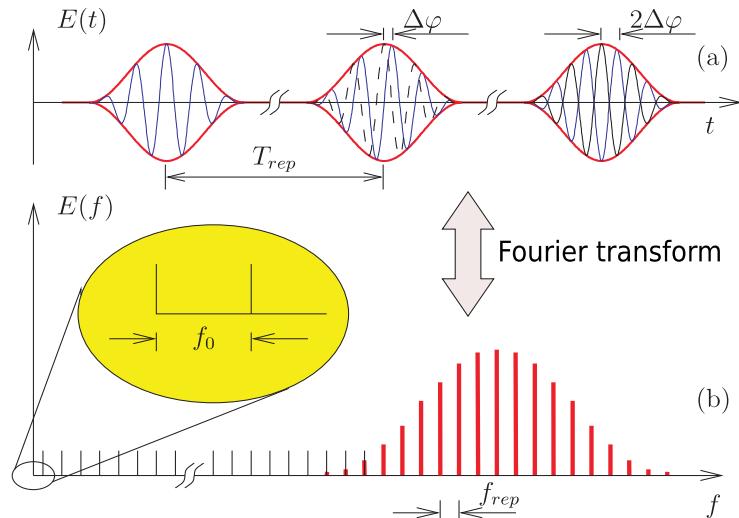
The frequency decomposition of this kind of signal gives a Gaussian-shaped frequency comb with each tooth regularly spaced at a frequency equivalent to that of the laser pulse. This is related to the fact that the length of the laser cavity is a multiple of the length of the electromagnetic waves emitted by the laser. The greater the multiple, the greater the frequency generated.

<sup>1548</sup> See [Chronometric Geodesy: Methods and Applications](#) by Pacome Delva, Heiner Denker and Guillaume Lion, 2019 (61 pages). It is the source of the graph on the evolution over time of the precision of clocks in the next page.

<sup>1549</sup> See [Nobel Lecture: Defining and measuring optical frequencies](#) by John Hall, 2006 (17 pages) and [Light rules: frequency combs](#) by Steven Cundiff, Jun Ye and John Hall in Pour la Science, 2008 (8 pages). John Hall describes frequency combs as the intersection of four initially independent fields of research: ultra-stable lasers, fast pulse lasers, nonlinear optical materials, and precision laser spectroscopy. This is a reflection of quantum computing and its many scientific and technological sources.

The frequency spectrum resembles a Gaussian curve. Its envelope is equal to the envelope of the spectrum of an isolated pulse, which is continuous. The width of the frequency spectrum covered can be narrow, a few nm in wavelength, or cover the entire visible spectrum, thus a few hundred nm.

A calculation is used to determine the very high frequencies of the frequency comb ( $f_n$ ). It uses several parameters: the reference frequency  $f_{rep}$  of the laser pulses which is of the order of 250 MHz to 1GHz,  $n$ , the number of frequencies detected via spectroscopy (there can be hundreds of thousands) and the emission phase of the blocked mode laser which is added to each pulse and generates the frequency offset  $f_0$ , which is evaluated with a method described below and which is also of a lower order than GHz<sup>1550</sup>.

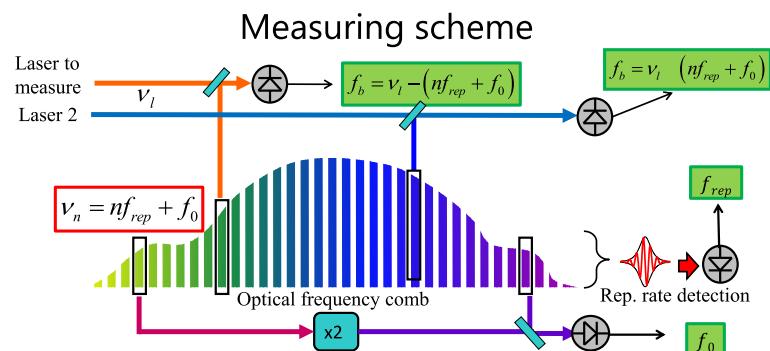


The measurement radio frequencies in the MHz/GHz wave range results in the measurement of frequencies in tens and hundreds of THz to the nearest Hz. The system thus acts as a frequency multiplier. The measurement of light frequencies is impossible with traditional electronics because of the frequencies used, which are several tens or hundreds of tera-Hertz. These calibrated frequency combs are also used to measure a frequency difference with this standard<sup>1551</sup>.

The frequency comb covers an octave, from one frequency ( $n$ ) up to its double ( $2n$ ). The evaluation of  $f_0$  is done by extracting the frequency  $f_n$ , and doubling it with a crystal. By adding this frequency doubled with  $f_{2n}$ , we obtain a beat at the frequency of  $f_0$ <sup>1552</sup>

$$2(f_0 + n \times f_{rep}) - (f_0 + 2n \times f_{rep}) = f_0$$

This is called **heterodyne detection**. The frequency comb becomes a kind of graduated ruler which is then used to position a frequency to be measured relative to the ruler. With that, you can build a new generation atomic clock<sup>1553</sup>!



If we know  $n$  (and we are sure of the signs in the equations), → the system is mathematically well determined

In practice, we may

- impose values to the different  $f$  with phase lock loops (multiplier scheme :  $\phi$ -lock  $f_{rep}$ , divider scheme:  $\phi$ -lock  $f_b$ ) (narrow line...)
- measure them with frequency counters
- and/or use clever tricks (exemple :  $f_b \otimes f_0 \rightarrow \text{BPF} \rightarrow v_l - nf_{rep} - f_0 + f_0 = v_l - nf_{rep}$ )

<sup>1550</sup> Illustration source: [Ultra-short light pulses for frequency metrology](#), CNRS (6 pages).

<sup>1551</sup> See [Phase Coherent Vacuum-Ultraviolet to Radio Frequency Comparison with a Mode-Locked Laser](#) by J. Reichert et al, 2005 (5 pages), [Direct Link between Microwave and Optical Frequencies with a 300 THz Femtosecond Laser Comb](#) by Scott Diddams et al, 2000 (4 pages), [Fundamentals of frequency combs What they are and how they work](#) by Scott Diddams (46 slides), [Optical frequency combs and optical frequency measurements](#) by Yann Le Coq, 2014 (38 slides) and [Chip-scale Optical Atomic Clocks and Integrated Photonics](#) by Matthew Hummon, NIST, 2018 (35 slides).

<sup>1552</sup> Schema source: [Optical frequency combs and optical frequency measurements](#) by Yann Le Coq, 2014 (38 slides), slide 11.

<sup>1553</sup> This is explained in [Optical Atomic Clocks](#) by Andrew Ludlow, Martin Boyd, Jun Ye, E. Peil and P.O. Schmidt, 2015 (65 pages) and [Optical atomic clocks](#) by N. Poli et al, 2014 (70 pages). See also [Photonic integration of an optical atomic clock](#) by Z. L. Newman et al, November 2018 (12 pages).

The readout of spectroscopy results using frequency combs can use CCD or CMOS cameras depending on the frequencies used in or around visible light<sup>1554</sup>. This measurement accuracy evolves with the use of lasers using a high pulse frequency.

These are usually based on titanium-sapphire with pulses of a few femtoseconds ( $10^{-15}$  to  $10^{-14}$  seconds).

To date, the record for the accuracy of an atomic clock using spectroscopy is that of **NIST**. It is built with an aluminum ion associated with a magnesium anion. The aluminum ion is excited by two ytterbium lasers. Measurement is carried out using a quantum logic spectroscopy which is using the frequency combs seen above<sup>1555</sup>.

The clock reaches an accuracy of  $10^{-18}$  seconds, a drift of one second per 33 billion years, 2.5 times the age of the Universe<sup>1556</sup>. In this market for optical quantum clocks, there are many research laboratories that produce their own equipment.

NIST is also working on an atomic clock that would fit into a component the size of a coffee bean, using a double frequency comb and rubidium gas. The whole thing consumes only 275 mW. This project was co-funded by DARPA<sup>1557</sup>. However, for the moment, the precision obtained is not yet satisfactory for industrialization.

One of the projects of the European Quantum Flagship, **iqClock** (Netherlands, €10M), also aims to create very high-precision, portable quantum clocks.

The consortium brings together six universities and six private partners including Teledyne EV (USA), Toptica (Germany), NKT Photonics (Denmark), AckTar (Israel) and Chronos (UK).



In the private sector, **Teledyne** sells Minac (cesium atomic clock), T-CSAC (also cesium, integrated in a chip) and Synchronicity (ytterbium-based).



**MicroSemi** (1960, USA) sells its Quantum SA.45s, a miniaturized chip-scale atomic clock. Among other use cases, it can be used in portable IED (improvised explosive devices) jammers. The company is a subsidiary of MicroChip Technology (1989, USA).

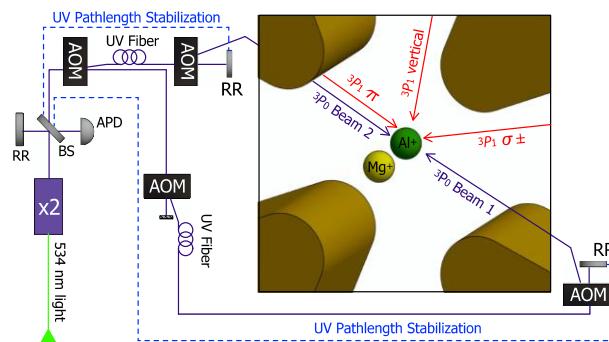
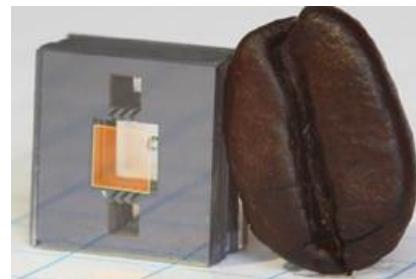


FIG. 1. Simplified schematic of the quantum-logic clock experimental setup. A frequency-quadrupled Yb-doped fiber laser is locked to the  $^1S_0 \leftrightarrow ^3P_0$  transition ( $\lambda \approx 267$  nm) by alternating the probe direction between two counterpropagating laser beams (shown in violet). An enlarged view of the trapping region is shown on the right. Three nominally orthogonal beams used for micromotion measurements are shown in red. Acousto-optic modulator (AOM), beam splitter (BS), retro-reflector (RR), frequency doubling stage (x2).



<sup>1554</sup> See [Frequency comb spectroscopy](#) by Nathalie Picqué and Theodor Hänsch, 2019 (27 pages) which describes the many methods and use cases of frequency comb based spectroscopy.

<sup>1555</sup> See this explanation: [Quantum Logic for Precision Spectroscopy](#) by Piet Schmidt et al, 2009 (6 pages).

<sup>1556</sup> Illustration source: [27Al+ Quantum-Logic Clock with a Systematic Uncertainty below 10<sup>-18</sup>](#), 2019 (6 pages).

<sup>1557</sup> The project is documented in [Architecture for the photonic integration of an optical atomic clock](#), 2019 (6 pages).



**HyperLight Corp** (2018, USA), based in Cambridge, near Boston, develops nanophotonic integrated circuits such as frequency combs or resonators that are used in quantum sensing.



**Cryoclock** (2016, Australia) develops sapphire-based cryogenic oscillators. The company was co-founded by John Hartnett. Applications include trapped ion quantum processors and atomic clocks.



**Orolia** (2005, France) creates atomic clocks with cesium, or based on rubidium oscillators. They mainly target the aerospace industry and provide the Galileo GNSS service.



**Syrlinks** (2011, France) develops miniature atomic clocks based on MEMS and cesium for embedded applications. Their MMAC is 40 x 35 x 22 mm and consumes less than 0.3 W.



**TMD** (1969, UK) sells microwave amplifiers. They also develop atomic clocks and instrumentation for the manipulation of cold atoms.



**VectorAtomic** (2018, USA) markets rubidium atomic clocks for quantum inertial navigation systems that can then avoid using GPS.



**Vescent Photonics** (2002, USA) offers optical frequency comb generators for use in atomic clocks. They also master the laser-based technique used for controlling cold. They are based in Colorado.



**Rydberg Technologies** (2015, USA) provides cesium or rubidium specimens for cold atom-based metrology solutions. They also sell a Rydberg atoms-based radio-frequency probe, a RFLS (Rydberg Field Measurement System). Their technology is also integrated in AM and FM radio-frequency receivers.

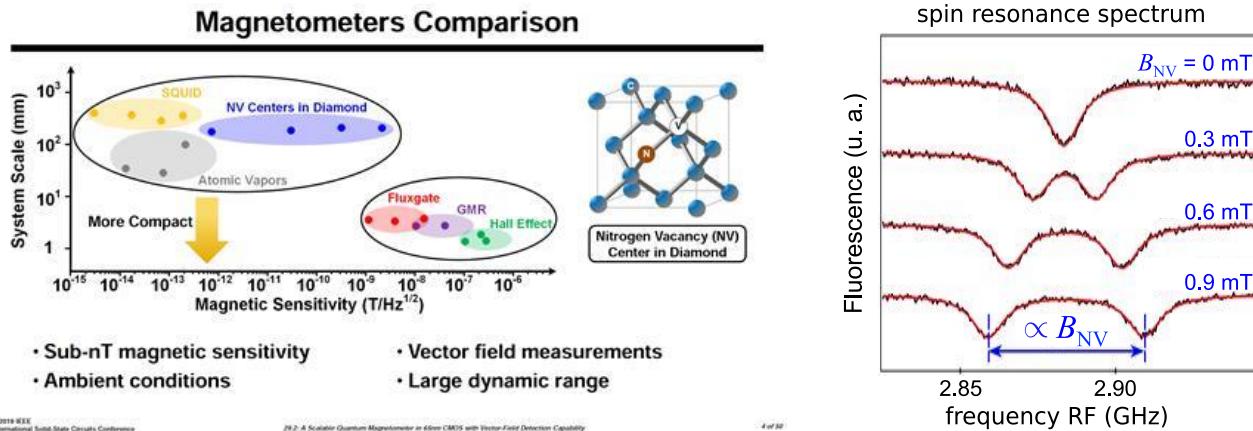
Finally, let us mention again **Muquans**, which also uses its cold atoms expertise to sell an atomic clock, the MuClock, designed in partnership with the LP2N laboratory in Bordeaux and the LNE-SYRTE. It is positioned as an alternative to cesium atomic clocks. The instrument weighs 135 kg and consumes 200W.

## Quantum magnetometers

Quantum magnetometers are used to detect small variations or levels of magnetism with high spatial accuracy. There are many uses cases: navigation, mineral exploration, current detection, magnetocardiography, magnetoencephalography, orientation of drones and autonomous vehicles in tunnels where GPS does not work<sup>1558</sup>, sonar, detection of moving metal objects such as vehicles and cellular imaging<sup>1559</sup>.

<sup>1558</sup> A UAV solution using GPS in a tunnel is proposed by the startup Hovering Solutions (Spain).

<sup>1559</sup> See [Nitrogen-vacancy centers in diamond for nanoscale magnetic resonance imaging applications](#) by Alberto Boretti et al, 2019 (24 pages).



Different techniques are available for precision magnetometry including cold atoms<sup>1560</sup>, SQUID (superconducting effect with a Josephson junction as in superconducting qubits<sup>1561</sup>) and NV-centers. Measuring magnetism with NV centers exploit the variation of the spin resonance spectrum in the diamond cavity, which depends on the ambient magnetic field (see the chart above on the right on spin resonance spectrum). The distance between the two fluorescent light pulses (Y) generated is measured as a function of the electromagnetic excitation frequency used (X)<sup>1562</sup>. The spins preparation is performed with a laser and its modification with 3 GHz microwave pulses.

The accuracy of magnetism measurement can reach a pico-Tesla<sup>1563</sup>, billions of times less than terrestrial magnetism<sup>1564</sup>. The NV-centers technique appeared in 2009. It is notably developed in France by Thales<sup>1565</sup>.

NV centers provide a lesser precision than cold atoms but their use is more practical because the instrument is easier to miniaturize and most of them work at ambient temperature<sup>1566</sup>.

Scanning probes magnetometers use a diamond nanocrystal containing a single cavity and a nitrogen atom, which ensures the accuracy of the measurement. The probe can be moved in space and used to analyze the magnetism of a material in 2D<sup>1567</sup>.

Laboratories in Bristol, the University of Ulm in Germany and Microsoft are working on the use of NV Centers techniques coupled with machine learning and Bayesian inference methods to correct the noise found at higher temperatures<sup>1568</sup>.

<sup>1560</sup> See the Rydberg atom technique described in [Quantum sensing using circular Rydberg states](#) by Rémi Richaud, LKB, November 2018 (41 slides). See also the thesis [Rubidium vapors in high magnetic fields](#) by Stefano Scotto, November 2017 (168 pages).

<sup>1561</sup> See this presentation of SQUID applications: [SQUID Fundamentals and Applications](#) by Robin Cantor, 2017 (48 slides).

<sup>1562</sup> After optical magnification, fluorescence can be analyzed by a CCD image sensor.

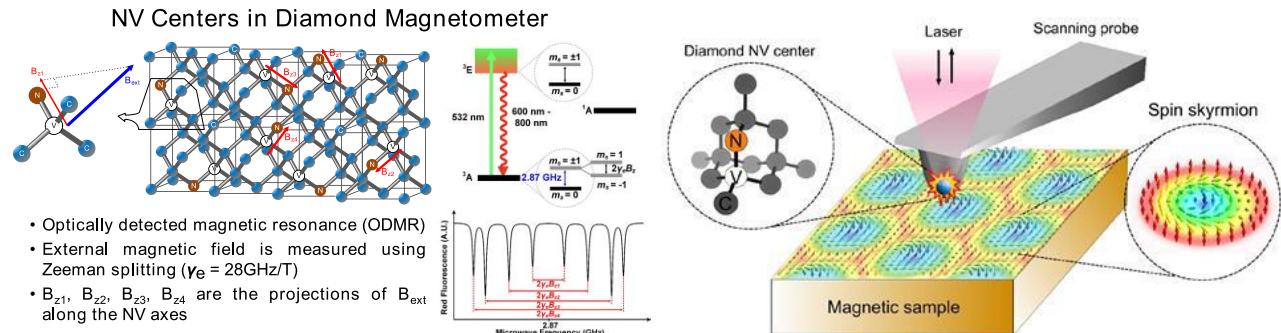
<sup>1563</sup> Source of illustration: [NV Diamond Centers: from material to applications](#) by Jean-François Roch, Collège de France, 2015 (52 slides).

<sup>1564</sup> The accuracy of magnetometry with NV centers is evaluated with the formula  $1\mu\text{T}/\sqrt{\text{Hz}}$ .

<sup>1565</sup> ASTERIQS (France, €9.7M) or "Advancing Science and Technology through diamond Quantum Sensing" is a European Quantum Flagship project launched in 2018 and led by Thales, which is expected to advance techniques for measuring magnetic, electric, temperature and pressure fields. There are many applications, such as sensors for vehicle battery monitoring, high-resolution sensors for nuclear medical imaging (NMR, nuclear magnetic resonance) or for creating radio frequency spectrum analyzers. The Swiss startup Qnami is involved in the project and provides artificial diamonds.

<sup>1566</sup> Illustration source: [A Scalable Quantum Magnetometer in 65nm CMOS with Vector-Field Detection Capability](#) by Mohamed Ibrahim from MIT 2019 (51 slides). It describes a miniaturization process of a quantum magnetometer combining a 65 nm CMOS circuit manufactured by TSMC and a diamond NV-center based system.

<sup>1567</sup> Illustration source: [Probing and imaging nanoscale magnetism with scanning magnetometers based on diamond quantum defects](#), 2016 (35 slides).



**QUSPIN**

**QuSpin** (2012, USA) is developing an optical magnetometer that is positioned as an alternative to NV centers based magnetometers.

 **Qubic**

**Qubic** (2019, Canada) is a startup from the Institut Quantique from the University of Sherbrooke in Quebec that is working on microwaves-based quantum sensing tools for sensing, imaging and communications. It is led by Jérôme Bourassa.



**SBQuantum** (2019, Canada) also known as SBTech and Shine Bright Technologies develops NV centers-based quantum magnetometers. They target the automotive market but are also working on integrating their technology into Cubesat-type satellites. It is also a startup coming from the Institut Quantique from the University of Sherbrooke.

Their technique is called "Optically Pumped Magnetometer (OPM)". They have even developed a tri-axial version of their system that measures magnetism in the three X, Y and Z axis. Research on this product was funded by the NIH (National Health Institute). The product is mainly targeting magnetoencephalography brain imaging.

**qutools**



**Qutools** (2005, Germany) offers its quNV quantum magnetometer, based on diamond NV-centers as its name suggests. It fits in a 3U rack.



Also in Germany, the University of Stuttgart is working with the Fraunhofer Institute to transfer NV-centered magnetometry technology as part of the **QMag**<sup>1569</sup> project.

 **supracon**  
SQUID AND MICROFABRICATION TECHNOLOGIES

**Supracon** (2001, Germany) manufactures magnetometers based on SQUIDs (Superconducting Quantum Interference Devices). It is a spin-off of the Leibnitz Institute of Photonics in Jena. It sells its sensors to astrophysics research laboratories and for geophysics prospection.

 **GREAT LAKES CRYSTAL TECHNOLOGIES**

**Great Lakes Crystal Technologies** (2019, USA) is a supplier of diamonds for use in NV center applications, especially for quantum magnetometers. It is a spin-off from the University of Michigan and Fraunhofer USA.

 **FieldLine**  
Magnetic sensing and imaging solutions

**FieldLine Inc** (2020, USA) develops NV centers quantum sensing systems, particularly for medical brain imaging and non-destructive materials testing.

<sup>1568</sup> See [Magnetic-Field Learning Using a Single Electronic Spin in Diamond with One-Photon Readout at Room Temperature](#) by Raffaele Santagati et al, 2018 (18 pages).

<sup>1569</sup> See [Quantum Magnetometers for Industrial Applications](#), April 2019.



## Twinleaf



It uses an optically-pumped magnetometers measuring weak magnetic fields. These are made with a laser illuminating a small glass cell containing a pressured gas of rubidium or cesium. A diode detects the transmitted light that depends on the local magnetic field perpendicular to the laser beam<sup>1570</sup>. The technology is competing with SQUIDs based MEGs.



**CIQTEK** (2016, China, \$15M) manufactures quantum sensors targeting quantum computation, healthcare, food safety, chemistry and material science markets. These sensors are NV center magnetometers.

At last, the **Ivar Giæver Geomagnetic Laboratory** (IGGL) in Norway also uses SQUIDs to detect underground magnetism for paleomagnetic applications, to measure the magnetic remanence of ancient rocks. Using SQUIDs, their magnetometer must be cooled to 4K with a pulsed tube<sup>1571</sup>.



**GEM Systems** (1980, Canada) is selling quantum magnetometers using optically pumped potassium (K-Mag).



**wainvam**

**ODMR Technologies** (2015, USA) is a stealth spin-off from Berkeley which designs a magnetic resonance spectroscopic analysis system based on NV centers.

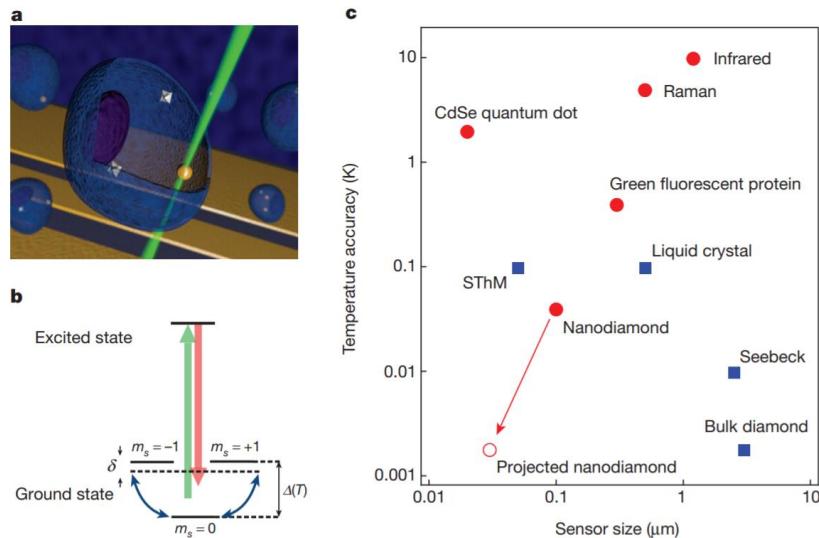
**Wainvam-E** (2020, France) is providing a set of magnetometry solutions based on NV centers targeting nondestructive measurement of various materials like steel and oxidation characterization in live cells.

<sup>1570</sup> See [Optically pumped magnetometers: From quantum origins to multi-channel magnetoencephalography](#) by Tim M.Tierney et al, 2019 (12 pages).

<sup>1571</sup> See [Instruments for Paleomagnetic Measurements WSGI \(2G\) Model 755 Superconducting Rock Magnetometer \(SRM\)](#).

# Quantum thermometers

NV centers have another use: temperature measurement with an accuracy of a few mK and with a very high spatial resolution, all with miniaturized sensors. It is currently the most powerful temperature measurement technology for these different dimensions. It allows, for example, to determine the temperature within living cells and organisms with a sub-mm precision<sup>1572</sup>.

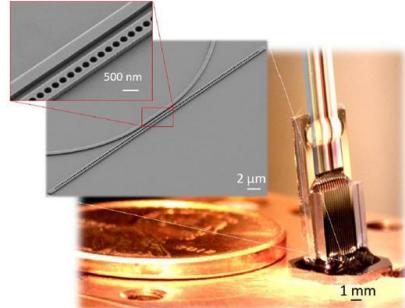


**Figure 1 | Nitrogen–vacancy-based nanoscale thermometry.** **a**, Schematic image depicting nanodiamonds (grey diamonds) and a gold nanoparticle (yellow sphere) within a living cell (central blue object; others are similar) with coplanar waveguide (yellow stripes) in the background. The controlled application of local heat is achieved by laser illumination of the gold nanoparticle, and nanoscale thermometry is achieved by precision spectroscopy of the nitrogen–vacancy spins in the nanodiamonds. **b**, Simplified nitrogen–vacancy level diagram showing a ground-state spin triplet and an

excited state. At zero magnetic field, the  $| \pm 1 \rangle$  sublevels are split from the  $| 0 \rangle$  state by a temperature-dependent zero field splitting  $\Delta(T)$ . Pulsed microwave radiation is applied (detuning,  $\delta$ ) to perform Ramsey-type spectroscopy. **c**, Comparison of sensor sizes and temperature accuracies for the nitrogen–vacancy quantum thermometer and other reported techniques. Red circles indicate methods that are biologically compatible. The open red circle indicates the ultimate expected accuracy for our measurement technique in solution (Methods).

There are also solutions for temperature measurement in biological matter by fluorescence that are based on quantum dots<sup>1573</sup>.

In 2017, NIST produced a quantum photonics thermometer of very small size for optically measuring the surface temperature of metals. However, the picture does not show the control electronics associated with the sensor.



**Southwest Sciences** (1985, USA) develops optical temperature sensors based on NV centers for use in cryogenic systems. The company was founded by Alan C. Stanton and Joel A. Silver.

## Imaging and microscopes

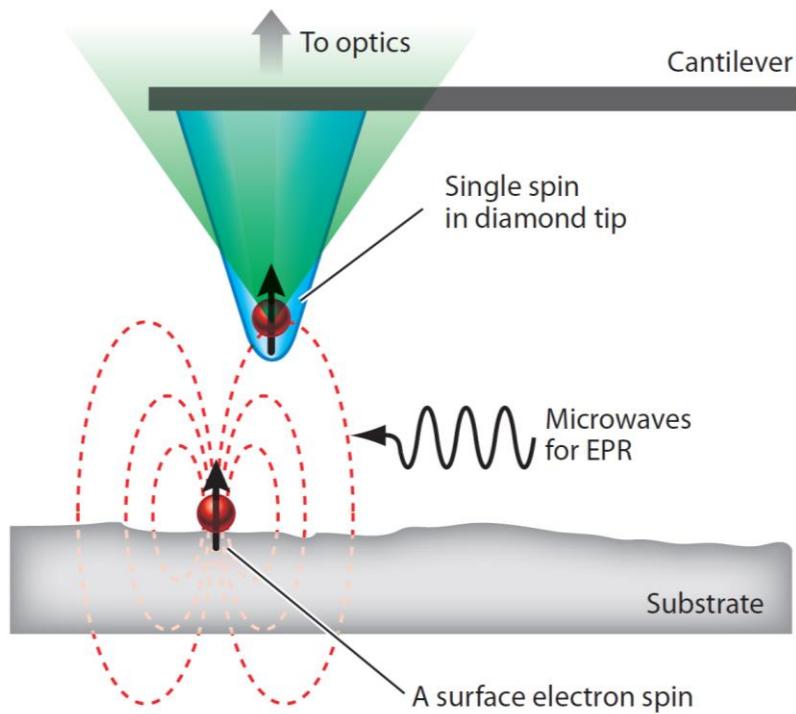
New generation microscopes are based on quantum effects. We will take a look at microscopes using NV-centers based magnetometers or cold atoms, some mysterious "ghost imaging" systems that take pictures of objects with a single pixel sensor and other special quantum sensors.

<sup>1572</sup> See [Nanometre-scale thermometry in a living cell](#), 2013 (6 pages) and [Real-time nanodiamond thermometry probing in vivo thermogenic responses](#) by Masazumi Fujiwara et al, September 2020 (10 pages).

<sup>1573</sup> See [Intracellular thermometry with fluorescent sensors for thermal biology](#) by Kohki Okabe et al, 2018 (15 pages).

NV-centers based imaging is a focus of the **Max Planck Institute for Solid State Research** and of the **Fraunhofer Institute** for Applied Solid State Physics (IAF) in Freiburg, Germany. Their microscopes are used to analyze organic molecules with excellent spatial resolution.

They are also working on electron spin resonance spectroscopy (ESR) at cryogenic temperature which allows to examine atoms and molecules at the level of their electron spin. The technique is integrated in scanning tunneling microscopes as well as in atomic force microscopes (AFM). The electron spin of the examined materials is excited by a magnetic field and microwaves.



The NV-center technique allows the examination of a hard disk and semiconductors defects with a probe equipped with a single NV-center (*below*<sup>1574</sup> *and above*<sup>1575</sup>). It is also used for the characterization (quality control) of integrated circuits working with millimeter frequencies such as in 5G<sup>1576</sup>. Others are working on NV centers-based microscopy of living cells<sup>1577</sup>. There is even an application to qualify malaria patients by analyzing hemozoin nanocrystals appearing in red blood cells affected by the disease parasite<sup>1578</sup>. These techniques are used with confocal microscopy. This generates images with a very shallow depth of field of about 400 nm, creating optical sections of the sample to analyze.

---

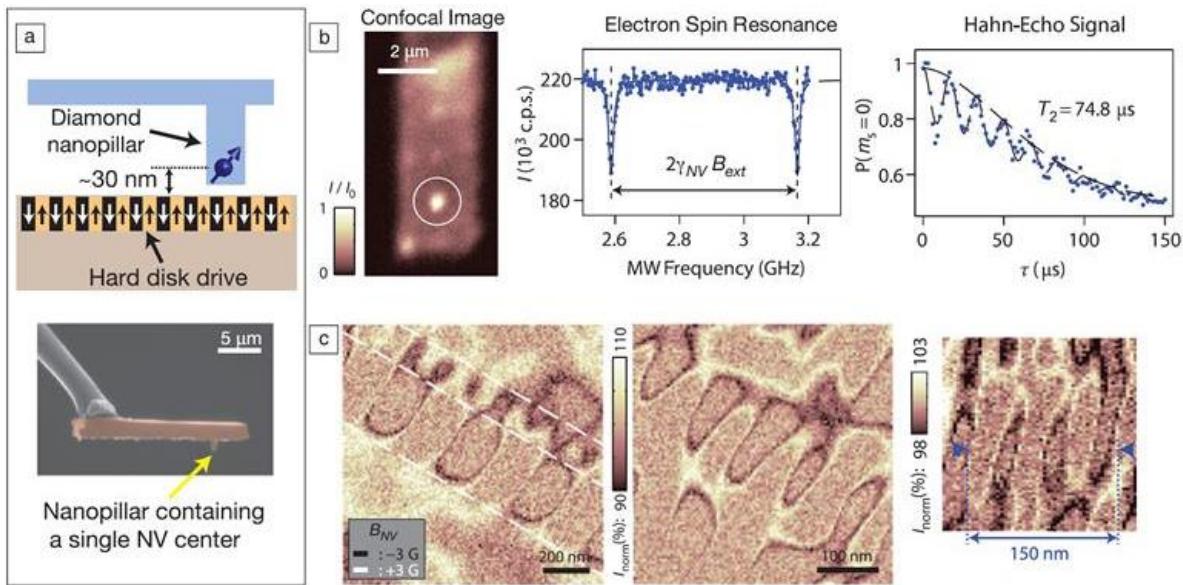
<sup>1574</sup> Illustration source: [Solid-State Spin Quantum Computers](#) (21 slides) and [Optical far-field super-resolution microscopy using nitrogen vacancy center together in bulk diamond](#), 2016 (5 pages) which describes a microscopy technique with a resolution down to 6 nm.

<sup>1575</sup> Illustration source: [Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology](#), 2014 (27 pages).

<sup>1576</sup> See [Microwave Device Characterization Using a Widefield Diamond Microscope](#), 2018 (10 pages) which involves in particular the LSPM of Paris.

<sup>1577</sup> See [A fluorescent nanodiamond foundation for quantum sensing in cells](#), 2018 (147 pages) which discusses microscopy of living cells.

<sup>1578</sup> See [Diamond magnetic microscopy of malarial hemozoin nanocrystals](#) by Ilja Fescenko et al, September 2018 (17 pages),

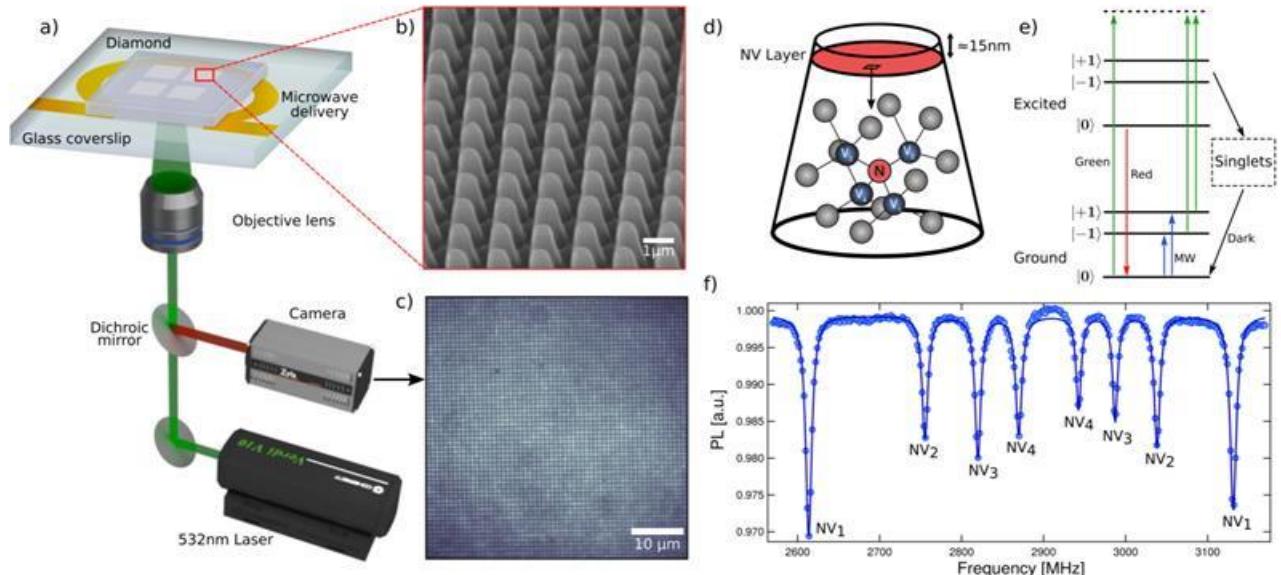


**Figure 4.** (a) Schematic of a monolithic diamond nanopillar probe (top) and representative SEM image of the nanopillar probe (bottom). (b) Characteristics of a nanopillar probe device. Confocal image of the device (left) clearly shows a localized fluorescence spot from a single NV center at the position of the nanopillar. Electron spin resonance (middle) was acquired with an enhanced fluorescence of 220,000 photons/sec. The coherence time of the measured Hahn-echo signal (right) is  $74.8 \mu\text{s}$ , an order of magnitude longer than a typical Hahn-echo coherence time of commercial diamond nanocrystals ( $\sim 5 \mu\text{s}$ ). (c) Magnetic images of a hard disk drive acquired by the nanopillar probe. Alternating magnetic bits were imaged with varying sizes down to 25 nm (right), indicating the distance between a single NV center at the probe and the hard disk sample is roughly within 25 nm. Adapted with permission from Reference 19. © 2012 Nature Publishing Group.

By modifying the position of the depth focal plane, a series of images are created which are then assembled to generate a 3D view of the analyzed sample. The light source is reflected or obtained by fluorescence in reaction to a laser beam. The result is a Confocal Laser Scanning Microscope (CLSM).

NV-centers can also improve the accuracy of adaptive optics, which are used in astronomy<sup>1579</sup>.

Other techniques using laser interferometry make it possible to examine molecules at the atomic level in their environment and not in a vacuum and cryogenic cold<sup>1580</sup>.



<sup>1579</sup> See [Nanodiamonds enable adaptive-optics enhanced, super-resolution, two-photon excitation microscopy](#), 2019 (7 pages).

<sup>1580</sup> See [An Entanglement-Enhanced Microscope](#) by Takafumi Ono, Ryo Okamoto, Shigeki Takeuchi, 2014 (8 pages).

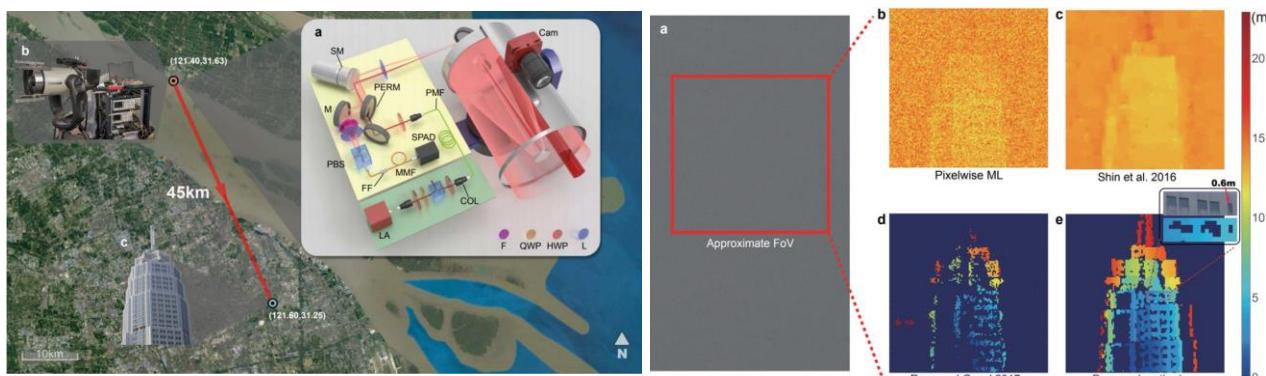
Imaging can also exploit an array of small NV centers that provide much better resolution than imaging systems based on SQUIDs magnetometers. The examples *above* show its architecture<sup>1581</sup>.

The second was made to study bacteria that contain magnetic microelements. In other cases, magnetic markers can be used to attach themselves to the cells to be detected, typically in oncology.

The European Quantum Flagship includes **MetaboliQs** (Germany, €6.7M), a diamond-based nuclear magnetic resonance cardiac medical imaging project. It also detects atrial fibrillation, a common cardiac pathology, with a rubidium-based atomic magnetometer<sup>1582</sup>. Another Flagship project, **PhoG** (United Kingdom, €2.6M) or [Sub-Poissonian Photon Gun by Coherent Diffusive Photonics](#), is about creating stable light sources for various applications, particularly in quantum sensing. It involves researchers from Belarus, Germany and Switzerland.

The Chinese laboratory of Jian-Wei Pan has developed a camera that analyzes the reflection of a single photon per pixel on the object to be observed. This is associated with algorithms filtering out the noise. Imaging is done in the infrared at 1550 nm and with polarized photons. This could be integrated in observation satellites<sup>1583</sup>.

Another application is single-photon LiDARs, used for remote wind detection at high resolution. It has been developed in China since 2014 and is used in transportable radars, including UAVs<sup>1584</sup>.



Similarly, **QLM Technology** (2017, UK) has developed a quantum magnetometer solution that detects methane leaks in pipelines up to 100 meters away. The measuring system weighing a few kg can be embarked in a large drone flying at 50 km/h. They use a laser that illuminates a gaseous medium of variable opacity and a photodetector. **IDQ** is involved in the creation of the solution at the LiDAR level.



<sup>1581</sup> See [Enhanced widefield quantum sensing with nitrogen-vacancy ensembles using diamond nanopillar arrays](#) by D. J. McCloskey, 2019 (7 pages). The NV centers matrices are 100 μm wide. The illustration comes from other work published in 2013, cited in the conference [Magnetic imaging using NV-diamond: techniques & applications](#) by Ronald Walsworth, 2015 (51 min). Notably [Optical magnetic imaging of living cells](#), Le Sage et al, Nature, 2013 (11 pages). See also [Principles and Techniques of the Quantum Diamond Microscope](#) by Edlyn V. Levine et al, 2019 (47 pages) and [Atomic Scale Magnetic Sensing and Imaging Based on Diamond NV Centers](#) by Myeongwon Lee et al, 2019 (17 pages).

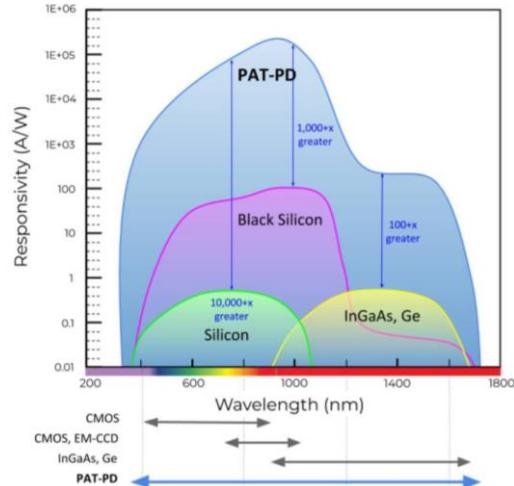
<sup>1582</sup> See [New quantum technology could help diagnose and treat heart condition](#), March 2020.

<sup>1583</sup> See [A new camera can photograph you from 45 kilometers away](#), May 2019 which refers to [Single-photon computational 3D imaging at 45 km](#) by Zheng-Ping Li et al, April 2019 (22 pages). And the presentation [Single Photon LiDAR](#) by Feihu Xu, June 2019 (25 slides).

<sup>1584</sup> See [Single-Photon Lidar for atmospheric detection](#) by Haiyun Xia et al, June 2019 (22 slides).



**Seedevice** (2017, USA) develops a quantum imaging system, the PAT-PD (Photon Assisted Tunneling Photo Detector), which exceeds the performance of traditional CMOS imagers. This imager contains photosites using the tunneling effect that can detect single photons in a wide range of wavelengths from near infrared (1800 nm) to ultraviolet (up to UVA1, at 350 nm). This can be used for seeing in the dark and for medical imaging, like for detecting blood vessels in the infrared range.



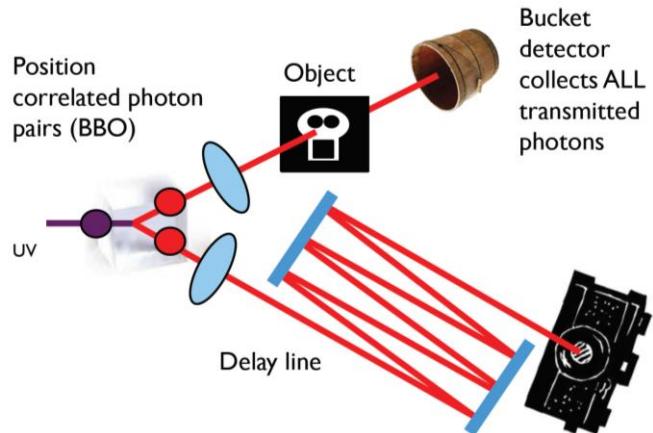
**QDTI** (2012, USA) is the only known startup initially engaged in the development of a quantum computer based on NV Centers. Created by a team from Harvard University, it is logically based in Boston.

The startup is now focused mainly on medical imaging systems also using these NV centers, with the creation of precision magnetometers combined with MRI and immunological tests.



**Nvision Imaging** (2015, Germany) is developing an NV centers-based MRI medical imaging solution.

Quantum imaging can also use the curious technique of ghost imaging or quantum phantom imaging. It exists in many variations. The first one used a generator of infrared photons in 1995<sup>1585</sup>. One half of the photons illuminates the object and the other half a photo sensor, by crossing an optical delay line<sup>1586</sup>. The photons illuminating the object are entangled with those illuminating the camera, which has not seen the object at all! The obtained image is very noisy and requires some appropriate processing.



What is the purpose of this? Mainly to analyze objects with a very low photon number to avoid that they modify the object to be analyzed. This can be interesting in microbiology<sup>1587</sup>. The analyzed objects are seemingly always very small<sup>1588</sup>.

<sup>1585</sup> See [Optical imaging by means of two-photon quantum entanglement](#) by Yanhua Shih et al, 1995 (4 pages), University of Maryland. And [Observation of two-photon 'ghost' interference and diffraction](#) by Yanhua Shih, 1995 (4 pages).

<sup>1586</sup> See [An introduction to ghost imaging: quantum and classical](#) by Miles Padgett and Robert Boyd, 2016 (10 pages) provides a good overview of the subject. See also [Quantum Ghost Image Identification with Correlated Photon Pairs](#), 2010 (4 pages).

<sup>1587</sup> See [The Dawn of Quantum Biophotonics](#) by Dmitri Voronine et al, 2016 (30 pages).

<sup>1588</sup> See this panorama of many ghost imaging methods: [The promise of quantum imaging](#) by Robert Boyd, 2016 (53 slides).



**Chipiron** (2020, France) develop a portable MRI system using SQUIDS quantum detectors (superconducting / Josephson effect based). The startup was created by Dimitri Labat and Evan Kervella.

**Qnami** (2017, Switzerland, \$7.3M) is a spin-off from the Quantum Metrology Research Laboratory at the University of Basel. Among other things, they produce artificial diamonds for various photonics applications.

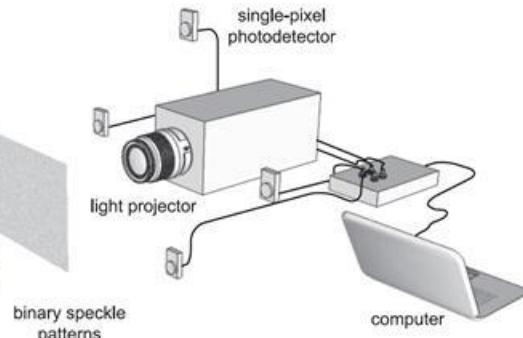
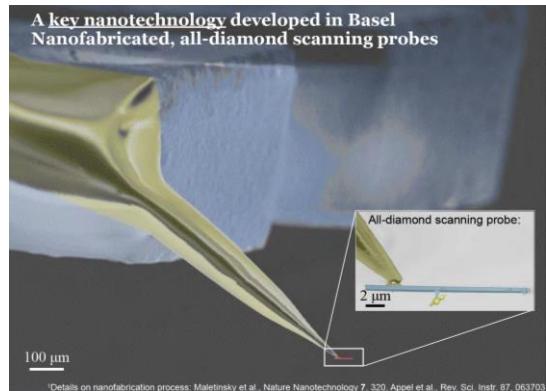
Their targeted first the quantum sensing market with their Quantilever MX nano-diamonds probes.

They then launched in 2019 the ProteusQ range of NV center confocal microscopes, used to analyze ferromagnetic materials, based on the Quantilever probe.

Quantonation and Runa capital are among their investors. And one of the co-founders and the CEO, Mathieu Munsch, came from Grenoble Phelma and worked at the CEA in Grenoble.

Other non-quantum techniques use a single-pixel color imager that uses 1300 structured lights per second to illuminate the object for a few seconds.

The sensor consists of four photodiodes positioned at different locations<sup>1589</sup>. This makes it possible to generate a 3D view of the object.



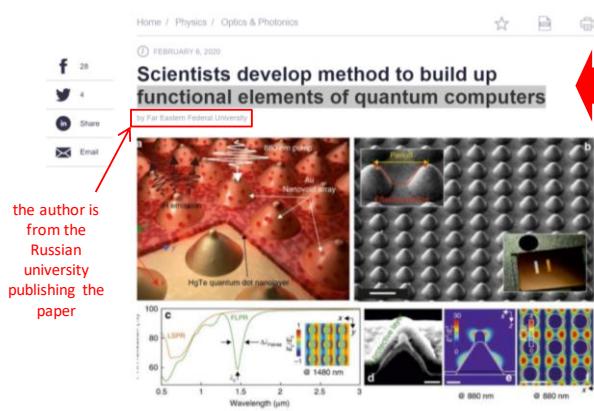
**Fig. 1. Experimental setup used for 3D surface reconstructions.** The light projector illuminates the object (head) with computer-generated random binary speckle patterns. The light reflected from the object is collected on four spatially separated single-pixel photodetectors. The signals from the photodetectors are measured and used to reconstruct a computational image for each photodetector.

Finally, quantum imaging can also rely on the illumination of the object by entangled microwaves, using the principle of quantum radar that we will see in the following section. It is interesting for analyzing objects with low reflectivity, which would be useful in medical imaging as well as for creating short-range radars<sup>1590</sup>. Entangled photon can also be used to create holograms, as recently discovered by a team of physicists from the University of Glasgow<sup>1591</sup>.

<sup>1589</sup> See [Fast full-color computational imaging with single-pixel detectors](#) by Stephen Welsh et al, 2013 (7 pages). Also seen in [3D Computational Imaging with Single-Pixel Detectors](#), 2013 (4 pages) which extends this to the capture of 3D objects using four single-pixel sensors. The video projector creates patterns that illuminate the object and alternate with its negative. See finally [Imaging with a small number of photons](#) by Peter Morris et al, 2014 (9 pages) and [Quantum-inspired computational imaging](#), 2019 (9 pages).

<sup>1590</sup> See [Experimental Microwave Quantum Illumination](#) by S. Barzanjeh et al, August 2019.

<sup>1591</sup> See [Polarization entanglement-enabled quantum holography](#) by Hugo Defienne et al, Nature, 2021 (31 pages).



in the original article, nothing on 'computers' and 'qubits'

"our results provide an important step towards the design of IR-range devices for various application"

=> the solution is targeting the quantum sensing market, not quantum computing

## ARTICLE Open Access

### Tailoring spontaneous infrared emission of HgTe quantum dots with laser-printed plasmonic arrays

A. A. Sergeev<sup>1</sup>, D. V. Pavlov<sup>2,3</sup>, A. A. Kuchmishak<sup>1,2</sup>, M. V. Lapine<sup>3</sup>, W. K. Yu<sup>4</sup>, Y. Dong<sup>5,6</sup>, N. Ke<sup>7</sup>, S. Juddkatz<sup>8</sup>, N. Zhao<sup>9</sup>, S. V. Kershaw<sup>9</sup> and A. L. Rogach<sup>10</sup>

Chemically synthesized near-infrared to mid-infrared (IR) colloidal quantum dots (QDs) offer a promising platform for the realization of devices including emitters, detectors, security, and sensor systems. However, at longer wavelengths, the quantum yield of such QDs decreases as the radiative emission rate drops following Fermi's golden rule, while non-radiative recombination channels compete with light emission. Control over the radiative and non-radiative channels of the IR-emitting QDs is crucially important to improve the performance of IR-range devices. Here, we demonstrate that engineering the spontaneous emission rate of HgTe QDs coupled to metal HgTe QDs coupled to periodically arranged plasmonic centers in the form of nanobumps, produced on a laser-supported Au films via ablation-free direct femtosecond laser printing. The enhancement is achieved by simultaneous radiative coupling of the emission channel that specifically matches the first-order lattice resonance of the array, as well as more efficient photoluminescence excitation provided by coupling of the pump radiation to the local surface plasmon resonances of the isolated nanorodres. Moreover, coupling of the HgTe QDs to the lattice plasmons reduces the influence of the ligand shell on the emission properties of the HgTe QDs. Considering the ease of the chemical synthesis and processing of the HgTe QDs combined with the scalability of the direct laser fabrication of nanorodres with tailored plasmonic responses, our results provide an important step towards the design of IR-range devices for various applications.

#### Introduction

Inexpensive near-infrared (IR) to mid-IR sources and devices operating in the 1–3 μm range have been revolutionizing technologies for the realization of various night vision and security systems, sensing and spectroscopy tools, etc. Colloidal semiconductor quantum dots (QDs) characterized by a high photoluminescence quantum yield (PLQY), which currently reaches at least 40% for QDs in the 1–2 μm range, represent a promising material for the realization of these devices<sup>1–3</sup>. However,

at longer wavelengths, the QY rapidly drops as the radiative and non-radiative recombination channels become more effectively with light emission. Control over the emission properties of the QDs is expected to provide a way to achieve the ultimate performance of such devices, providing a means of restoring the chance of radiative emission and increasing the overall efficiency. The emission properties of any quantum emitter are known to be strongly modified in the vicinity of a plasmonic nanostructure, which can resonantly interact with pump radiation via excitation of collective oscillations of a free electron plasma<sup>4</sup>. In particular, both spontaneous radiative and non-radiative emission rates, the lifetime of an

Correspondence: A. A. Kuchmishak (alexander.kuchmishak@rane.ru) or A. L. Rogach (andrey.rogach@phys.org).  
†These authors contributed equally to this work.  
✉Far Eastern Federal University, Vladivostok 690041, Russia.  
✉Russian Academy of Sciences, Vladivostok 690041, Russia.  
✉Far Eastern Federal University, Vladivostok 690041, Russia.  
Full list of author information is available at the end of the article.

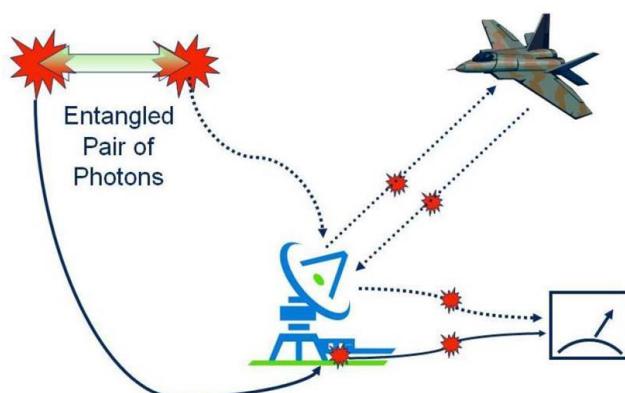
© The Author(s) 2020. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in other forms, without prior permission or written permission from the copyright holders, for non-commercial purposes, provided the original author and source are credited and no changes are made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

Note that the topic of quantum imaging can sometimes be confusing. This is eloquent with this promotion of a particular type of quantum dot, confused with some fancy quantum computing technique (*above*). And here, it was not a problem with some journalist since the "wrong" article comes from the laboratory promoting the research results<sup>1592</sup>.

## Quantum radars

Quantum radars are slowly emerging from research. The idea initially came from Seth Lloyd from the MIT in 2008 when he devised the concept of quantum illumination. They rely on photons in the visible spectrum, and in three different ways:

- The radar emits classical photons in the visible and receives the photon reflected by the target. This does not work very well because of clouds and light noise surrounding the object.
- Radar emits photons but uses quantum photo-sensitive sensors to improve its performance. It does not work better enough.
- The radar prepares pairs of entangled photons. One is sent to the target and reflected and the other remains in the radar. The reflected photon is compared with the one that remained in place. As they have a common past, it is possible to sort the photons received by the radar to keep only the photons reflected by the target.



<sup>1592</sup> See [Scientists develop method to build up functional elements of quantum computers](#) by Far Eastern Federal University, February 2020, which refers to [Tailoring spontaneous infrared emission of HgTe quantum dots with laser-printed plasmonic arrays](#) by A.A. Sergeev et al, 2020 (10 pages). Quantum dot seems to be more suited for night vision than for quantum computing. It is not a source of single photons. And the words "computer" and "qubit" are absent in the article.

It is in fact a variant of the third way which is studied. It consists in converting the photons sent to the target into a radio wave photon, while preserving their quantum state. A conversion of the same kind takes place for the photon remaining in the radar. This allows the radar waves to pass through bad weather, what photons in the visible cannot do.

This technique is expected to improve the accuracy of traditional radars and to improve its resistance to noise and interference. This kind of radar could theoretically detect stealth aircraft, modulo the fact that their flat reflective surfaces reduce their radar signature whatever the radar frequency<sup>1593</sup>.

Entangled photons could also make it possible to effectively resist jamming systems. The first concepts saw the light of day in 2015<sup>1594</sup>. But there are some serious issues with noise and detection.

China is very interested in this technology and is working hard on it to be able to detect American stealth fighters or bombers like the F-22 and B-2. They announced a test of their first quantum radar in 2016, which was to become a prototype in 2018, produced by the government company **China Electronics Technology Group**<sup>1595</sup>, with a range exceeding 100 km.

Other labs and companies are developing such radars, such as the **Institute for Quantum Computing** at the University of Waterloo in Canada<sup>1596</sup>. This project is funded by the Canadian Department of Defence for \$2.7M. There are also some similar projects in Austria at the Institute of Science and Technology in Klosterneuburg. In the USA, **Lockheed Martin** is also invested in this emerging field.

This technology could also be used in LiDARs to verify that the inbound photons correspond to those emitted by its own laser, avoiding unwanted optical interference from other LiDARs. Without malicious interference, this will be very useful when many autonomous vehicles equipped with LiDARs will have to coexist on the road<sup>1597</sup>.

Specialists such as Marco Lanzagorta of the US Naval Research Laboratory believe that QKD satellites launched by the Chinese like Micius would have military applications of this type<sup>1598</sup>.

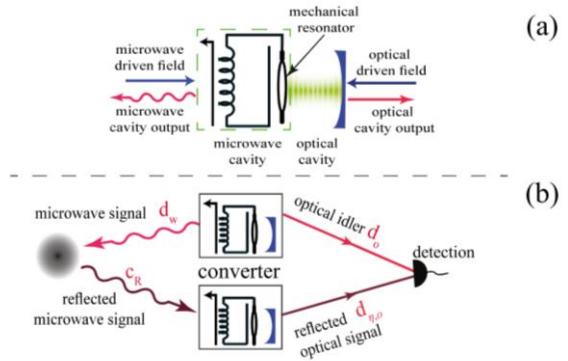


FIG. 1. (a) Schematic of the electro-opto-mechanical (EOM) converter in which driven microwave and optical cavities are coupled by a mechanical resonator. (b) Microwave-optical QI using EOM converters. The transmitter's EOM converter entangles microwave and optical fields. The receiver's EOM converter transforms the returning microwave field to the optical domain while performing a phase-conjugate operation.

<sup>1593</sup> See [Can quantum mechanics improve radar technology?](#) by Giacomo Sorelli and Nicolas Treps, November 2020. Which was maybe inspired by [Quantum Flashlight Pierces the Darkness With a Few Percent as Many Photons](#) by Adrian Cho, 2020.

<sup>1594</sup> See [Focus: Quantum Mechanics Could Improve Radar](#), 2015, [Microwave Quantum Illumination](#) by Shabir Barzanjeh et al, 2015 (5 pages) which is the source of the illustration FIG 1, and [Enhanced Sensitivity of Photodetection via Quantum Illumination](#) by Seth Lloyd, 2018 (4 pages).

<sup>1595</sup> See [China's claim of developing "quantum radar" for detecting stealth planes: beyond skepticism](#) by Ashish Gupta, 2016 (4 pages) and [The US and China are in a quantum arms race that will transform warfare](#) by Martin Giles, MIT Technology Review, January 2019.

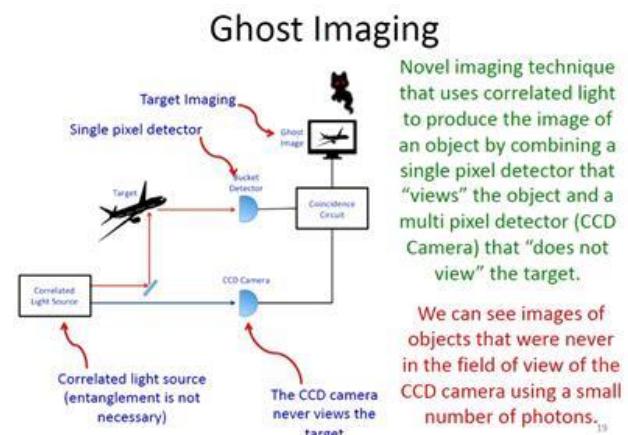
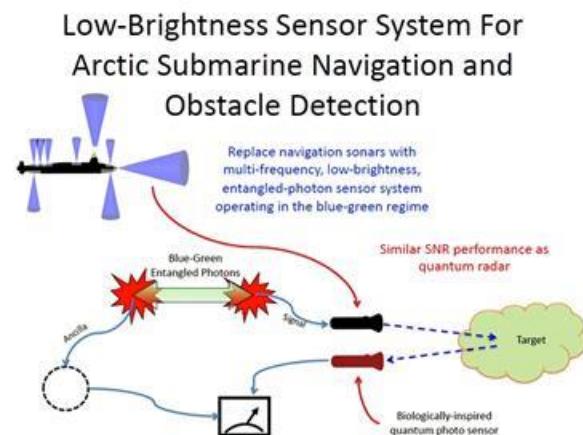
<sup>1596</sup> See [Quantum radar will expose stealth aircraft](#), April 2018.

<sup>1597</sup> This approach has been studied since at least 2009. See [Quantum Lidar - Remote Sensing at the Ultimate Limit](#), 2009 (97 pages).

<sup>1598</sup> See [The Future of Quantum Sensing & Communications](#) by Marco Lanzagorta of the US Naval Research Laboratory (USA), September 2018 (37 minutes). I have extracted two illustrations from this page of the video of his intervention (on sonars and ghost cameras). He is the author of the book [Quantum Radar](#) which has been translated into Chinese by China, and officially bought the rights.

In a domain close to radar, quantum sonar could also emerge, so to speak. They use photons in the blue-green zone of the visible spectrum and would be usable for navigation in the Arctic Ocean.

It would be a kind of quantum LiDAR. These systems could also implement optical communication with submarines via satellite, to replace radio waves that do not penetrate underwater well and are exploitable for very low-speed links.



Another envisaged technique is the generation of ghost images, generated by a system coupling a camera that does not see the object to be captured and a single pixel sensor that sees the object. This kind of technique can be based on the entanglement of photons in the visible between the two sensors.

On the other hand, one day, it may be necessary to find countermeasures against "quantum" coatings that allow the infrared signature of objects to be removed or reduced<sup>1599</sup>.

## Quantum chemical sensors

Quantum sensing is also applicable with chemical sensors used to analyze the chemical composition of various materials and substances. It is commonly used with optical interferometers<sup>1600</sup>.



**Entanglement Technologies** (2010, USA) is a spin-off of Stanford and Caltech that offers the AROMA (Autonomous Rugged Optical Multigas Analyzer) quantum gas detector that uses lasers and optical resonators similar to those used to detect gravitational waves in the LIGO, with a spectroscopy technique (CRDS: Cavity Ring-Down Spectroscopy). In particular, it allows the detection of dangerous gases in industry, especially in the extraction of fossil fuels. They were funded by EDF, via their Environmental Defense Fund.



**Oxford HighQ** (2017, UK) is a spin-off from the University of Oxford developing chemical and nanoparticles sensors using optical microcavities.

<sup>1599</sup> See [Camouflage made of quantum material could hide you from infrared cameras](#) by Kayla Wiles, December 2019 which refers to [Temperature-independent thermal radiation](#) by Alireza Shahsaf et al, September 2019 (17 pages).

<sup>1600</sup> See [Quantum Optical Technologies for Metrology, Sensing, and Imaging](#) by Jonathan Dowling, 2014 (20 slides) and [Advanced Micro- and Nano-Gas Sensor Technology: A Review](#) by Haleh Nazemi et al, 2019 (23 pages).

## Quantum NEMS and MEMS

Nano or micro electromechanical structures are widely used in long-connected objects, such as accelerometers. They use many quantum phenomena, notably photonics-based, with mechanical resonators whose motion is analyzed by lasers and diodes.

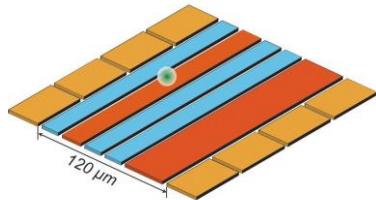


At the heart of a new NIST portable pressure sensor is a dual cavity for laser measurements that is only 2.5 cm long.

### Reversible Quantum Squeezing NIST

#### Improving Measurement of Ultrasmall Motions

- 7X more precise than previous methods
- A single magnesium is manipulated in an ion trap made with sapphire base and gold electrodes
- Boost sensitivity in quantum sensors & speed up process for quantum entanglement



<https://www.nist.gov/news-events/news/2019/06/nist-team-supersizes-quantum-squeezing-measure-ultrasmall-motion>

27

They are found in quantum pressure sensors<sup>1601</sup> and motion detectors, both from NIST (*above*<sup>1602</sup>). Other sensors are used to detect electrical resistance, temperature, mass and force, vacuum or voltage<sup>1603</sup>.

Finally, let's mention the European Quantum Flagship project **macQsimal** (Switzerland, €10.2M) or "Miniature Atomic vapor-Cells Quantum devices for SensIng and Metrology Applications", for the creation of quantum sensors aimed at the market of autonomous vehicle piloting and for medical imaging. This includes the creation of atomic clocks, gyroscopes, magnetometers, imaging systems using microwaves and electromagnetic fields in the tera-Hertz waves as well as gas detectors. In short, a fairly generalist approach. It is based on the use of cold atom vapor integrated in MEMS, a technique that Thales is also using.

## Radio frequencies sensing

Radio frequency analysis is an old subject but it is also progressing thanks to quantum technologies often associating optronics with cold atoms.

<sup>1601</sup> See [FLOC Takes Flight: First Portable Prototype of Photonic Pressure Sensor](#), February 2019.

<sup>1602</sup> See [Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact](#), 2019 (39 slides).

<sup>1603</sup> See [Quantum electro-mechanics: a new quantum technology](#) by Konrad Lehnert from NIST JILA lab (47 slides) and [From micro to nano-optomechanical systems: light interacting with mechanical resonators](#) by Ivan Favero (45 slides).

This often reaches extremes dimensions such as this recent quantum sensor based on alkaline Rydberg atoms which can analyze the radio spectrum from 1 kHz to 100 GHz<sup>1604</sup> or this other quantum sensor analyzing radio waves in the 1 THz band, intermediate between infrared and microwaves, with potential applications in the measurement of thickness of thin layers of heterogeneous materials<sup>1605</sup>.

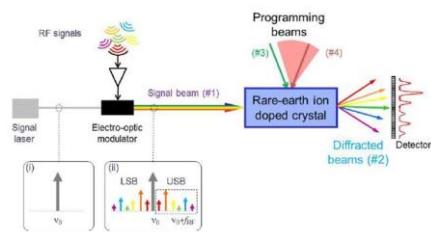
**Thales** is also developing frequency analyzers with a bandwidth of 0 Hz to 20 GHz based on rare earth-doped crystals.

NV centers can also help run RF signals spectral analysis, from 0 to 40 GHz.

## RF spectrum analyser

### Spectral Hole burning

- TRT / LAC
- Rare-earth doped crystals
- bandwidth: 20 GHz



## Quantum sensing key takeaways

- Quantum sensing is the most mature and underlooked market of quantum technologies.
- Quantum sensing enables better precision measurement of nearly anything: time, distance, temperature, movement, acceleration and gravity, magnetism, light frequency, radio spectrum and matter chemical composition.
- Quantum sensing has been extensively used to update the new metric system put in place in 2019.
- Lasers and the frequency combs technique is used to measure time with extreme precision, beyond atomic cesium clocks. It is based on blocked-mode lasers generating very short pulses, aka femtosecond-lasers.
- The most used quantum sensing technology is based on NV centers. It help measure variations of magnetism and has applications in many domains like in medical imaging and non-destructive control.
- Another one is cold atoms based interferometry that is implemented in micro-gravimeters. It can also be used to analyze the radio frequency spectrum.
- China supposedly built some quantum radars using photons entanglement and up/down converts between visible photons and radar frequencies but the performance is driving a lot of skepticism in the Western world.

<sup>1604</sup> See [Scientists create quantum sensor that covers entire radio frequency spectrum](#) by The Army Research Laboratory, March 2020 and [Quantum sensor for entire radio frequency spectrum](#), March 2020 which reference [Assessment of Rydberg atoms for wideband electric field sensing](#) by David H Meyer et al, January 2020 (16 pages). See also another less impressive performance from the same lab and published later: [Waveguide-Coupled Rydberg Spectrum Analyzer from 0 to 20 GHz](#) by David H. Meyer, 2021 (10 pages).

<sup>1605</sup> See [Researchers demonstrate first terahertz quantum sensing](#), March 2020, which refers to [Terahertz quantum sensing](#) by Mirco Kutas et al, 2020 (9 pages).

# Quantum technologies around the world

Quantum computing in the broadest sense is a strategic technology domain for various reasons. In cryptography, states sovereignty is at stake with the protection of sensitive communications. Quantum computing has critical applications that will extend the scope of digital computing beyond what is feasible today, particularly in the fields of healthcare, the environment and artificial intelligence.

In terms of maturity, quantum and post-quantum cryptography represent more established fields with economic players and commercial solutions, even if the standardization of post-quantum cryptography is not yet complete. However, it has fewer scientific and engineering unknowns compared to scalable quantum computing.

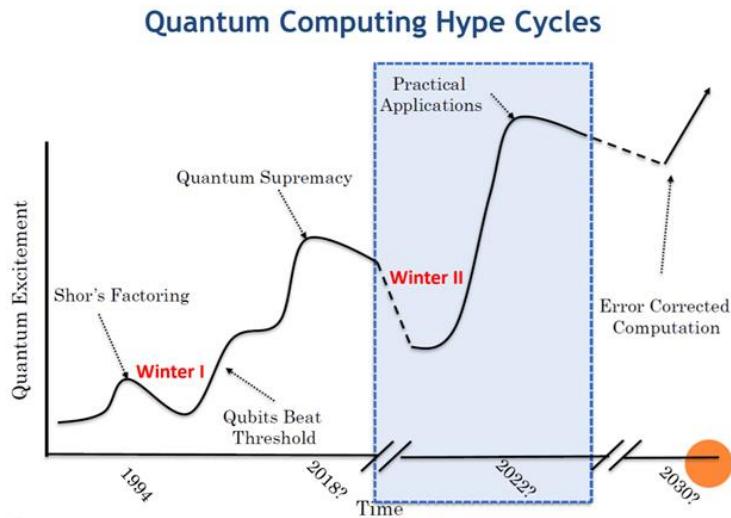
Quantum computing is much less mature. The feasibility of commercially and useful quantum computers remains an open question. There are significant technological challenges to overcome, including the thorny issue of qubits noise, quantum error correction, and how to scale the number of physical qubits by several orders of magnitude. So, quantum computing is full of scientific and technological uncertainties even before being economical and market ones. How countries deal with that is a good revelator of their innovation and forward-looking culture.

For the time being, fundamental research is mainly funded by governments in most countries, then from very large IT players who entertain many technology bets in parallel (IBM, Google, Microsoft, Intel, Honeywell, Alibaba), and a more or less well-funded startups, mainly in North America (D-Wave, IonQ, Rigetti, PsiQuantum, Xanadu) and, way behind, in Europe (IQM, OQC, Pasqal) and in other regions (SQC in Australia, Quantum Machines in Israel, etc).

The quantum computers software industry is in its infancy. The major players and startups creating quantum computers have all invested the software arena, starting with the low-level supporting tools and sometimes, for developing quantum applications. Some systems are already available in the cloud, directly or through cloud services provided like Amazon, Microsoft and Google. Most of these and Atos also sell cloud access to classically run quantum emulators.

One way of looking at things is coming from **Yuri Alexeev** of the Argonne National Laboratory in the USA, who draws a parallel between the history of quantum computing and that of artificial intelligence and anticipates the arrival of two winters, the first which occurred in the late 1990s, the second he expected in 2020 and the next around 2030<sup>1606</sup>.

Since this excitement is a somewhat fuzzy wave function and difficult to evaluate, it doesn't mean much. We can however anticipate at least a small winter with the startups of the sector and large customers engagements. Hardware startups will have a hard time delivering useful machines, while software startups will not have a large enough addressable market due to the lack of hardware. But this will not prevent public research laboratories and large tech companies from doing fundamental and applied research.



<sup>1606</sup> See [Quantum Computing Trends](#) by Yuri Alexeev, August 2019 (42 slides).

## Quantum computing startups and SMEs

Mapping these vendors is a bit easier than in other deep techs like in artificial intelligence because there are not so many. There are many methods to inventory worldwide quantum startups and small businesses. I have accounted about 450 such companies, more than the 265 I had in store in September 2020 and their total funding is about \$4.7B as of October 2021.

The increment comes mostly from existing quantum enabling technologies companies that I uncovered. I added them when and if I found that they were enabling “second quantum revolution” solutions. So metal cutting lasers and classical telecommunications photonics are out!

This ecosystem began to take shape even before quantum computers were working on a small scale. It is fascinating to discover startups that make long-term bets, particularly with hardware. Software startups rely on a still limited hardware infrastructure but often reduce their risks by also supporting traditional computing architectures like Nvidia GPGPUs in machine learning. Their customers are large companies who test algorithms on a small scale to get their hands on quantum programming, often on D-Wave annealers and sometimes with IBM who is very pushy in its quantum evangelism efforts. To date, no application seems to have been deployed in production. We are therefore in the field of applied research and small scale prototyping within client companies. The software ecosystem is to be monitored closely. It will probably expand once hardware works on a larger scale, particularly with NISQ computers and quantum simulators<sup>1607</sup>.

For their part, quantum cryptography systems are operational and correspond to a very separate market, just like the quantum sensing market that is more mature technologically but still in its infancy.

The stakes for many startups in this field are common with those of deep techs: how to develop real products with economies of scale, how to expand internationally rapidly, how to avoid falling into models that are too "service-oriented" and at last, how to resist what some people are already calling the quantum winter. Enabling technologies niche companies (photon sources, cryostats, ultra-vacuum, various sensors, electronics) can do well by reaching out diversified markets, notably targeting several different branches of research, telecommunications, military or aerospace applications.

### Investors

Quantum technologies investments may be impressive for the large rounds like those from PsiQuantum and IonQ and the associated “FOMO” factor (“*fear of missing out*”). But it’s still small in volume in the technology sphere. The first investment funds more or less specialized in quantum technologies have already emerged with:

- **Quantonation**, a French seed fund created by Charles Beigbeder and managed by Christophe Jurczak, a physicist who got his PhD with Alain Aspect. They have already invested in over a dozen startups<sup>1608</sup>. They organize quantum meetups and hackathons in Paris (with **QuantX**, the quantum alumni association from Ecole Polytechnique), the first edition having taken place in October 2018. It participated to the launch **Le Lab Quantique**, which was jointly created with **Bpifrance**. It is federating the country vendors and users quantum ecosystem.

---

<sup>1607</sup> See [Some Teams Go For NISQ-y Business Some are NISQ-Averse](#) by Doug Finke, February 2020.

<sup>1608</sup> Quantonation invested in LightOn (France), Spark Lasers (France), which offers laser sources not specifically dedicated to quantum computers, Pasqal (France, cold atoms), Quantum Benchmark (Canada, software), Kets Quantum Security (UK, QKD component), Orca Computing (UK, hardware, photonics-based computing), CryptoNext Security (France, PQC), Qunnect (USA, repeaters for QKD), Quandela (France, photon source), Qubit Pharma (molecular simulation), Qnami (Switzerland, NV center-based metrology), Orca Computing (photon qubits, UK), Foqus (Canada, quantum sensing software), Qu&Co (Netherlands, software) and QPhoX (Netherlands, communications between quantum computers).

- **Quantum Valley Investments** (QVI), a \$100M Canadian investment fund, raised in 2013, dedicated to quantum technologies. Their founders had invested in 1984 in Blackberry / RIM. They do not disclose their investments, except in ISARA Corporation, part of which are spin-offs from the Canadian research laboratory Institute for Quantum Computing at the University of Waterloo in Ontario.
- **Quantum Ventures** is a quantum investment company launched in 2016. Its "Quantum Revolution Fund" is managed from London and Switzerland. It aims to raise €100M.
- **Quantum 1 Group** is an American investment fund specializing in quantum technologies since 2015.
- **Summer Capital** is a Dutch investment fund specialized in quantum technologies, data and finance. Their investments include Horizon Quantum Computing, Rigetti and Turing.
- **Phystech Ventures**, previously Quantum Wave Fund, created by Russians in Silicon Valley and having already invested in the IDQ and Nano-Meta Technologies. Their fund is not 100% specialized in quantum. They also invest in robotics, drones, sensors and connected objects.
- **Parkwalk Advisors** is a British deep tech fund. As of 2021, they have invested in Phasercraft, Quantum Motion Technologies, Riverlane, nu quantum, nu nano and Oxford Quantum Circuits. This fund is part of IP Group Plc since December 2016.
- **Machine Capital**, a UK fund focused on quantum and AI, which has so far invested in **QuantumX Incubator**, an incubator for quantum software projects launched jointly with **Cambridge** startup **Quantum Computing**, which specializes in the development of quantum software, with a 20-week incubation period.
- **SpeedInvest** is an Austrian investment fund specializing in deep tech start-ups, which invests among others in quantum technologies. They invest in seed stage with up to 1M€. They have invested in QPhoX and Kets.



**The Quantum Daily** produced in early 2020 an [inventory of investors](#) in quantum technologies startups. Here is an excerpt with general and specialized VC investors. It contains a few mistakes such as Worldquant which is positioned as an investor specialized in quantum technologies whereas it is a generalist investment company created in 2007. The use of the word quantum or a piece of quantum is not a guarantee of specialization.

	Generalist VCs	Generalist early stage	Deep Tech	AI / ML / Computation	Specialist QC	
Americas	a16z Battery Georgian Partners DFJ GrowthWorks KENSINGTON	SEQUOIA USA TUTTER HILL VENTURES Canaan Capital atomico GFC NEA Redpoint Sierra Ventures SOCIALCAPITAL VENROCK JEREMY BROOK OMERS   Ventures	1517 8VC AE ACME KEC VENTURES New GridVentures octopus ventures b2v eQventure UC MANTARAY global brain	Amplify Partners CANTOS VENTURES boostVC DC RisingTide Redpoint Sierra Ventures SOCIALCAPITAL VENROCK JEREMY BROOK OMERS   Ventures	Morado Ventures AME CLOUD VENTURES playground OpenOcean streamlined ventures Pathfinder VANEDGE AI SEED	Quantum Ventures WORLDQUANT Quantum Valley Quantum Group
EMEA	Amadeus Capital Balderton Capital High-tech Buntferndes MTG pitango	b2v eQventure UC MANTARAY global brain	Apex Fluxus Ventures MAKI.VC VITO VENTURES Martlet	FLUXUS VENTURES IQ CAPITAL PIV ENTREE CAPITAL	Alpha Intelligence Capital	Quantonation SUMMER CAPITAL
APAC	anrl Golden Gate Ventures SBI Holdings Square Peg			Abies main sequence ventures		Latent

Investment in startups started to take off worldwide from 2016 onwards as shown in the following chart<sup>1609</sup>.

## Startup maps

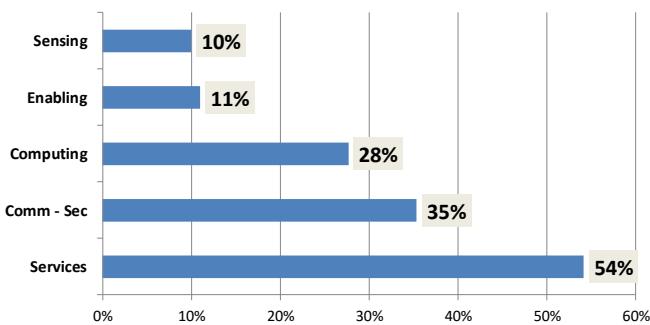
An inventory of quantum startups is available on the [Quantum Computing Report](#) website. It allowed me to identify a good number of the startups mentioned in this section. Some startups spread so little information about them that one may wonder if they are not scams. This lack of communication may simply be due to the fact that many creators may be uncommunicative researchers, that they are poorly funded, and that their projects have business prospects that are too remote and risky. Also, many times, they are so early-stage that they can't talk about anything that would drive interest, such as "*I have two functioning qubits*".

Many of the startups mentioned here are not yet in the "pure" form of the startupian model, i.e. they are far from having a scalable model or even, just a product. They are often either industrial small businesses targeting very low-volume niche markets, or startups where the scientific and technological risk is still very high before they can sell anything. And often, with a combination of both. They can then finance themselves with contract research and various consulting services for large companies or public institutions.

In the vast majority of cases, I relied on public information available on the Internet to describe what these startups do in the various parts of this ebook. One way to find out what these startups do is to identify their founders, if they are researchers, and find their original laboratories, their past scientific publications, and their PhD thesis if it is available. Finally, search for possible patents filed by the startups. This is technology intelligence using open-sourced information (OSINT). You of course can also meet with entrepreneurs, live or distantly.

This mapping also does not include companies that seem to offer only service and consulting in quantum computing, without having their own technology or products<sup>1610</sup>.

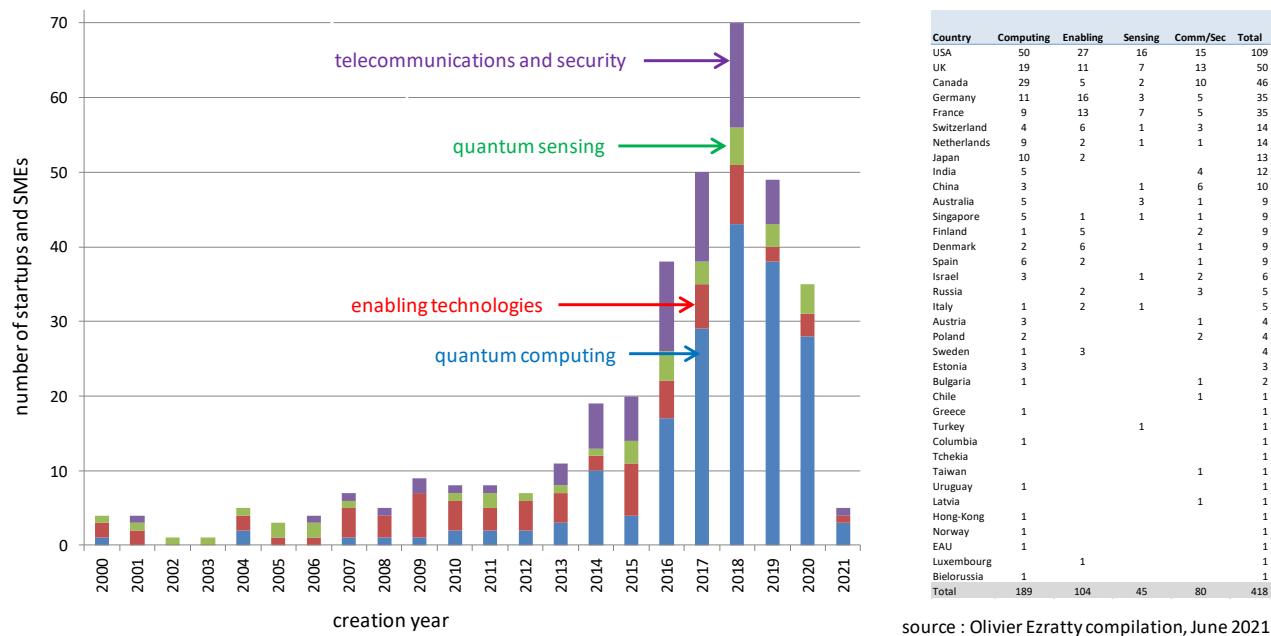
share of quantum startups and small businesses whose name start with a Q



fun fact: in some fields like telecommunications, cryptography and consulting services, quantum startups branding shows a lack of creativity with many names starting with a Q.

<sup>1609</sup> See [European Seed Investment: Quantum Applications](#) by Patrick Gilday, April 2019.

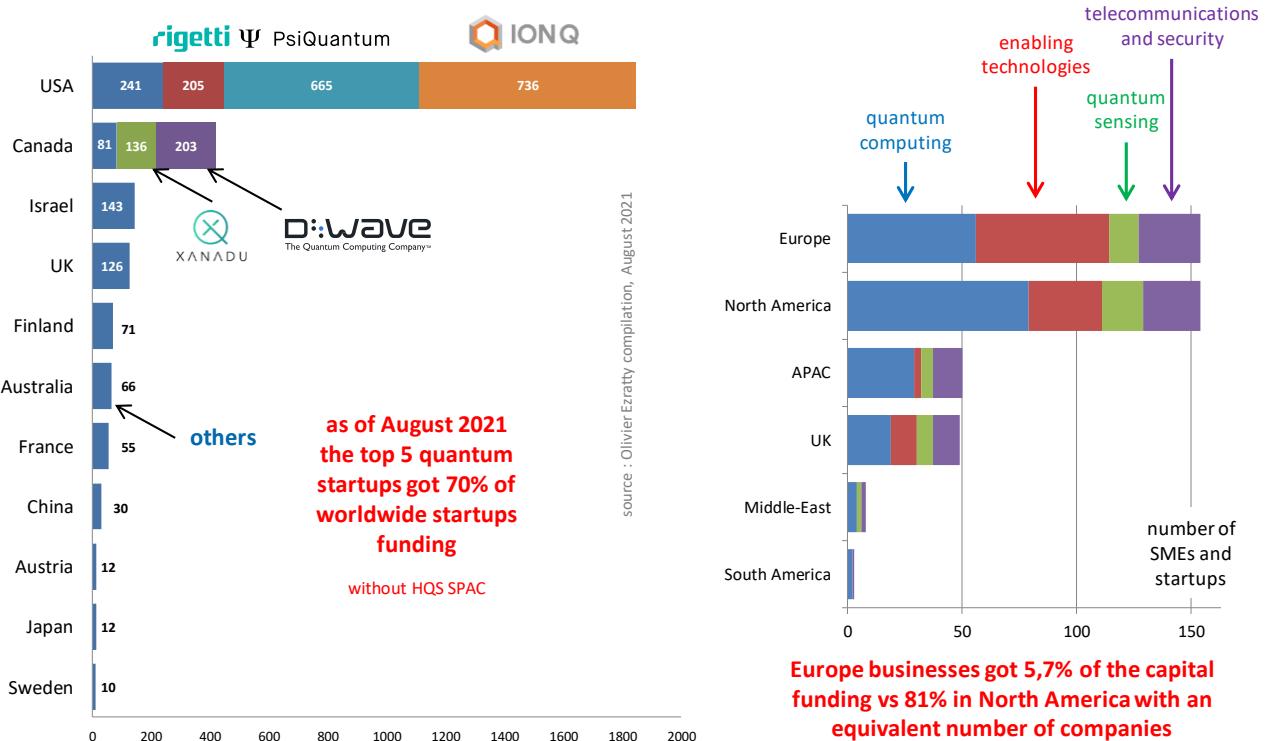
As far as data is concerned, here are some charts extracted from my database of startups and SMBs. The first one provides an indication of the number of startup creations per year. The second provides a breakdown by country. Of course, other sources will publish different charts!



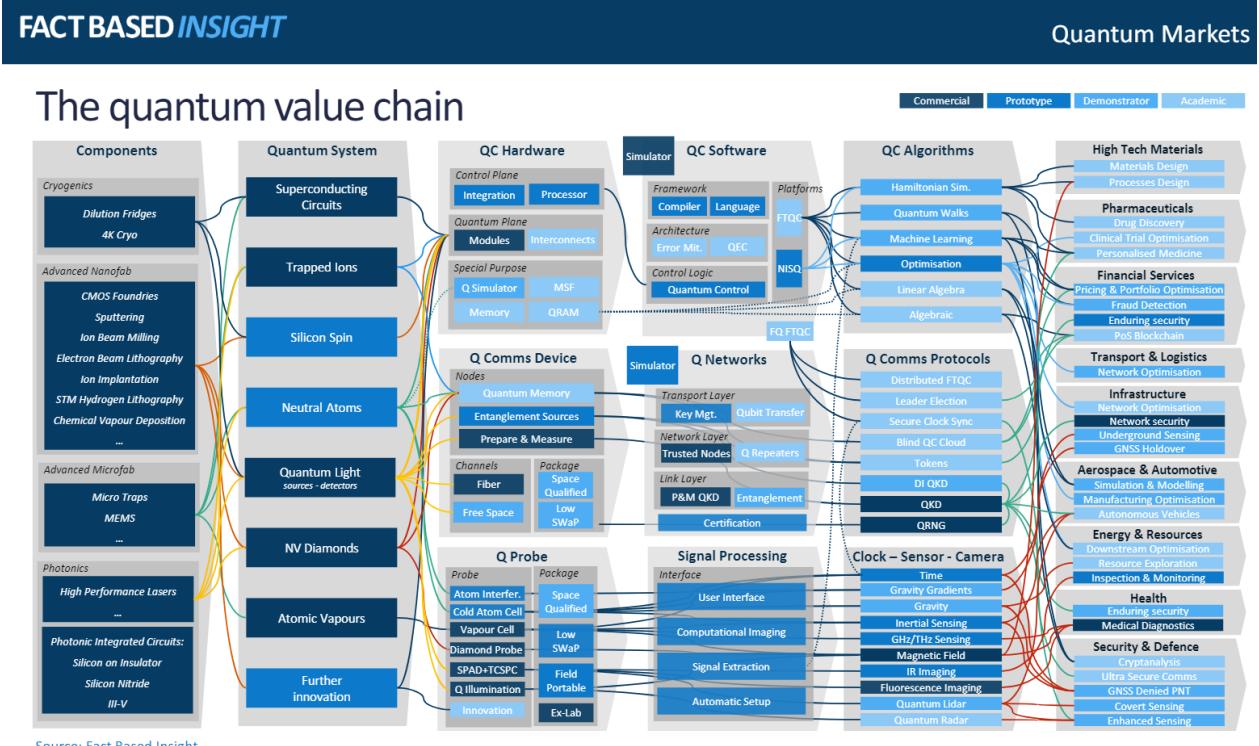
And in this third diagram, a different breakdown by country that highlights the largest funding. As usual, we see a significant financing gap between North America and Europe. One of the reasons is that European startups were created later or are more traditional small business which don't rely on venture capital for their development<sup>1611</sup>. The other is of course a different access to capital. And 68% of worldwide startups funding went to the top 5 startups: IonQ, PsiQuantum, Rigetti, D-Wave and Xanadu, all from the USA and Canada, while Europe has an equivalent number of companies compared to North America. If there are as many quantum startups and small businesses in mainland Europe than in North America, their visible equity funding represents only 5,7% of worldwide funding while North American companies got a hefty 81%. And this doesn't include the investments from IBM, Google, Intel and Honeywell.

<sup>1610</sup> Here are some examples of quantum services and consulting companies throughout the world: **Safe Quantum Inc** (2020, USA) sells PQC services, **D-fine** (2002, Germany), **Q&I** (UK) also called Qandi, **QuantGates** (UK), **Quantum Phi** (Czech Republic). **RayCal** (UK) which is an analyst firm in quantum technologies, **Inside Quantum Technology** (2018, UK) created by Lawrence Gasman with the help of 3DR Holdings, **Qureca** (Spain) whose name means Quantum Resources & Careers and which does training, recruitment, business development and events, **Max Kelsen** (Australia), **Quantum Quants** (Netherlands) and **Unitary Zero Space** (Finland). **SoftServe** (1993, Ukraine), **StrategicQC** (USA) is also specialized in recruiting talent in quantum technologies. **Quantum Computing Engineering** (USA) or QCE, provides generic consulting services on quantum computing. **Aspen Quantum Consulting** (USA) does due diligence investigation of startups for investors. **AmberFlux** (2013, India) provides quantum computing consulting services on top of existing machine learning and data science services. **QRDLab** does about the same, also in India. **Quemix** (2019, Japan) is an IT company specialized in providing quantum computing solutions. **QuRISK** (2021, France) does consulting on quantum computing originated risks on cybersecurity and **Q. BPO Consulting** (2020, France) seems to be a generalist quantum computing consulting shop. **ColibrITD** (2021, France) is a technology consulting shop also providing some services in quantum computing. At last, **Reply Data IT** (Italy) is a quantum computing service company that deployed its custom MegaQUBO solver in the cloud, first on classical computers, and supposedly on quantum computers by the middle of 2021.

<sup>1611</sup> See [New record looms in VC funding of quantum startups](#) by Michel Kurek, September 2020 and [The European Quantum Computing Startup Landscape](#) by Alex Kiltz, October 2020.



**David Shaw** from Fact Based Insight (UK) created a very complete map of all quantum technologies in the global quantum ecosystem chart below<sup>1612</sup>. We cover most of these companies in different parts of this book, split between quantum computing (page 239), enabling technologies (page 361), software (page 566), telecommunication and cryptography (page 631) and sensing (page 644).



<sup>1612</sup> See [Quantum Value Chain Overview](#), by David Shaw, Fact Based Insight, April 2021.

## Quantum Startup incubation and acceleration

There are already a few incubation and acceleration programs for deep tech startups which host quantum startups in the world. One of the most famous is the **Creative Destruction Lab**, based in Toronto, Canada. **Xanadu** and **North** came out of it. Similarly, **Unit DX** is a deep tech incubator based in Bristol, UK, which started in the biotech industry and also helped some quantum startups<sup>1613</sup>. **Duality** is a quantum dedicated startup accelerator in the USA with a sponsorship from Amazon. **Quantum Startup Foundry** is the University of Maryland accelelatator. In France, the **HEC Challenge+** program and the **Deeptech Founder** program created by the team behind the deep tech Hello Tomorrow event, accelerated a big share of France's quantum startups like Quandela, Pasqal and Alice&Bob. To create such acceleration programs, you need to be close to critical mass pool of talents, such as a dynamic academic and research zone.

## Global investments

What about global investments in quantum computing? A [2015 McKinsey](#) study provided an overview of investments that likely compiled public research budgets. At that time there were 1500 researchers worldwide with a total budget of \$1.5B. This number has since increased much although there are no new inventory being made. The USA and China were obviously leading that space. But the distribution of these investments, which probably include both quantum cryptography and quantum computers, is intriguing for other countries. As usual, Europe was fragmented with Germany, France, The Netherlands, Finland, Italy, Spain, the United Kingdom (then, in the European Union) and Switzerland (geographically in Europe). And we have strong quantum countries in other regions like Canada, Japan, Singapore and Australia.

A European study produced in 2016 used the same figures and added the number of employees. With 224 researchers in France compared to 1,217 researchers in the USA, which is a normal ratio of 1 to 6. However, it is difficult to distinguish between those who do research in fundamental physics and those who develop qubits, so it is difficult to count the number of these researchers. Most importantly, these numbers are beginning to date and seem largely understated. In France, we have at least 300 full time researchers on quantum technologies plus at least an equivalent number of docs and post-docs.

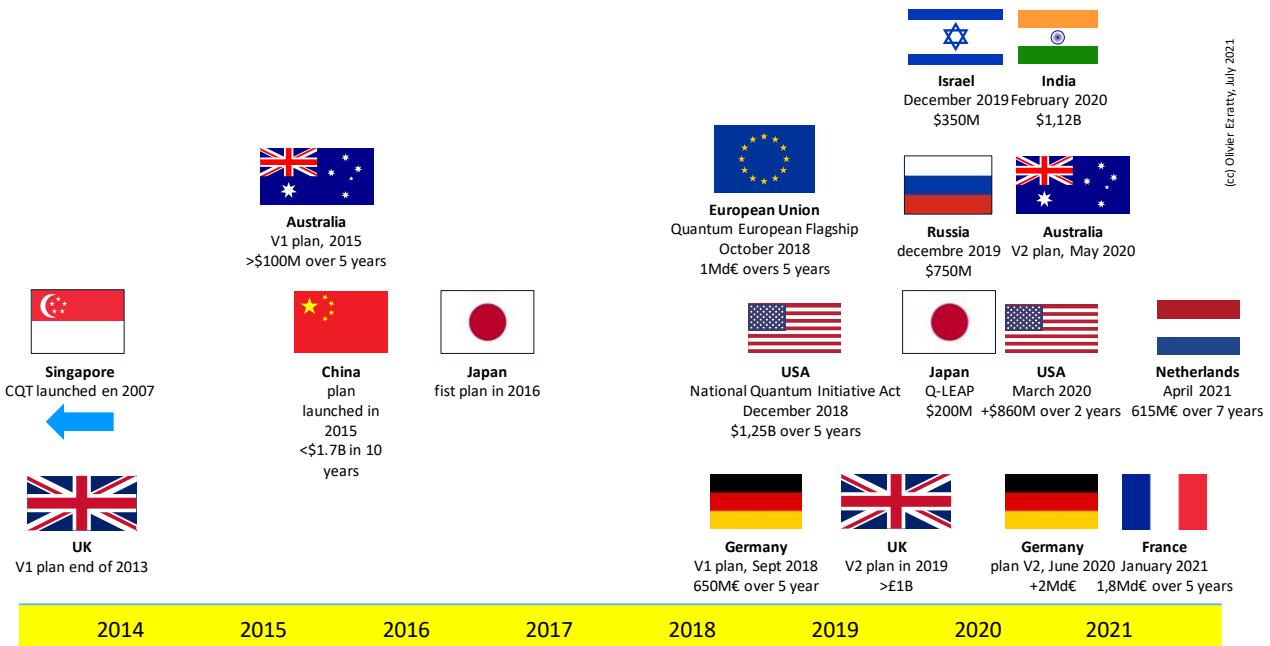
Quantum technologies have become a geopolitical issue, almost like nuclear deterrence<sup>1614</sup>. The public authorities in these different countries have mobilized in very different ways on quantum. Most developed countries governments coordinate efforts in the quantum field. Plans with up to \$2B over 5 or 10 years periods have been announced here and there. It's still quite difficult to compare these investments between countries and for a couple reasons:

- What is the **existing run-rate investment**? It's sometimes not easy to capture this data, particularly with highly decentralized research like in the USA and most European countries.
- What are the **undisclosed investments** in military and intelligence? It may be high in the USA and Russia. But lower in Europe, given these countries don't allocate a great share of their GDP to military expenses.
- Is the publicized funding **incremental** or including existing investment? You can easily embellish things with the latter accounting method.
- Are some countries **overinflating** their investment? This is a hypothesis for China's investments which have been highly confusing. We provide as accurate data for this regard here.

---

<sup>1613</sup> See [Incubators & Accelerators: Launchpads For Quantum Success?](#) by James Dargan, 2020.

<sup>1614</sup> See [Quantum, AI, and Geopolitics \(3\): Mapping The Race for Quantum Computing](#) by Hélène Lavoix, December 2018.



An evaluation of scientific publications in quantum computing done by **Insead students** in 2018 did show with no surprise to discover that the USA, Canada and China are the first countries to publish<sup>1615</sup>.

A more detailed analysis was produced by **Michel Kurek** in September 2020 (sources of the illustrations *below*) which did help relativize the influence of Chinese publications<sup>1616</sup>. Indeed, the Citations Per Publications is very low in China and also India, compared all Western countries.

COUNTRY	TP	%TP	TC	%TC	CPP	RCI	%ICPEI
1  USA	4,295	26.4%	108,128	44.8%	25.2	1.7	70%
2  China	3,706	22.8%	38,611	16.0%	10.4	0.7	44%
3  UK	1,428	8.8%	32,435	13.4%	22.7	1.5	120%
4  Germany	1,400	8.6%	38,339	15.9%	27.4	1.9	123%
5  Japan	1,106	6.8%	20,996	8.7%	19.0	1.3	99%
6  Canada	1,056	6.5%	23,104	9.6%	21.9	1.5	124%
7  India	991	6.1%	5,847	2.4%	5.9	0.4	33%
8  Australia	777	4.8%	20,777	8.6%	26.7	1.8	130%
9  France	699	4.3%	14,016	5.8%	20.1	1.4	117%
10  Italy	635	3.9%	10,522	4.4%	16.6	1.1	116%
Total 10 countries	16,093	98.9%	312,775	129.5%	19.4	1.3	83.1%
Total world	16,279		241,536		14.8		

\*TP= Total Publication ; TC = Total Citation ; CPP = Citation par Publication = TC/TP ;  
RCI = Relative Citation Index ; ICPEI = International Collaboration Publication Extended Index

<sup>1615</sup> See [VC investment analysis Quantum Computing](#), April 2018 (18 slides).

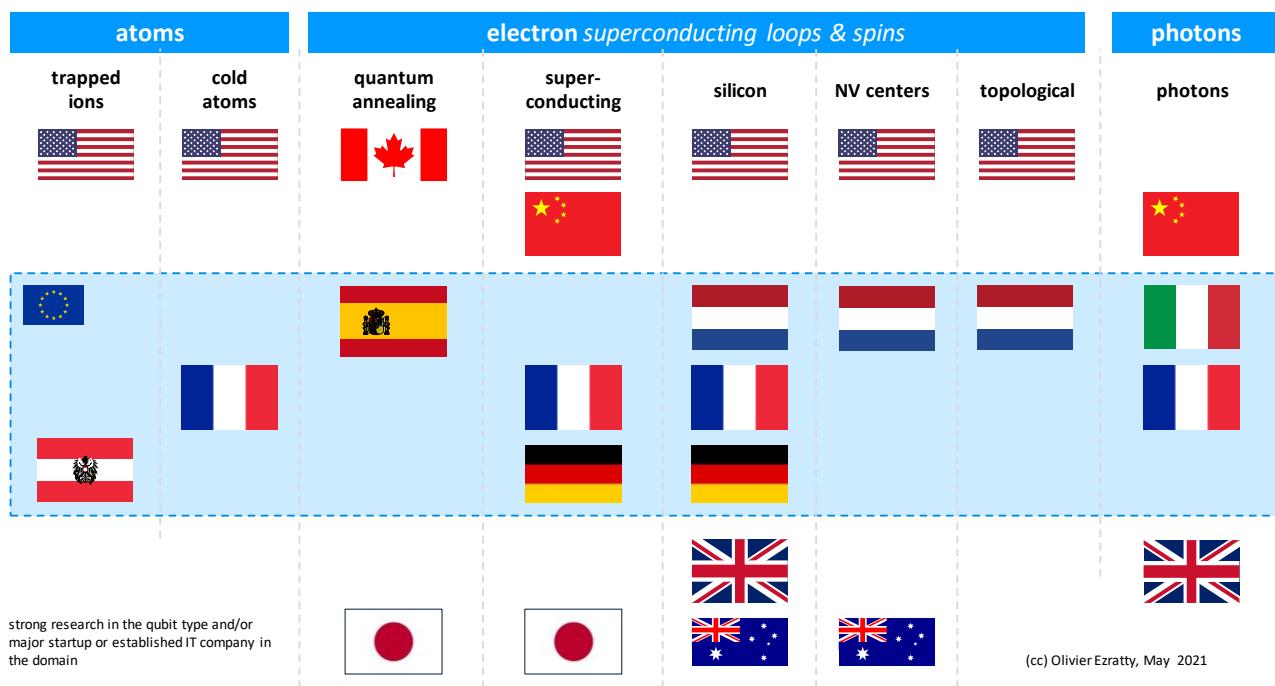
<sup>1616</sup> See [Quantum Technologies : Patents, Publications & Investissements Landscape](#) by Michel Kurek, September 2020 (52 pages).

The significant investments made by developed countries in quantum technologies raise fears that computing power could end up being concentrated in the hands of a few or even a single country or company. I don't believe this, at least not in the initial phase of development of these technologies. Knowledge on the subject is highly distributed, as are enabling technologies and strategic materials. I would rather situate the risk of concentration in a second phase of the maturation of this market, one that will see a market that was initially fragmented with many players concentrating through consolidation. It will probably do so for reasons that are more macro-economic than scientific or technological, through economies of scale and the platforming of offers. This explains why it is necessary to simultaneously keep an eye on the hardware, development tools and software applications of quantum computing.

Once the main scientific and technological uncertainties are lifted, the success of each company and country will depend on the classic key success factors of technology ecosystems: execution speed, teams quality, funding levels, communication, marketing, sales, the ability to promote technology platforms to a maximum number of players and on a global scale. This is where sovereigntist approaches combining protectionism of key players while ensuring maximum trade openness to the world to enable them to achieve economies of scale will have to be carefully adopted.

We'll go through the details, country by country, continent by continent. With one exception, Africa, which is little invested in the subject, at least as a producer of quantum technologies, maybe besides South Africa which seems to have started to get involved in the academic side<sup>1617</sup>.

This summary shows which country best masters quantum computing technology per qubit type. All in all, we have a good balance between the USA and the European Union, although the USA have the benefit from having large IT vendors invested in the field in superconducting (Google, IBM), silicon (Intel), trapped ions (Honeywell, IonQ) and topological qubits (Microsoft).



What are the key success indicators of success for countries investing in the quantum race?

<sup>1617</sup> See [Will Africa miss the next computational revolution?](#) by Amira Abbas, April 2020.

We'll probably have some analyst shops create their own quantum sort-of Shanghai ranking using composite metrics: public funding, scientific publications, patents and the likes, entrepreneurship spirit, number of startups, startups funding, large companies investments, corporate adoption, skilled workforce and else. Guess what? US and China will probably rank first there. And smaller countries behind in some variable order. But what if Europe was consolidated?

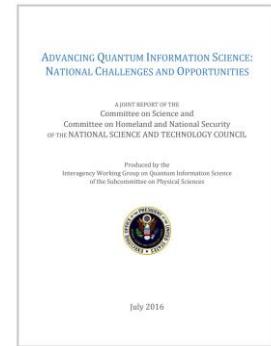
## North America

### USA



Whatever the metric you use, the USA is leading the world in quantum technologies. They mix three components no other country or region has: a powerful Federal government investing significant amounts in fundamental research, large IT companies investing a lot as well in research and industrialization and a healthy well-funded dense startup ecosystem.

The coordination of research in the different branches of quantum physics started in October 2014, the White House produced two reports<sup>1618</sup>. It was not a plan but rather an inventory of what existed. Like almost all countries, quantum technologies were segmented in four quantum communication, sensing, computing and simulation. In 2017, lobbying from the industry and research started to push the federal government to launch a national quantum plan. It started with U.S. House of Representatives organizing a hearing in October 2017 ([video](#)). For three hours, elected officials questioned a panel of scientists including James Kurose of the NSF and John Stephen Binkley of the Department of Energy, who explained the basics of qubits and the associated sovereignty issues.



The Democrats were concerned about the Trump administration's proposed cuts in funding for civilian research in favor of defense budget increases and tax cuts. But the US Congress increased federal research budgets for fiscal year 2018 and beyond ([source](#)), knowing that these budgets are then traditionally channeled mainly to American universities research laboratories. This is one of the few cases where the Republican-controlled Congress opposed the Trump administration. This happened consistently throughout all fiscal years of the Trump administration and will probably happen again with the Biden administration.

### National Quantum Initiative Act

Then came the National Quantum Initiative Act that was first proposed on June 26, 2018 by the House of Representatives Science Committee ([H.R. 6227](#), 25 pages). An equivalent proposal was done by the Senate on the same day. This project was the result of a proposal, the [National Quantum Initiative-Action Plan](#), prepared by public and private research stakeholders (IBM, Google, Rigetti).

An intense lobbying campaign was carried out by several professional associations<sup>1619</sup>, with the **National Photonics Initiative**, a professional association bringing together photonics physicists and industrialists in the sector, accompanied by the lobbying firm **BGR Group**.



<sup>1618</sup> The report [Advancing Quantum Information Science: National Challenges and Opportunities](#), July 2016 (23 pages) was followed by a [working meeting](#) in October 2016.

<sup>1619</sup> See [Quantum computing finds its lobbying voice](#) by Aaron Gregg, Washington Post, June 2018.

This association, which wanted to make photonics a priority, was launched in 2012. It is sponsored by other entities: The Optical Society (OSA), SPIE (The International Society for Optics and Photonics), American Physical Society, IEEE Photonics Society, ALIA Laser Institute of America and a lot of other professional associations. The lobbying was also pushed by **Jonathan Dowling** (1955-2020, American), professor of physics at Louisiana State University and specialist in photonics<sup>1620</sup>.

The **Quantum Industry Coalition** brings together more generalist manufacturers such as Microsoft, Intel and Lockheed Martin as well as startups<sup>1621</sup>. This coalition is helped by the lobbying firm KL Gates. It is the 41<sup>st</sup> largest law firm in the world making \$1B annually. The director of the Quantum Industry Coalition is Paul Stimers, a partner of KL Gate<sup>1622</sup>. To this should be added the **Quantum Alliance Initiative** launched in 2018 by the Hudson Institute, a conservative think tank, which creates proposed standards for QKD and QRNG and of course advocates for the development of this industrial sector in the USA.

NIST had also created with **SRI International** the **Quantum Economic Development Consortium** (QED-C) to develop the American quantum industry in the fields of communication and sensing<sup>1623</sup>. It is chaired by Joseph Broz, who is also vice-president of SRI, and by Celia Merzbacher, a semiconductor industry lobbyist who worked in the White House during the Bush 43 administration.

The Quantum National Initiative Act proposed allocating \$1,275B over five years to fund civil quantum R&D, divided among the Department of Energy (\$625M), NSF (\$250M) and NIST which is focused on cryptography issues (\$400M).

The Act also proposed the creation of a National Quantum Coordination Office within the White House Office of Science and Technology Policy. It asked the President of the United States to create a 10-year quantum plan, the first step being a five-year plan to be delivered one year after the passage of the law.

This bill was pushed by elected officials fearing that China will take over the quantum, especially in computer security<sup>1624</sup>. The USA likes to scare itself, even if, in the field of quantum technologies, it has nothing to be ashamed of with a density of public and private research laboratories and the major players having a large-scale industrialization capacity that almost no country can compete with. And their domestic market remains the largest in the world for enterprise computing applications.

---

<sup>1620</sup> See [Schrödinger's Killer App - Race to Build the World's First Quantum Computer](#) by Jonathan P. Dowling, 2013 (445 pages) where the author was sending a warning about the risk to see China lead the quantum technology race. If the USA were not investing more: "The future of the quantum Internet is in photons and the short circuiting of the development of optical quantum information processors in the United States means that the future quantum Internet will have 'Made in China' stamped all over it.", page 173.

<sup>1621</sup> See their [Quantum Industry Coalition](#) website.

<sup>1622</sup> See [The US National Quantum Initiative](#) by Paul Stimers, K&L Gates, October 2019 (6 pages).

<sup>1623</sup> See [NIST Launches Consortium to Support Development of Quantum Industry](#), September 2018. And more details in [U.S. Consortium Pulls Ecosystem Into Quantum](#) by Susan Rambo, August 2019. As of July 2020, the association has 130 members from the private sector - large corporations and startups - and about 40 laboratories from universities and the U.S. public sector.

<sup>1624</sup> See [How suspicions of spying threaten cross-border science](#) by Patrick Howell O'Neill, December 2019, which discusses the direct and indirect methods used by China to plunder European and American quantum research and exploit it both civil and military, such as quantum radars, quantum sonars and QKD. Here is the [link](#) to retrieve the Quantum Dragon Strider study mentioned in the article, November 2019 (22 pages). You can indicate a bogus email to get it, the download does not go through an email. It evokes various partnerships in research that help the Chinese to exploit Western research. It is based on a few examples including the very detailed one from the University of Heidelberg in Germany. On the same subject, see also [China's top quantum scientist has ties to the country's defense companies](#), December 2019, [Quantum USA Vs. Quantum China: The World's Most Important Technology Race](#) by Moor Insights and Strategy, October 2019 and [New Warnings Over China's Efforts in Quantum Computing](#) by Sintia Radu, January 2020.

This bill was voted by the House in September and then by the Senate in December 2018<sup>1625</sup>. In September 2018, the White House published the [National Strategic Overview for Quantum Information Science](#) that included the terms of the congressional proposal. They emphasized research, training of scientists and international collaboration. At last, Donald Trump signed this law on December 21, 2018 just before the shutdown, but with no fanfare nor any scientists in the Oval Office<sup>1626</sup>.

In December 2019, the **Quantum Information Edge** alliance was created, bringing together Lawrence Berkeley National Laboratory and Sandia Labs of the Department of Energy, the University of Maryland, Duke University (North Carolina), the University of Colorado at Boulder, Harvard, Caltech, MIT and the University of New Mexico<sup>1627</sup>. For the most part, the usual suspects of basic research in quantum computing, thus creating their "virtual hub" for coordinating research in this field. With a focus on error reduction at the qubit level, techniques for interconnecting qubits and the development of new quantum algorithms. For its part, the NPI embarked on a new lobbying campaign at the end of 2019 and early 2020 to increase once again the federal funds allocated to research in quantum technologies<sup>1628</sup>.

In February 2020, the White House published a memo from the National Quantum Coordination Office recommending the development of quantum networks<sup>1629</sup>. And in March 2020, the US executive proposed a new increase in quantum research budgets for the years 2020/2021<sup>1630</sup>.

It included \$450M for the Department of Energy, \$330M for the NSF and \$80M for the NIST. This was matched by a \$1B increase for artificial intelligence research programs<sup>1631</sup>. In August 2020, the White House announced a 30% increase in the quantum and AI budgets for fiscal year 2021. Other budget increase will probably come during the Biden administration given the usual Congress bi-partisan agreements reached on these strategic matters.



(quantum|gov)

The US NQI (National Quantum Initiative) is run by the **National Quantum Coordination Office** (NQCO), hosted by the White House Office of Science and Technology Policy (OSTP).

It has a web site and a logo since October 2020<sup>1632</sup>! Its director is Charles Tahan<sup>1633</sup>.

---

<sup>1625</sup> See [SIA Welcomes House Passage of Quantum Computing Legislation](#), September 2018.

<sup>1626</sup> See [President Trump has signed a \\$1.2 billion law to boost US quantum tech](#) by Martin Giles in the MIT Technology Review, December 2018. In the signature in the oval office, the President was flanked by his daughter Ivanka Trump and two White House science advisers. No representatives from the quantum research ecosystem or Congress were present. The next day, December 22, 2018, began the famous 35-day government shutdown initiated by the President. See Jeremy Tsu's [The Race to Develop the World's Best Quantum Tech](#) in IEEE Spectrum, December 2018, which discusses the CNAS report [Quantum Hegemony-China's Ambitions and the Challenge to U.S. Innovation Leadership](#) published in September 2018, which describes China's quantum strategy (52 pages). See also [US intelligence community says quantum computing and AI poses an 'emerging threat' to national security](#) by Zack Whittaker, December 2018.

<sup>1627</sup> See [US alliance for quantum computing](#) by David Manners, 2019.

<sup>1628</sup> See [NPI Brings Quantum Experts to Capitol Hill to Advocate for Additional NQI Funding](#) by Jo Maney, March 2020.

<sup>1629</sup> See [A Strategic Vision for America's Quantum Networks](#), White House, February 2020 (4 pages).

<sup>1630</sup> See [Why is Trump funding quantum computing research but cutting other science budgets? The national security implications of this technology may be exaggerated](#) by John Lindsay, March 2020.

<sup>1631</sup> See [White House reportedly aims to double AI research budget to \\$2B](#) by Devin Coldewey in TechCrunch, February 2020.

<sup>1632</sup> The NQCO published the quick status report [Quantum frontiers report on community input to the nation's strategy for quantum information science](#) in October 2020 (32 pages).

<sup>1633</sup> Charles Tahan is a physicist specialized in condensed matter physics and quantum information science.

And if you wonder about the bureaucracy in your own country, here you are also with several related committees: the **National Science and Technology Council** (NSTC) Subcommittee on Quantum Information Science (SCQIS) that coordinates Federal R&D in quantum technologies, the **National Science and Technology Council** (NSTC) Subcommittee on the Economic and Security Implications of Quantum Science (ESIX) that handles economic and security implications across federal agencies<sup>1634</sup> and the **National Quantum Initiative Advisory Committee** (NQIAC) that advises the President, the Secretary of Energy and the NSTC Subcommittee on QIS.

In April 2021, the story went on with yet another Congress proposal, the **Quantum for Universal Advancement in Nationwide Technology Use and Modernization** (QUANTUM) for National Security Act of 2021<sup>1635</sup>. Two Senators introduced two bills to “*better position the United States to be globally competitive in quantum information science*”. It’s focused on developing Department of Defense quantum networking and telecommunications use cases and workforce developments. This bill appears as a direct response to China’s massive investments in quantum telecommunications infrastructures. It’s kind of a military grade version of the National Quantum Initiative Act launched in 2018 that had mostly a civilian face despite the significant DoE funding it did incorporate.

### ***Military and intelligence federal agencies***

Public laboratories investing in quantum computing cut across much of the federal military-industrial complex with internal research or external research funded through calls for proposals or joint laboratories with universities:

**IARPA** (Intelligence Advanced Research Projects Agency) funds third-party projects on quantum computing and quantum algorithms. They run several quantum programs that happen to involve Universities outside the USA. The only that seems still in place is **LogiQ**. Its goal is to improve the quality of qubits. It involves TU Delft (Netherlands), the University of Innsbruck, Duke University and IBM. IARPA also funds programs conducted by third parties. It is a small agency that employs fewer than a hundred people.

**NSA** is investing heavily in quantum technologies, both in the race to implement Shor’s algorithm for breaking RSA-based public-key protected communications and for protecting sensitive communications with quantum keys and cryptography. This work is obviously not public. The NSA subcontracts some of its research to private companies such as Lockheed-Martin. It is also part of a joint laboratory with NIST and the University of Maryland, QuICS, which was launched in 2014.

**DARPA** funds three programs in quantum technologies: long-distance quantum communications, quantum metrology applied to imaging, and neurological trauma diagnosis and PTSD. Funding goes to projects led by universities, startups and established companies<sup>1636</sup>. In 2020, they launched a NISQ computation challenge which led to the selection of 7 research teams as part of the ONISQ program<sup>1637</sup> and QAFS, a program on quantum annealing involving among others the Lincoln Lab from the MIT.

**Army Research Office** also has its own quantum research program covering the entire spectrum from sensing to quantum computing, cryptography and quantum communications.

---

<sup>1634</sup> In [The role of international talent in quantum information science](#) by National Science and Technology Council of the White House, October 2021 (20 pages), the NSTC worries about the quantum talent shortage in the USA and advocates a balanced approach between hiring international talent and protecting national security. The global hunt for talent is launched!

<sup>1635</sup> See [Thune, Hassan Introduce Bills to Bolster the United States’ Leadership in Quantum Information Science](#), April 2021.

<sup>1636</sup> See [The DARPA Model for Transformative Technologies](#), 2019 (511 pages) which tells the story of how the agency works. It has about one hundred program managers in total with a total budget of about \$3.5B. It explains how it connects fundamental research to difficult technology challenges.

<sup>1637</sup> See [DARPA Challenge May Boost Quantum Value of NISQ Devices](#) by Matt Swayne, June 2020. One of the selected teams includes a certain Davide Venturelli who studied at the University of Grenoble.

**US Air Force** and its Air Force Research Laboratory's Quantum Communications lab is focused on quantum cryptography (QKD). The AFRL announced in December 2020 that it planned to work with the Office of Naval Research to test quantum technologies with the "Five Eyes" countries (USA, Canada, Australia, New Zealand and UK) for a Naval exercise. Another lab, the Quantum Information and Sciences Laboratory, does applied research in superconducting qubits, photonic qubits, trapped ions qubits, quantum algorithms and quantum sensing. They even deployed their own superconducting qubits system prototype, created with the MIT.

**Office of Naval Research** (ONR) is working on the use cases of QKDs for the Navy and on using of quantum algorithms related to the Navy operational needs.

### *Federal civil agencies*

**Department of Energy** (DoE) has many research laboratories that are big consumers of supercomputing capacities like in Oak Ridge and Argonne. It also operates the Los Alamos National Laboratory (LANL) and its Quantum Institute (QI) launched in 2002 that also invests in quantum computing and cryptography. In particular, they fund research at UNSW in Australia as well as in Maryland. The DoE also runs the Sandia National Laboratories, which also conducts applied research in all areas of quantum physics.

The DoE launched a call for proposals to award 158 grants totaling \$32M to 118 SMEs through the SBIR program. The grants are delivered in two phases, a first phase of \$200K followed by a second phase of \$1.1M for the best projects, spread over a period of two and a half years.

The DoE also announced in August 2020 the funding of five research centers in quantum technologies, all led by DoE laboratories, with \$300M coming from the DoE and the rest from relevant institutions and the industry (IBM, Microsoft, Intel, Lockheed Martin)<sup>1638</sup>. These new research centers are **Q-NEXT** (Next Generation Quantum Science and Engineering Center, David Awschalom) led by Argonne National Laboratory which focuses on the industrialization of quantum hardware, **C<sup>2</sup>QA** (Co-design Center for Quantum Advantage, Steve Girvin) led by the DoE Brookhaven National Laboratory which will focus on ways to achieve quantum advantage in scientific applications, the **SQMS** (Superconducting Quantum Materials and Systems Center, Anna Grassellino) led by the Fermi National Accelerator Laboratory which will focus on superconducting qubits, the **QSA** (Quantum Systems Accelerator Center, Irfan Siddiqi<sup>1639</sup>) led by the Lawrence Berkeley National Laboratory which works on quantum computing hardware and software and the **QSC** (Quantum Science Center, David Dean) led by the Oak Ridge National Laboratory which will focus on quantum computing scalability issues.

The DoE then launched a \$30M program in March 2021 on nanoscale matter and their use case in energy applications. It will fund the five existing DoE Nanoscale Science Research Centers and their research partners over 3 years. The awards size is between \$1M and \$2.5M<sup>1640</sup>. It also launched a \$25M program in April 2021 on Quantum Internet including quantum repeaters, quantum memory and quantum communication protocols, opened to the 17 DoE labs.

**NSF** funds various research projects<sup>1641</sup>. In 2019, it launched a call for **Quantum Leap Challenge Institutes**, to fund research institutes conducting interdisciplinary research projects advancing the state of the art in quantum technologies ([details](#)).

---

<sup>1638</sup> See [National Quantum Information Science Research Centers](#) by Ceren Susut, December 2020 (17 slides). Unstable link.

<sup>1639</sup> The QSA was awarded a funding of \$115M for 5 years in August 2020. See [New \\$115 Million Quantum Systems Accelerator to Pioneer Quantum Technologies for Discovery Science](#) by Dan Krotz, August 2020.

<sup>1640</sup> See [DOE Announces \\$30 Million for Quantum Information Science to Tackle Emerging 21st Century Challenges](#), March 2021.

<sup>1641</sup> See for example [NSF Awards \\$2M For Research on Quantum Machine Learning With Photonics](#), September 2019 for the University of Maryland.

Their format is reminiscent of the UK quantum program hubs. Three hubs were selected in July 2020 for a total of \$75M spread over five years: a first dedicated to quantum sensing led by the University of Colorado, a second dedicated to quantum computing led by the University of Illinois - Urbana-Champaign and a third also on quantum computing and rather software side led by the University of Berkeley ([source](#)). These three hubs bring together 16 academic institutions, 8 national laboratories and 22 industrial partners. On top of that, the NSF is also funding the consolidation of other initiatives like the one around Purdue University in Indiana<sup>1642</sup>. The NSF also launched a **Quantum Algorithm Challenge** in March 2020 ([source](#)).

**NIST** is a federal research institute with the Department of Commerce. Its historical role is sensing and the definition of weights and measures. Its work on atomic clocks naturally led it to look after quantum technologies. It has an annual budget of \$1.2B and employs 3,400 people on two campuses, one in Boulder, Colorado and another one in Maryland, next door to the University of Maryland and north of Washington DC. Several of its research groups are dedicated to quantum technologies with the Quantum Processing Group for quantum computing, another for spintronics, one for quantum sensing and another for superconducting electronics. On top of this, the Computer Security Division of the Information Technology Laboratory (ITL) manages the call for tenders on the standardization of PQC (Post-Quantum Cryptography) that we have already covered in a [dedicated chapter](#) after page 616<sup>1643</sup>. NIST's PQC standardization strategy has wide implications. It will sediment the market around a dozen standards that will be royalty-free. This may favor large cybersecurity vendors instead of enabling new players to disrupt the market.

NIST is also a stakeholder in and a co-founder of three joint laboratories with two major universities, each located near its own campuses in the states of Colorado and Maryland.



The University of Maryland's **Joint Quantum Institute** (JQI), established in 2006 is a fundamental quantum physics laboratory. It is the home of David Wineland, a long-time specialist in ion control by laser cooling, who won the Nobel Prize in Physics in 2012 along with Serge Haroche. It is in this laboratory that the IonQ startup by Christopher Monroe was launched in 2015. Many alumni from this lab also joined Honeywell's quantum team in Denver, Colorado.

This laboratory employs 35 permanent researchers, 55 post-docs and 85 PhD students with an annual budget of \$6M supplemented by various external funding.

The **Joint Center for Quantum Information and Computer Science** (QuICS) at the University of Maryland (UMD) launched in 2014 in partnership with NSA's research directorate that focuses on quantum computing architectures, algorithms and complexity theories to complement the JQI.

The **JILA** at the University of Colorado at Boulder which is dedicated to sensing technologies<sup>1644</sup>. It is home to two Nobel Prize winners: Eric Cornell (in 2001, for his work on Bose-Einstein condensates) and John Hall (in 2005, for his work on laser frequency combs).

---

<sup>1642</sup> Purdue University launched in July 2021 a new Center for Quantum Technologies funded by the NSF with an established team of 50 quantum scientists and engineers coming from various research institutions in Indiana working on many quantum fields (atomic and molecular optics, solid state quantum systems, quantum nanophotonics, quantum information and communication).

<sup>1643</sup> See this overview of NIST's scientific activities: [Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact](#), 2019 (39 slides).

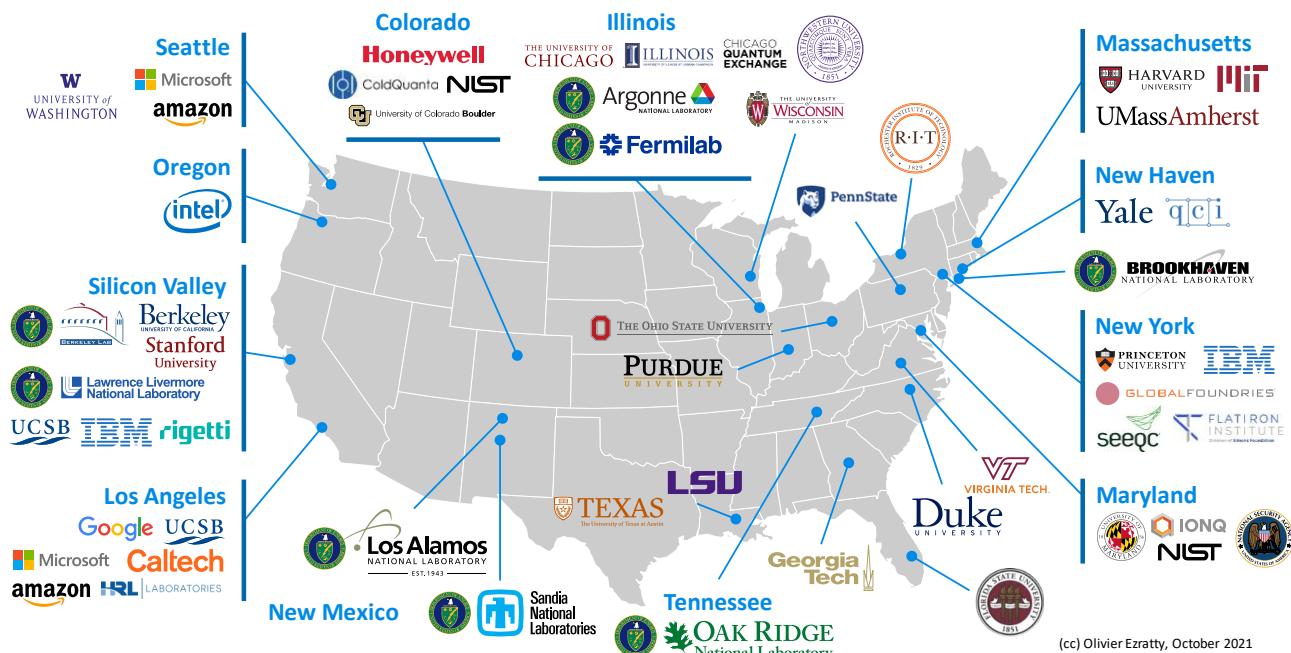
<sup>1644</sup> JILA was created in 1962 as the Joint Institute for Laboratory Astrophysics but they now use only the acronym without this meaning given its extended activities beyond astrophysics.

NIST employs a fourth Nobel Prize winner in physics, William Phillips for his work on atoms laser cooling in 1997, shared with Claude Cohen-Tannoudji from France.

**NASA** created in 2013 the Quantum Artificial Intelligence Laboratory (QuAIL) jointly with Google, located at the Ames Research Center near the Google's headquarters in Mountain Views to explore the field of quantum algorithms, in particular on a D-Wave quantum annealer they acquired and installed there.

### USA local quantum ecosystems

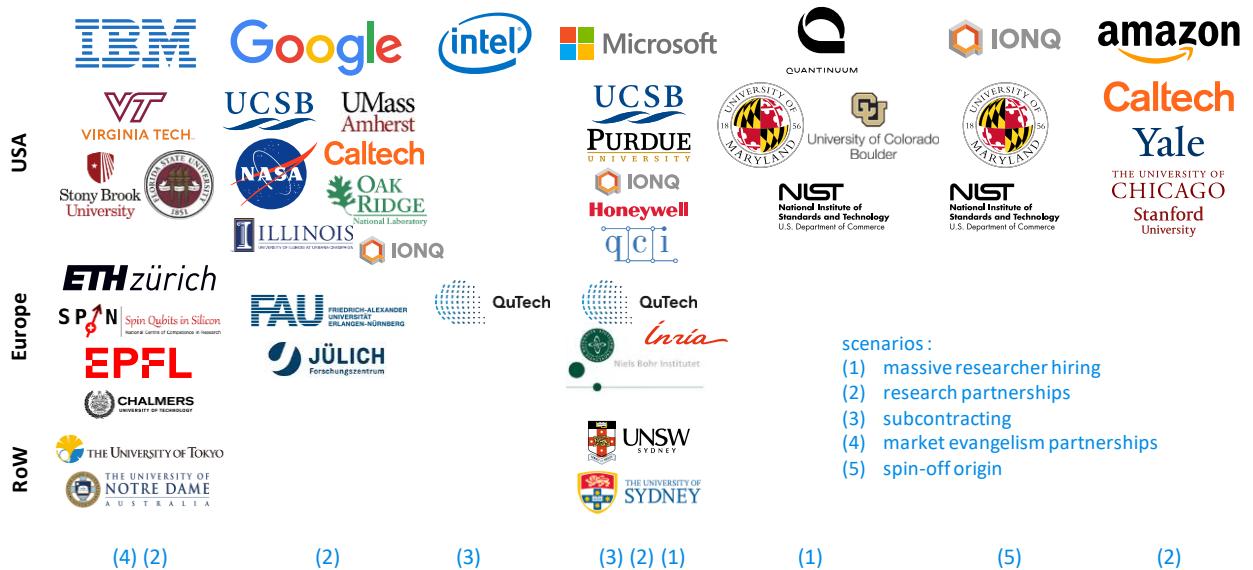
The main geographical quantum hubs in the USA combine a mix of national labs like those from the DoE, Universities and commercial companies. They are located in **California** (Silicon Valley and Los Angeles), **Colorado** (at Boulder, with Honeywell, NIST and the University of Boulder<sup>1645</sup>), Illinois/Chicago (with two DoE labs, Fermi and Argonne, and several universities), **Massachusetts** (MIT, Harvard and UMass Amherst), **New Haven** (with Yale and Qci), **New York** (with Princeton, Flatiron Institute, IBM, Global Foundries and SeeQC) and **Maryland** (University of Maryland, IonQ, NIST, NSA). On top of that, **Tennessee** and **New Mexico** host three DoE labs and their quantum research centers. Lesser developed ecosystems can be found in **Florida**, **Virginia** (Virginia Tech) and **Georgia** (GeorgiaTech). I crafted the never released map below to showcase this geographical distribution of USA's quantum technology efforts. The distribution is more even than in classical digital technologies, which are more concentrated on the country's west coast. In California, thanks to Caltech and UCSB, the Los Angeles area even competes with the Silicon Valley.



Other quantum hubs get organized. For example, the Chicago quantum ecosystem is federated by the **Chicago Quantum Exchange** which regroups the Argonne National Laboratory from the DoE, the University of Chicago, the University of Illinois, the Fermi Lab, the University of Wisconsin and Northwestern University. The University of Chicago Polsky Center and the Chicago Quantum Exchange launched the first national quantum startups accelerator program in April 2021.

Finally, let us recall a market reality that echoes economist **Maria Mazzucato**'s thesis on the public origin of technological innovations: the major American players are sourcing at different levels and throughout the USA and the world to advance their quantum technologies.

<sup>1645</sup> The University of Boulder created the Qubit Quantum Initiative to foster interdisciplinary quantum research.



The diagram *above* is a good illustration of this showing how large IT players like IBM, Google, Intel, Microsoft, Amazon, Honeywell and even IonQ, surf on the work of publicly funded research labs not only in the USA but throughout the world.

## Canada



In Canada, a parallel can be drawn between artificial intelligence and quantum technologies. In both cases, the country's influence is far greater than its economic weight, at the basic research level, with a healthy startup ecosystem and best-in-class investment per capita.

This is due in particular to a constant and early-stage investments in research by government and universities and to a certain entrepreneurial dynamism.

Canada has two great quantum stars in research with **Gilles Brassard** of the University of Montreal who is with **Charles Bennett** of IBM Research the co-inventor of QKD's BB84 protocol.



## Research

Canada is distinguished by a strong investment in basic research in quantum computing, including more than \$1B of public investment over a decade, mainly in three institutions<sup>1646</sup>:

**University of Sherbrooke** Quantum Institute, near Montreal, is home to Alexandre Blais, a recognized specialist in superconducting qubits. Their **QSciTech** training program organized with industry partners and the Q2 initiative encourage student entrepreneurship. Several startups came out of it such as SBTech (metrology), Nord Quantique (quantum computing) and Quantic (sensing).

**University of British Columbia** Quantum Matter Institute (QMI), located primarily in Vancouver.

<sup>1646</sup> See [Quantum Canada](#) by Ben Sussman, Paul Corkum, Alexandre Blais, David Cory and Andrea Damascelli, February 2019 (6 pages) for an overview on Canada's quantum investments.

**University of Waterloo** Institute for Quantum Computing, near Toronto, which obtained \$120M in 2017 to fund its various quantum research institutes, complemented by \$53M in Australian funding from UNSW, the operator Telstra and the Commonwealth Bank of Australia. The IQC does both research and teaching. They offer short courses of one to two weeks in the summer on quantum cryptography and quantum computing. The IQC is directed by Raymond Laflamme, one of the fathers of QEC. They cover all aspects of quantum technologies with about thirty teams of theorists and experimentalists, about fifty post-docs and 125 PhD students. A dozen startups were created since 2002. The IQC is leading the Transformative Quantum Technologies (TQT), a seven-year research commercialization program funded by the Canadian government and its First Research Excellence Funds to the tune of \$76M. In January 2020, TQT launched the Quantum Alliance, an umbrella for IQC and TQT to link them to their Canadian and international ecosystem, including the fabric of quantum startups.

Other laboratories are involved, such as the **University of Calgary**, which is working on quantum communications and has deployed an experimental QKD network of a few tens of kilometers. The **University of Alberta** in Edmonton, north of Calgary, is also involved in this work<sup>1647</sup>.

### ***Government funding***

As in most countries, the government is funding quantum research and the industry. In 2020, the government of Alberta dedicated \$11.8M to the creation of an international hub for quantum computing, \$3M of which will fund quantum research. The government of Quebec is also very active to fund the development of its ecosystem, particularly around the University of Sherbrooke.

In April 2021, the Federal government announced its national quantum initiative with a \$300M plan spread over 7 years. Just before, in March, it announced a public funding of \$40M for D-Wave<sup>1648</sup>.

And then they have a Prime Minister who [knows how to explain what is a qubit](#), since 2016. It's a feat that was well noticed at the time and that is still rare. As curious as it may seem, Canada has not yet produced a true national quantum strategy.

All this is packaged in highly optimistic business forecasts. The National Research Council of Canada (NRC) estimated that quantum technologies would generate \$142.4B turnaround and create 229,000 employments in Canada by 2040<sup>1649</sup>. It's quite optimistic given it's even larger than the most bullish worldwide forecasts!

### ***Quantum industry***

In the industry side, you can't escape **D-Wave** and the quantum software specialist **1QBit**. With over 36 quantum startups and SMEs, they are the second largest ecosystem in the world in this respect after the USA and UK.

Private funding includes donations from Michael Lazaridis, one of the RIM BlackBerry co-founders, with \$75M to the **Institute for Quantum Computing** at the University of Waterloo and \$128M in 1999 to the **Perimeter Institute for Theoretical Physics** also located in Waterloo. Together with Doug Fregin, also co-founder of RIM, they also created the **Quantum Valley Investment Fund** with a total of \$100M in funding.

---

<sup>1647</sup> See [Quantum Communication Network Activities Across Canada](#) by Barry Sanders and Daniel Oblak, June 2019 (10 slides).

<sup>1648</sup> See [Government of Canada contribution strengthens Canada's position as a global leader in quantum computing](#), March 2021. This funding looks curious considering the company was created back in 1999. But it's probably not yet break even and has a strong need for cash to maintain its activity and leadership in a yet unmatured market.

<sup>1649</sup> Source: [Economic impact of quantum technologies](#).

Let us also note the existence of the **Creative Destruction Lab**, a deep techs startup acceleration structure with a specialty on quantum technologies. They are located in Canada (Toronto, Montreal, Vancouver, Calgary, Halifax), in the USA (Atlanta) as well as in Oxford and Paris.

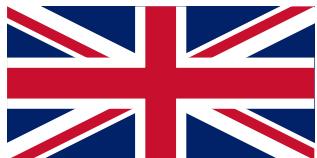


In 2020, a group of industry vendors created **Quantum Industry Canada** (QIC), an association promoting the Canadian quantum industry. It includes D-Wave, 1Qbit, Xanadu, Zapata and ISARA.

## Europe

Just making things clear, we're dealing here with geographical Europe, including European Union member states, the UK and Switzerland!

### United Kingdom



As with many continental European countries, the United Kingdom has contributed to many advances in quantum physics since the 18<sup>th</sup> century with precursors and founders, followed by a new generation of scientists in the second half of the 20<sup>th</sup> century.

Let's mention **Thomas Young** (1773-1829), **Ernest Rutherford** (1871-1937), **Joseph John Thomson** (1856-1940), **James Chadwick** (1891-1974), **Paul Dirac** (1902-1984), **Brian Josephson** (1940), **David Deutsch** (1953), **Andrew Steane** (1965) and even more recently the creators of the QML language, **Thorsten Altenkirch** and **Jonathan Grattage**.

### Research

In the UK, the main quantum research laboratories are located in the Universities throughout the country. All of these have one or several quantum physics laboratories. Their main specialties are found later in the UK quantum plan rollout with a lot of advanced photonics (Bristol, Oxford), electron spin (UCL), telecommunication and cryptography (nearly all of them), sensing (same) and the likes. See the list of UK Universities in the UK map in a forthcoming page.

## Government funding

At the instigation of the physicist Sir Peter Knight (1947), UK was the first large country to launch a quantum technologies structured plan, the **UK National Quantum Technologies Programme**, announced in November 2013. It had an initial funding of £270M over five years<sup>1650</sup>.

This represented a much larger amount of funding than for previous initiatives in innovative materials or robotics. The plan did not start from scratch. It was built on an existing ecosystem of university research laboratories in quantum physics.

The plan was and remains coordinated by the **EPSRC** (Engineering and Physical Sciences Research Council), a non-governmental organization funded and supervised by the government. The plan involves **Innovate UK** (basic research funding), the **Department for Business, Energy and Industrial Strategy**, the **NPL** (National Physical laboratory, where Peter Knight had been Chief Science Advisor), the **GCHQ** (their NSA) and **dstl** (army research).



In a fairly conventional way, the UK plan targeted all the usual quantum fields: computing, security, and sensing with a strong focus on medical imaging. Funding was based on thematic hubs bringing together universities and selected by call for projects (£124M), training, technology transfer and industrialization<sup>1651</sup>.

From the outset, the plan showed a strong commitment to creating business and attracting private capital. The original plan was to move research into startups as quickly as possible.

Four quantum hubs cover the major fields of quantum technologies and bring together teams spread over the territory in some thirty universities. All the hubs managers are scientists, supplemented by a business development director and a board of 8 people including industry vendors CTOs.

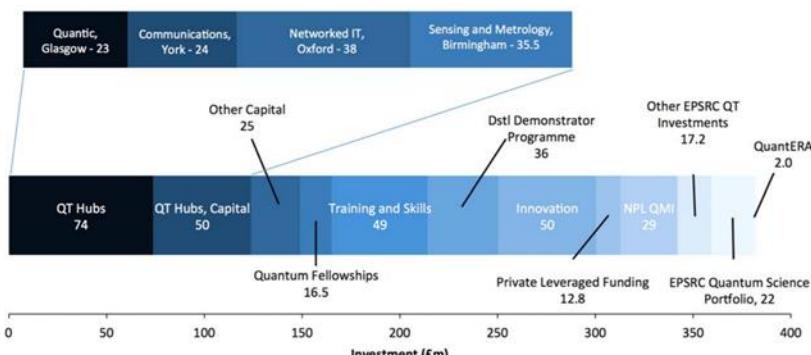


Figure 1. Representation of the funding allocated to the elements of the UK NQTP 2014–2019.



The **UK Quantum Technology Hub Sensors and Timing** covers sensing, including time measurement and involves the universities of Birmingham, Glasgow, Nottingham, Southampton, Strathclyde and Sussex.

<sup>1650</sup> See [The UK National Quantum Technologies Programme Current and Future Opportunities](#) by Derek Gillespie, November 2014 (29 slides) and [Delivering the National Strategy for Quantum Technologies](#) (5 pages).

<sup>1651</sup> Diagram source: [UK national quantum technology programme](#) by Peter Knight and Ian Walmsley, October 2019 (10 pages).

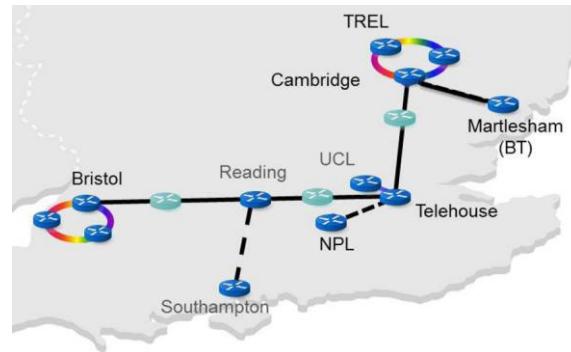


They are developing a quantum communication network between Bristol, Cambridge and Ipswich via the **UK National Dark Fibre Infrastructure Service** launched by the EPSRC (also linking Southampton and UCL in London)<sup>1653</sup>. This did not prevent the state security agency from expressing skepticism about the suitability of QKD in a four-page white paper published in April 2020<sup>1654</sup>.

The **Quantic** hub brings together the Universities of Glasgow, Bristol, Edinburgh, Heriot-Watt, Oxford and Strathclyde and focuses on quantum imaging. This gives us two hubs in the field of quantum sensing.

The **Quantum Computing & Simulation Hub** brings together 17 universities and is led by Oxford University. It took over from the NQIT (Networked Quantum Information Technologies) hub in 2019. It focuses on computing and security issues<sup>1652</sup>. They are working on creating a network of trapped ions quantum computers.

The **Quantum Communications Hub** consolidates a dozen universities: Bristol, Cambridge, Glasgow, Heriot Watt, Kent, Oxford, Queen's Belfast, Sheffield, Strathclyde under the leadership of York University, companies such as Airbus, Toshiba, ID Quantique, QinetiQ, Kets, and public agencies.



These hubs are finally very multipolar, bringing together universities that are involved in several different hubs, according to the map on the next page<sup>1655</sup>. The United Kingdom has had a lot of ideas in managing this plan over the long-term.

A progress report was published in 2015 by the EPSRC and Innovate UK followed by another interim report, the Quantum Age-Blackett review in 2016 investment launched in 2014 and in particular extending the effort to the algorithmic and software part, in particular in liaison with the **Alan Turing Institute** and the **Heilbronn Institute for Mathematical Research** to propose case studies of computational problems to be solved<sup>1656</sup>.

<sup>1652</sup> This includes the [QuOpal](#) (Quantum Optimization and Machine Learning) initiative funded by Nokia and Lockheed Martin.

<sup>1653</sup> Diagram source: [The Quantum Communications Hub](#), 2016 (11 slides).

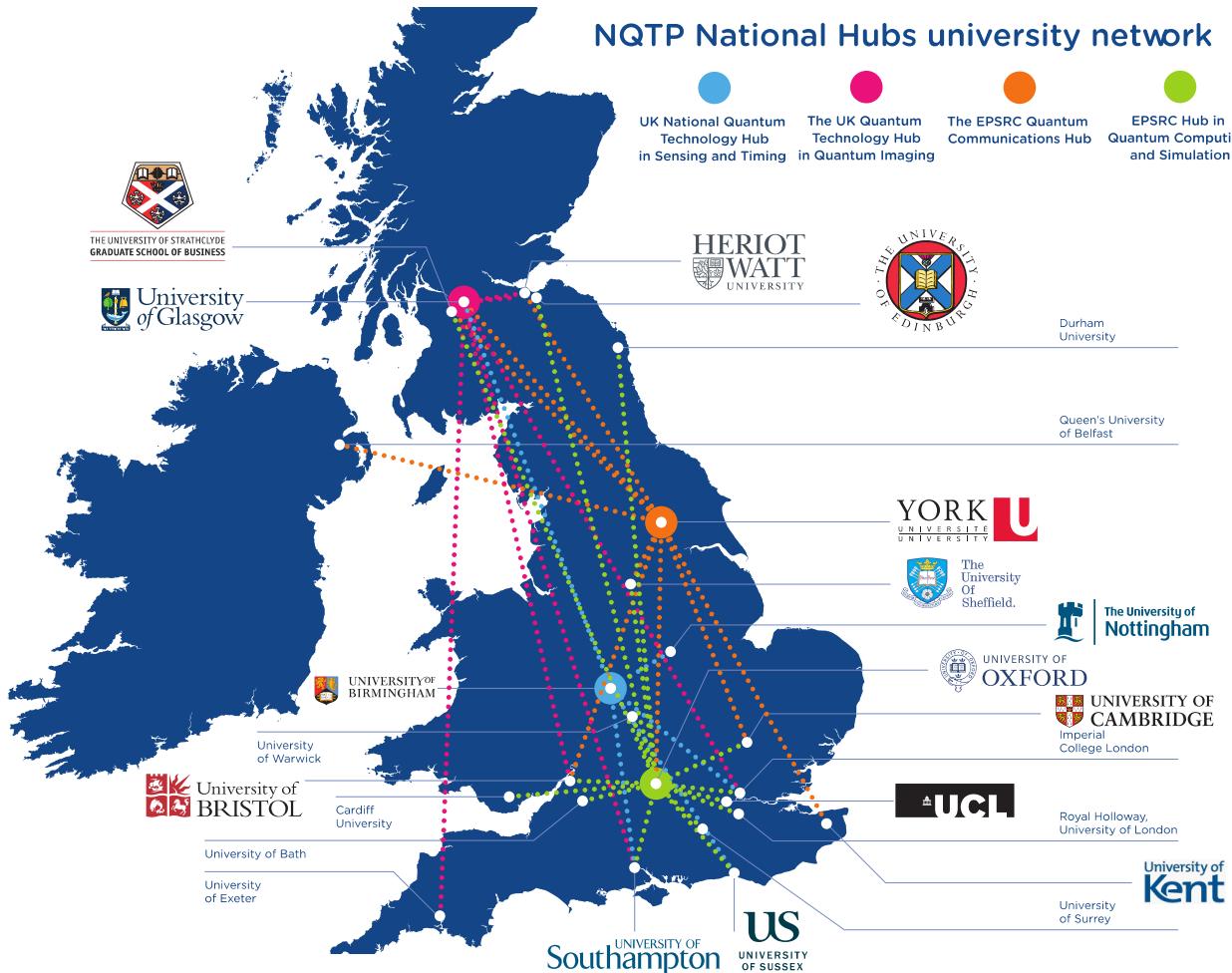
<sup>1654</sup> See [Quantum Security Technologies](#), NCSC, March 2020 (4 pages).

<sup>1655</sup> Map source: [UK National Quantum Technologies Plan Strategic Intent](#), 2020 (38 pages). I added some of the large universities logos. See also [UK national quantum technology programme](#) by Peter Knight and Ian Walmsley, October 2019 (10 pages).

<sup>1656</sup> See [The Quantum Age Technological Opportunities](#), 2016 (64 pages) and [A roadmap for quantum technologies in the UK](#), 2015 (28 pages).

This was followed by a parliamentary report published in November 2018 which supported the continuation of the plan, the launch of a second phase of £350M over the period 2019-2024 and some fine tuning on the coordination between the different stakeholders (hubs, innovation centers, companies)<sup>1657</sup>. This led to the official announcement of Phase 2 in June 2019, following the recommendations of the House of Commons<sup>1658</sup>. With the expected private sector investments, the total of the two phases of the UK Quantum Plan was estimated at \$1,227B.

Phase 2 funding renewed funding for hubs (£94M over 5 years), industrialization projects (£153M from the Industrial Strategy Challenge Fund, over 6 years<sup>1659</sup>), training (£25M over 5 years<sup>1660</sup>). It added the launch of the NQCC (National Quantum Computing Centre) for the development of quantum computing solutions, with £93M over 5 years<sup>1661</sup>.



<sup>1657</sup> See [Quantum technologies](#), House of Commons Science and Technology Committee, November 2018 (75 pages).

<sup>1658</sup> See [UK government invests \\$194M to commercialize quantum computing](#) by Frederic Lardinois.

<sup>1659</sup> The Industrial Strategy Challenge Fund (ISCF) was a multi-domains initiative of £2.6B backed by £3B of private investments, created to invest in challenges having a strong economical and societal impact. A dedicated Commercialising Quantum Technologies Challenge was then launched in two stages, first in 2018 with £20M and second with £153M completed by £205M from the private sector, in July 2019. To date, in 2021, over 40 such projects were funded. As of late 2020, over £200M were invested in UK startups.

<sup>1660</sup> Doctoral training in quantum technologies is not managed in the hubs but in doctoral centers such as the Quantum Engineering Centre for Doctoral Training in Bristol.

<sup>1661</sup> See [Establishing the National Quantum Computing Centre \(NQCC\)](#), August 2019 (64 slides). The construction started in September 2021.

The first “UK” quantum computer was to be built by Rigetti (US). How can this be? It’s linked to Rigetti having acquired a local startup, QxBranch and to its various connections with the local ecosystem and universities. But Oxford Quantum Circuits announced the launch of its cloud based superconducting qubits based computer in July 2021.

All in all, the UK government has invested £100M per year in quantum technologies since 2014.

The bulk of Phase 2 is the NQCC, which is led by **UKRI**, the **EPSRC** and the **STFC** (Science and Technologies Facilities Council), a government agency that conducts research in physics and astronomy and manages the country's major scientific instruments (particle accelerators, lasers, space engineering, etc.)<sup>1662</sup>.

This center will produce NISQ and then LSQ computing demonstrators, develop quantum algorithms and software and their uses, and build a community of users around them. The center should open by the summer of 2021 and become fully operational in 2022. It will set up a NISQ machine that should be operational by 2025. In 2020, the preferred technologies were superconducting and ion-trapped qubits.

### National Quantum Computing Centre -what it should and shouldn't be

#### What it will be:

- Part of a quantum computing landscape involving academic led research and industry led innovation
- Able to explore the options for quantum computing machines
- A partner for UK industry in this area
- A pathway to impact and testing ground for academic led research
- An opportunity for training with access to prototype quantum computing systems
- A mechanism for growing a supply chain for quantum computing
- The basis for hosting working quantum computers that academia and industry can access

#### What it won't be:

- An isolated effort to develop quantum computers
- Closed to new partners and collaborations
- A competitor with a growing UK industry
- A short term intervention
- Partisan
- Outside of the UK NQTF or UKRI
- Only restricted to what can be done on its primary site

### National Quantum Computing Centre -benefits realisation

The NQCC could evolve in a number of ways (some of which could overlap) which all give benefit to the UK. Due to both its own efforts and the development of the area at large. For example the NQCC will:

- become the **enabler for a quantum computing supply sector** in the UK, due to it supporting the early efforts of start-ups companies in this area (such as through being a consortia member in ISCF projects) and its own development programme driving the formation of a supply chain they can use.
- be the natural host for work on quantum computing that is getting beyond that which can be continued in university environments, and give a **pathway to impact** for this which is within the UK.
- be natural partner for industry led projects and consortia in quantum computing. Bringing expertise, access to facilities and an environment in which development work can be hosted. **Lowering the barriers for companies** to start work in this area.
- be the **natural partner** in efforts to develop and build quantum computers for **government departments** and **agencies**.
- become a **source of trusted expertise** in quantum computing for potential users of this technology, and which in a feedback loop shapes the efforts of companies wishing to develop and sell quantum computing products and services. A technical authority.
- be a **training ground** for a quantum computing workforce for the UK. Through secondments from start-ups, hosting students, and later hosting working machines.
- is a facility where users from academia, industry and government can **access trusted quantum computing services** and get advice on how their problems can be solved.

The UK had recovered approximately 14% of the budgets for the first wave of European Quantum Flagship projects by October 2018. Despite the Brexit, the country will continue to benefit from it, as the collaboration with Europe on research survives the Brexit. For example, John Morton's UCL laboratory is part of the flagship project QLSI on silicon qubits driven by CEA-Leti and awarded in March 2020.

### **Quantum industry**

On the entrepreneurial side, around 40 quantum technologies startups were launched in the UK with a good balance by category. It is the third country in the world in terms of the number of startups, behind the USA and Canada.

The intellectual property management company **IpGroup**, launched in August 2020 a £12M fund to fund startups, these being selected by the independent agency **UKRI**. Projects funding range from £125K to £2M. Let's also mention the **Quantum Technology Enterprise Centre** from the University of Bristol which was a sort of startups incubator and training program for quantum startup founders. The QTEC incubation program offered a 12-months salaried fellowship to quantum scientists during the build-up of their startup and business skills training. Since 2016, QTEC helped the creation of 31 startups including KETS, QLM, Nu Quantum, Quantum Dice and Vector Photonics. The program funding ended in 2021 and QTEC is looking for funding to launch a new “cohort” of quantum entrepreneurs.

<sup>1662</sup> UKRI (UK Research and Innovation) is an autonomous non-governmental organization created in April 2018 with an annual budget of £7B and consolidates seven former research councils including the EPSRC and STFC, Innovate UK and Research England.



Notable players are **Oxford Instruments** (cryogenics), **Oxford Quantum Circuits** (superconducting qubits<sup>1663</sup>), **Quantum Motion Technologies** (silicon qubits), **Cambridge Quantum Computing** (operating system, software, services, which merged with Honeywell Quantum Systems in 2021), **TundraSystems** (photonic qubits), **Orca Computing** (photon qubits) and **River Lane Research** (software). On the other hand, no major company in the country seems to be particularly invested in quantum computing, except perhaps in telecommunications.

## Germany



Germany is a land of dense basic research in quantum technologies. It builds on a strong history of the many German founders of quantum physics with **Max Planck**, **Albert Einstein**, **Werner Heisenberg** and many others. It also has a strong ecosystem of industry vendors, particularly in quantum enabling technologies.

## Research

The main research organizations and laboratories involved in quantum technologies are:

**Max Planck Institute for Quantum Optics** (MPQ), based in Munich, is one of the 84 MPIs and their 24,000 employees. They specialize in cold atom-based qubits in particular. This MPI is associated with the International Max Planck Research School also based in Munich. Two other MPIs are dedicated to information technology, but do not seem to be invested in quantum.

**Munich Center for Quantum Science and Technology** (MCQST) in Munich was launched in 2019. It brings together Munich's quantum research centers: the MPQ, the Walther-Meißner-Institute for Low Temperature Research (WMI) and the city's two leading scientific universities: Ludwig-Maximilians-Universität München and Technical University of Munich (TUM).

<sup>1663</sup> Oxford Quantum Circuit obtained funding from Innovate UK in April 2020 in a consortium of four companies and two universities. See Oxford Quantum [Circuits-led consortium wins Grant to Boost Quantum Technologies in the UK](#) by Quantum Analyst, April 2020.

The ensemble covers all quantum technologies (simulation, computing, communication, sensors). The whole with a budget of 31M€ over five years and about 55 permanent researchers.

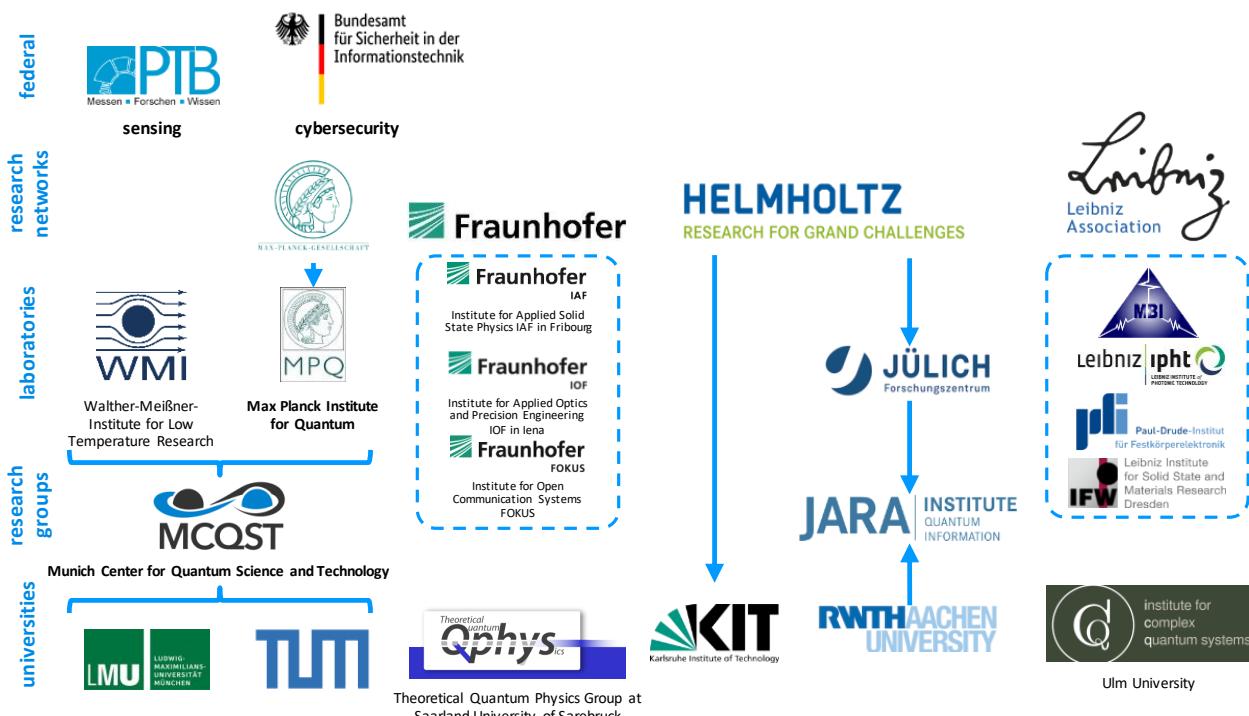
**Fraunhofer Institutes** for Applied and Partnership Research with its 72 institutes and 26,600 people. They comprise three institutes specializing in quantum physics: the Fraunhofer Institute for Applied Solid State Physics IAF in Freiburg, the Fraunhofer Institute for Applied Optics and Precision Engineering IOF in Jena and the Fraunhofer Institute for Open Communication Systems FOKUS in Berlin.

**Helmholtz Association** groups 18 Research Centers that conduct basic research in response to major societal challenges, with a total of 40,000 people. It includes the Quantum Laboratory of the **Jülich Forschungszentrum** (*aka* Jülich FZ or Jülich Research Center) located between Aachen and Cologne and headed by Kristel Michielsen<sup>1664</sup>, where Tommaso Calarco, who coordinates the European Quantum Flagship, also works. He is associated with the University of Aachen in the **JARA Institute Quantum Information** (IQI). The Helmholtz Network also includes the **Institute of Photonics and Quantum Electronics at the Karlsruhe Institute of Technology** (KIT).

**Leibniz Association** with its community of 96 centers conducting basic research includes the Institute for Solid State and Materials Research (IFW) in Dresden, Germany, which focuses on superconductivity and magnetism, the Institute of Photonic Technology (IPHT) in Jena, Germany, the Max-Born-Institute for Nonlinear Optics and Short Pulse Spectroscopy (MBI) in Berlin, Germany, and the Paul Drude Institute for Solid State Electronics (PDI) in Berlin, Germany.

**Institute for Complex Quantum Systems** at the University of Ulm between Stuttgart and Munich.

**PTB** is the federal office of sensing, which is obviously investing on quantum sensing like the NIST.



<sup>1664</sup> Jülich Forschungszentrum started in 1956 in nuclear research. It also houses a number of supercomputers, such as the CEA's DAM at Bruyère le Chatel in France or the US DoE Los Alamos research center.

**BSI** is the federal office for information technology security<sup>1665</sup>.

### **Government funding**

In September 2018, the German Federal Research Ministry announced €650M in funding for quantum technologies over four years (2018 to 2022)<sup>1666</sup>. Like all such plans, it funds projects in quantum computing, quantum communication and quantum metrology. In September 2019, IBM announced that it would join this plan. IBM was to install a quantum computer in Germany addressing researchers and cloud usages. It is not certain that this is the best approach to develop a German and European quantum industry, at least on the hardware side. The computer was actually launched early in 2021 in the Stuttgart region in an IBM facility.

In June 2020, the German government more than doubled its efforts by announcing a seemingly incremental €2 billion in funding for its quantum plan, including investment in two quantum computers<sup>1667</sup>. The \$2B seemed to include the initial 650M€ of the 2018 plan.

The German government put in place a scientific and industry experts board of 16 members to propose a roadmap and funding allocation with a Joint presidency of a scientist (Stefan Filipp from TU Munich) and an industry member (Peter Leibinger from Trumpf).

It made some proposals in December 2020 including creating an independent coordination body, Deutschen Quantengemeinschaft (DQG). In January 2021, the BMWi disagreed with some of these proposals, estimating that too much funding was directed to fundamental research at the expense of startups.

In May 2021, the plan was split in two parts with 1,1B€ managed by the Federal Ministry of Education and Research (BMBF) and 878M€ by the Federal Ministry of Economic Affairs and Energy (BMWi), focused on applications developments. One key showcased goal for this plan is to build two national quantum computers with 24, then 100 and later 500 functional qubits (seemingly, physical qubits). DLR (Germany's Aerospace Center) will receive the bulk of this funding (740M€) to work with small, mid-sized and large companies and create two related consortia.

The Federal government is not the only public body funding quantum research. The Bavaria region funds quantum technologies with an impressive budget of 300M€ to develop the Munich Quantum Valley, mostly in research institutions. How is that possible? German Landers (regions) have a very large budget independent from the Federal government (in a 42%/58% ratio). Bavaria being a large Lander, they have the means to invest significantly on research.

Like with each and every country, the German quantum plan covers quantum computing, communications and sensing.

Germany funds several key quantum computing projects: GeQCoS, DAQC, JUNIQ and QUASAR.

**GeQCoS** (German Quantum Computer based on Superconducting Qubits) with 14,3M€ BMBF funding, involving Fraunhofer Fribourg and Infineon). It was launched in February 2021 and will seemingly use German born technologies.

---

<sup>1665</sup> In Germany, the federal agency that protects information systems, which is the counterpart of the French ANSSI, published in May 2018 the report [Entwicklungsstand Quantencomputer](#) (*State of the art of quantum computing*), which provided an update on quantum computing, focusing in particular on cybersecurity issues (231 pages, in English). This was a very good overview of global quantum computing research. It provided a surprisingly accurate inventory of efforts in the field, particularly in US public research. But things have changed a bit since 2018.

<sup>1666</sup> See [German Government Allocates €650M for quantum technologies](#), the [German government's announcement](#) (in German) and [the plan itself](#) (51 pages).

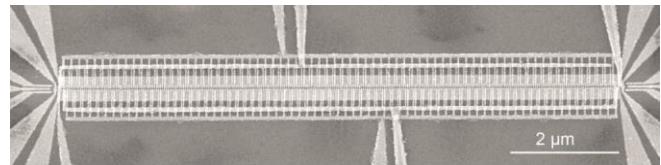
<sup>1667</sup> See [Germany: 2 Billion euros for quantum technology](#), June 2020.

**DAQC** was also launched in February 2021 and got 12.4M€ from BMBF. It is coordinated by IQM Germany and involves Jülich, Infineon and Parity QC from Austria as well as the Leibniz Computing Center and Free University of Berlin. It will create a digital-analog superconducting qubits system using IQM's architecture. This project is related to the Quantum Flagship OpenSuperQ project.

**JUNIQ** (Jülich UNified Infrastructure for Quantum computing) is an initiative from the Jülich Supercomputing Centre. It deployed a D-Wave quantum annealer in 2019 with 10M€ public funding, half from the BMBF and half from the Bavarian region. It's the first D-Wave installed in Europe.

**QUASAR** is a semiconductor-based project using shuttling electrons with a QuBus (*pictured next*), a quantum bus to transport electrons and their quantum information over distances of 10 µm. The partners are Infineon, HQS, Fraunhofer (IAF, IPMS), Leibnitz Association (IHP, IKZ) and the Universities of Regensburg and Konstanz. The project will run until 2025 to create 25 coupled qubits.

The resulting computer is to be deployed at JUNIQ. Jülich is also participating to the European Flagship QLSI project driven by CEA-Leti in France. QUASAR got a 7.5M€ funding from BMBF<sup>1668</sup>.



Germany also launched the creation of two QKD-based telecommunications networks, both funded by BMBF:

**QuNET** (165M€) which uses a standard QKD associated with terrestrial and satellite links. The project involves several Fraunhofer Institutes including the Heinrich Hertz Institute (HHI), the Max-Planck Institute for the Physics of Light and the German Aerospace Center (DLR)<sup>1669</sup>.

The project launched in November 2019 was scheduled to last seven years and aims to create a communications protection infrastructure for the German government. This should lead to the creation of a secure European network. The private sector is also involved with Deutsche Telekom, ADVA Optical Networking and Tesat-Spacecom. Test sites will be implanted in Bavaria, Saxony and Thuringia.

**Q.Link.X** (14.8M€) for the creation of a terrestrial network in optical fiber and QKD based on quantum repeaters, managed by the Fraunhofer HHI<sup>1670</sup>.

Germany also leads or participates to various European Flagship programs: **MetaboliQs** (NV center based medical imaging), **UNIQORN** (photon qubits chipsets), **S2QUIP** (hybrid photonic chipsets), **QRANGE** (QRNGs).

At last, the German national plan is funding three other initiatives associating research labs and industry vendors: **BrainQSens** (medical imaging with NV centers, 2,8M€), **Opticlock** (compact optical clock to synchronize communication networks, 6M€) and **QUBE** (space QKD with Cube-Sat, 3,12M€).

---

<sup>1668</sup> See [Quanten-Shuttle zum Quantenprozessor "Made in Germany" gestartet](#), Jülich, February 2021.

<sup>1669</sup> See [Germany's QuNET Receives €165 Million To Establish Quantum Communications Infrastructure](#), 2019, [German ministry and research sector join forces to launch major quantum communications initiative](#), May 2019 and [German Aerospace Center In QuNET Working On Satellite-Based Quantum Communication](#), November 2019.

<sup>1670</sup> See [Germany splashes further €15m in quantum networks R&D project](#), October 2018.

## Quantum industry

On the private sector side, Germany has a variety set of quantum startups including **Avanetix** (hybrid algorithms), **InfiniQuant** (CV-QKD cryptography), **PicoQuant** (photon counters), **Kiutra** (magnetic cryogenics), **HQS Quantum Simulations** (algorithms), **JoS Quantum** (software in finance), **Quantum Factory** (ions trapped in the cloud), **QuantiCor Security**, **QuBalt** (both in post-quantum cryptography) and **QuTools** (sensing).



Many of the country's major industrial companies are also interested in quantum applications, particularly in chemistry (**BASF**), health (**Merck**), telecommunications (**Deutsche Telekom**), components and automotive (**Bosch**, **Daimler**).

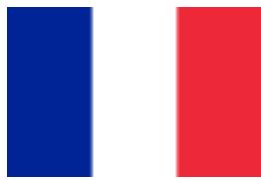
**PlanQK** (Platform and Ecosystem for Quantum-Assisted Artificial Intelligence) is a project to build a market place of quantum assisted artificial intelligence components, at first, quantum inspired algorithms. It gathers scientists from various universities (Stuttgart, Berlin, Munich) on top of Accenture, HQS, Deutsche Bundesbahn, Deutsche Telekom and other industries. It is supported by BMWi with a total funding of €19M.



In June 2021, ten German companies created **QUTAC** (Quantum Technology and Application Consortium) to develop quantum computing usable industrial applications in the technology, chemical and pharmaceutical, insurance and automotive industries.

The consortium was launched by BASF, BMW Group, Boehringer Ingelheim, Bosch, Infineon, Merck, Munich Re, SAP, Siemens, and Volkswagen. One of its goals is to create a cross-industry application portfolio. Let's also mention **PushQuantum**, a students initiative born in Munich that organizes lectures, workshops and entrepreneurship labs for wannabe quantum entrepreneurs.

## France

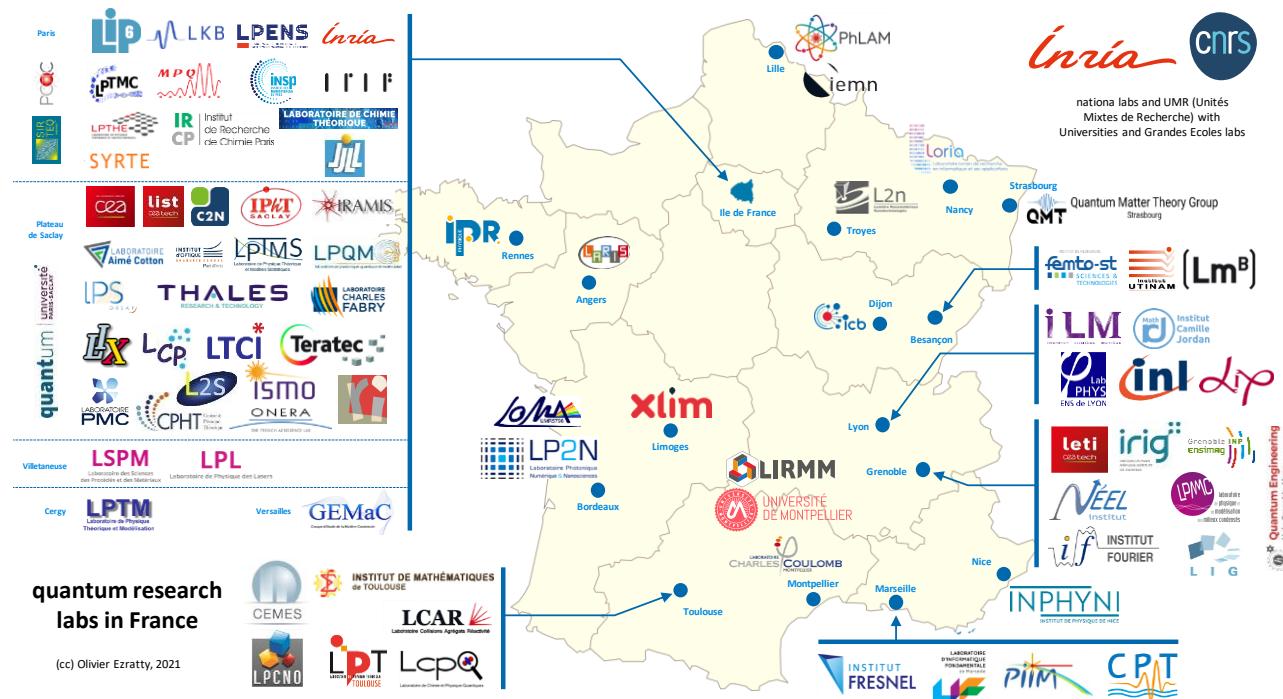


France has a good breadth of research and industry activities in quantum technologies. Let's first mention its greatest scientists with **Henri Poincaré** (1854-1912), **Louis de Broglie** (1892-1987, Nobel prize in physics in 1929), **Alfred Kastler** (1902-1984, Nobel prize in physics in 1966), and **Claude Cohen-Tannoudji** (1934, Nobel prize in physics in 1997).

**Serge Haroche** (1944, Nobel Prize in Physics in 2012) is a pioneer in cavity quantum electrodynamics and on the interaction between photons in a superconducting cavity and Rydberg atoms passing through the cavity). Of course, we can add **Alain Aspect** (1946), who invalidated Bell's inequalities in 1982 and verified the principle of non-locality of entangled photons, a cornerstone of the second quantum revolution. A former PhD student of Alain Aspect, **Philippe Grangier** is a world specialist in quantum cryptography.

## Research

Public research is organized around three national research organizations: **CNRS**, **CEA** and **Inria**. The first is involved in fundamental research in physics, mathematics and algorithms. The second also does fundamental research in physics, particularly on superconducting qubits, and applied research on electron spins qubits as well as on photonics. At last, Inria is doing research in computer science, and for quantum technologies, on quantum error correction, cryptography and quantum algorithms. Many laboratories are joint research units between universities and these national organizations.



These research laboratories are mainly located in Ile de France and in Grenoble, but other regional locations are active such as Toulouse, Montpellier, Marseille, Lyon, Bordeaux, Besançon and Lille<sup>1671</sup>. Like many large countries, French laboratories are exploring many qubit tracks: superconducting, cold atoms, electron spins, photons and topological matter.

Public sector researchers get projects funding by answering various country and European RFPs<sup>1672</sup>. Of the more than 20 quantum startups in France 2021, 7 are from CNRS, two from Inria, two from ENS and one from CEA.

### Ile de France

Ile de France is home to a good half of the country's research laboratories devoted to quantum technologies. Let's start with the laboratories that are located within Paris.

<sup>1671</sup> For this purpose, I consulted the websites of these laboratories and the fields of research they present, plus, when they were easy to find, the scientific publications of the researchers of these laboratories.

<sup>1672</sup> Some obtain ERC Grants (European Research Council): Synergy Grants for a few handfuls of teams (up to €14M over 6 years), and more often Starting (young researchers, up to €1.5M), Consolidators (experienced researchers, up to €2M) and Advanced (emeritus researchers, up to €2.5M spread over 5 years). Then European FET funding, funding via the European Quantum Flagship, or finally through various calls for projects at the national level (ANR).

Inria's efforts in the Paris region are concentrated in the Quantic (Quantum Information Circuits) team of Pierre Rouchon, Mazyar Mirrahimi, Zaki Leghtas and Alain Sarlette, which is a joint venture between the CNRS, ENS and the Ecole des Mines de Paris.

They work on mathematical models of superconducting qubits, on quantum error correction (including cat-qubits), on proof of superiority of quantum algorithms and on cryptographic issues<sup>1673</sup>. The Cosmiq team led by Anne Canteaut, works on cryptographic algorithms, and David Pointcheval's Cascade team, works in cryptography and PQC. Inria also jointly runs many other teams with various labs from CNRS.

IQA (LTCI, Saclay) is working on networking aspects in quantum computing, cryptography and photonics and quantum machine learning, QI with LIP6, MOCQUA with LORIA, CAPP (LIG, Grenoble) on contextuality and quantum combinatorial games, AlgoComp with IRIF, MC2 with LIP Lyon and PACAP with IRISA and Inria Rennes working on mapping quantum circuits to particular architectures and the new QUACS team on quantum algorithms.



**LIP6** (Laboratoire d'Informatique de la Sorbonne) hosts several recognized specialists in cryptography and quantum telecommunications (QKD): Eleni Diamanti was awarded a European Synergy Grand ERC for her work in the QUSCO (Quantum Superiority with Coherent State) project. Elham Kashefi is co-founder of the VeriQloud startup. She is also working on verified quantum computing, secure multiparty quantum computing, and features to achieve quantum advantages.

The **LPENS** (Laboratoire de Physique de l'Ecole Normale Supérieure) is the result of the merger in early 2019 of several physics research laboratories at ENS Paris, including the **LPA** (Laboratoire Pierre Aigrain), which specializes in nanotechnology and photonics.

They are working on numerous nanotechnologies used for the creation of qubits and the transport of quantum information: superconducting thin films, superconducting and microwave circuits for their control, two-dimensional electron gases with very high mobility, semiconductor quantum boxes, qubits based on carbon nanotubes.

Taki Kontos and Audrey Cottet's teams are at the origin of the creation of carbon nanotubes used as electron traps potentially usable in electron spin qubits, which led to the creation of the **C12** startup, already mentioned. The lab is also a participant on the work on cat-qubits related to the startup Al-ice&Bob.



The **LKB** (Laboratoire Kastler Brossel) from ENS Paris focuses on quantum information and photonics, interactions between light and matter (Nicolas Treps and Valentina Parigi), quantum simulation and precision sensing with cold atoms (Christophe Salomon).

Thibault Jacqmin is working on microwave photon generation with NEMS (nano MEMS).



The **IRIF** (Institut de Recherche en Informatique Fondamentale) from CNRS and the University Paris Diderot is led by Frédéric Magniez who also teaches at Collège de France and hosts Iordanis Kerenidis, Sophie Laplante and two Inria teams. It works in quantum computing, cryptography and communications.

<sup>1673</sup> This is specified in Inria [strategic scientific plan 2018-2022](#), 2018 (93 pages), pages 47 and 48.



Philippe Goldner is working on the creation of qubits based on nanocrystals doped with rare earth ions such as europium or erbium, and is involved in the SQUARE project of the European Quantum Flagship, coordinated by the Karlsruhe Institute of Technology and also involving Thales. The laboratory is also involved in the European Quantum Flagship ASTERIQS project which is working on NV-based qubits in diamonds.

The **LPEM** (Laboratory of Physics and Study of Materials) of the ESPCI and the UMPc works in particular in superconductivity as well as on the fermions of Majorana.



The **MPQ** laboratory (Materials and Quantum Physics) of the University Paris Diderot is particularly interested in the technique of ions trapped in the Quantum Physics and Devices (QUAD) and QITE (Quantum Information and Technologies) groups. But also, to the generation of entangled photon pairs (Sara Ducci).

The **LPTHE** (Laboratoire de Physique Théorique et Hautes Energies) of the University Paris Sorbonne works in condensed matter and statistical physics with applications in superconducting qubits.

The **INSP** (Institut des Nanosciences de Paris) of Paris-Sorbonne University is a generalist laboratory on nanosciences. They work in particular in different branches of photonics, on NV centers, on color centers qubits in silicon carbide, on spin and magnetism and on photonics components in III-V materials.

The **IRCP** (Institut de Recherche de Chimie Paris) associated with the Ecole Nationale Supérieure de Chimie ParisTech conducts research in innovative materials.

The **LPEM** (Laboratory of Physics and Study of Materials) of the ESPCI and the UMPc works in particular in superconductivity as well as on the fermions of Majorana.

The **LPTMC** (Laboratoire de Physique Théorique de la Matière Condensée) of the University Paris-Sorbonne does not seem to be involved in quantum physics in relation with quantum computing. Nevertheless, they are interested in the simulation of the living, which is one of the key applications, in the long-term, of quantum computing.

The **SYRTE** (Laboratoire Systèmes de Référence Temps-Espace) located at Paris Observatory works in quantum sensing, in particular gravimetry, quantum gyroscopes and on time measurement with atomic and optical clocks. They are partnering with NIST. The quantum gravimeter and interferometry team is led by Franck Pereira dos Santos. SYRTE is led by Arnaud Landragin.

The **Laboratoire Jacques Louis Lions** (LJLL) is specialized in applied mathematics. It focuses on the analysis, modeling and high-performance scientific computation of phenomena represented by partial differential equations. Mario Sigalotti and Ugo Boscain, who specialize in the control of quantum systems and are also members of Inria, are among others.

The **Laboratory of Theoretical Chemistry** at Sorbonne University is directed by Jean-Philippe Piquemal (co-founder of Qubit Pharma) and is interested in computational chemistry, including quantum.

In September 2020, the **Quantum Innovation Center Sorbonne** (QICS) was inaugurated, a collaborative research structure associating LIP6, the LKB of the ENS and Inria.

The **Saclay plateau** has an even higher density of laboratories, located south-west of the Paris region. Most of these entities are consolidated in **Université Paris Saclay**.



At the **CEA**, Daniel Esteve's Quantronics team at the Iramis laboratory in Saclay has been working on superconducting qubits for nearly 20 years. Daniel Esteve's laboratory includes about fifteen people.



**IphT** (Institut de Physique Théorique de Saclay) associates CEA and CNRS. They work on the physics of condensed matter, including high-temperature superconductors, and on Majorana fermions. But their main focus seems to be mainly astrophysics.



The **LAC** (Laboratoire Aimé Cotton) is located at the ENS Saclay. It also works on cold atoms and interactions between atoms and light. In particular, they create qubits by combining an optically active erbium ion and a nuclear spin of yttrium.



The **C2N** (Centre des Nanosciences et des Nanotechnologies) of CNRS and Université Paris Saclay is a key quantum photonics laboratory. It is the home to Pascale Senellart and Jacqueline Bloch's labs. They work in particular on light-matter coupling in semiconductors. It also host quantum electronics teams (Frédéric Pierre).



The **LPS** (Laboratoire de Physique des Solides) works on magnetism, Josephson junction superconductors, thermodynamics, superconducting spintronics and quantum dynamics. They also develop codes for quantum and semi-classical dynamics and quantum control with applications in quantum information.



The **LPTMS** (Laboratoire de Physique Théorique et de Modèles Statistiques) has several strings to its bow in quantum physics without the link with quantum computing being immediately detectable.



The **LCP** (Laboratoire de Chimie Parisud) works on superconductors and on the dynamics and control of ions trapped by laser pulses. They develop hybrid computational models of quantum chemistry (quantum+traditional) using MCTDH (Multi-configuration time-dependent Hartree) which allows to solve the Schrödinger equation for the simulation of interactions between atoms in molecules.

On the program: condensed matter physics, modeling of classical and quantum systems via statistical physics, quantum chaos, number theory and quantum chaos, theoretical aspects of quantum information; cold atoms, quantum integrable systems, quantum groups, etc.



TelecomParistech's **LTCI** (Laboratoire Traitement et Communication de l'Information) is an industry laboratory operating with partnerships with the private sector and via chairs. Its "Quantum Information and Applications" (QIA) team specializes in the theoretical and experimental aspects of quantum communications.

They develop hybrid CV-QKD-based quantum cryptography protocols compatible with telecom operators' fiber networks and QKD repeaters. They are contributor, founding member and reporter to the ETSI QKD-ISG on the QKD standardization processor. The team is led by Isabelle Zaquine and includes Romain Alléaume.



**ISMO** (Institut des Sciences Moléculaires d'Orsay) works on quantum dynamics, interactions between heavy particles and electrons at low temperature, light/matter coupling and on software for the simulation of quantum physics.



The **CPhT** (Centre de Physique Théorique de Polytechnique) is specialized among other things in the physics of condensed matter. But not to the point of creating superconducting qubits! We find there Karyn Le Hur's group, who is specialized in condensed matter physics.



The **Charles Fabry Laboratory** of the Institute of Optics Graduate school (IOGS) is specialized in lasers and quantum optics. It is home to Alain Aspect, Philippe Grangier as well as Antoine Browaeys, co-founder of the startup Pasqal and its laser-controlled cold atom qubits.



The **LIX** (Laboratoire d'Informatique de l'Ecole Polytechnique) is particularly active in post-quantum cryptography algorithms.



The **PMC** (Laboratoire de Physique de la Matière Condensée) is another laboratory of the Ecole Polytechnique. They work in particular on spin dynamics in semiconductors and magnetic thin films.



The **L2S** (Signals and Systems Laboratory) of CentraleSupélec is active in quantum systems research. In particular, the L2S is staffed by Zeno Toffano, who is focused on quantum states measurement.



The **LPQM** (Laboratory of Quantum and Molecular Photonics) associates the ENS Paris Saclay and the CentraleSupélec school. Their domains are coherence and quantum correlations.



The **LRI** (Laboratoire de Recherche en Informatique) located at CentraleSupélec is managed by Benoît Valiron, who teaches and conducts research in quantum computing, a field that is still relatively under-taught in engineering schools.



Thales **RT** (Thales Research and Technology) carries out R&D to create industrialized quantum sensing solutions. In particular, they have developed expertise in diamond NV centers.



**Onera** studies quantum optics at its Palaiseau site. It is in this capacity that it coordinates the ASTERIQS project of the European Quantum Flagship, "Advancing Science and Technology through diamond Quantum Sensing".

They also have teams of researchers in photonics, in III-V semiconductor materials (gallium, ...) with a prototype manufacturing unit located in their premises in Palaiseau, in metrology (gravimeter, atomic clock, accelerometer) and in QKD.

Let's move on to other parts of the Ile de France: Cergy-Pontoise, Villetaneuse and Versailles.



The **LPTM** (Laboratoire de Physique Théorique et Modélisation) of the University of Cergy-Pontoise is interested in cold atoms, in liaison with the Institut Francilien de Recherche sur les Atomes Froids (IFRAF). They also study graphene, electronic quantum transport, topological phases and entanglement.

The **LSPM** (Laboratoire des Sciences des Procédés et des Matériaux) of the University of Paris 13 in Villetaneuse is working on the manufacturing processes of NV centers, carbon nanotubes and graphene centers and associated applications.

The **LPL** (Laboratoire de Physique des Lasers) of the University Paris 13 in Villetaneuse works in photonics and cold atoms, their traps and on quantum metrology. It is the laboratory of Hélène Perrin, already mentioned, who is its Deputy Director.

The **GEMaC** (Groupe d'Etude de la Matière Condensée) of Versailles also works in the field of diamonds and graphene, on spin electronics and magnetism. It also works on QKD and photonic quantum memory.

Launched in 2014, the **Paris Center for Quantum Computing** (PCQC) brings together several dozen researchers from various laboratories in the Paris region, including Philippe Grangier. The CNRS has informally grouped its efforts with the [Quantum Computing working group](#) which works more on the algorithmic dimension.

Finally, the **SIRTEQ** (Science and Engineering in the Ile de France Region for Quantum Technologies) is a community that groups research laboratories in the Ile de France region that are focused on quantum communications technologies. According to them, there are 650 quantum researchers in the Ile-de-France region in all (physics, algorithms, telecommunications, cryptography) spread over 100 teams in 30 research laboratories.

We can also mention the initiative of the high-performance computing cluster **Teratec** (based in Bruyère le Chatel, near the CEA's Military Affairs Department) around quantum physics<sup>1674</sup>.

It aims to develop quantum algorithms, hybrid development methods, use cases, and to inform, train and animate a community. They benefit from an Atos QLM simulator installed at the CRTT (Centre de Calcul, Recherche et Technologie) of the CEA in Bruyères-le-Châtel.

### Grenoble

Grenoble's quantum ecosystem is dense, well-organized and very focused on the creation of qubits based on electron spins but also on superconductors, all with good skills in photonics. It is probably the place where coordination between research teams works best, particularly by integrating the key stages of industrialization.

<sup>1674</sup> Teratec brings together several private and public HPC players including Atos, CEA, CERFACS (European Center for Advanced Research and Training in Scientific Computing), Dassault-Aviation, EDF, IFPEN, PCQC (Paris Centre for Quantum Computing), Total and the University of Reims.

Quantum research in Grenoble is led by different branches of the CEA (Leti in nanoelectronics and IRIG in fundamental physics), the CNRS with Institut Néel, LPMMC and two joint CNRS and CEA teams: NPSC (NanoPhysics and Semiconductors) focused on quantum sensing, quantum photonics, quantum thermodynamics and the quantum foundations, and Quanteca, created in 2019, which deals with all kinds of solid states qubits (electron spins, superconductors).



**CEA-Leti** (Electronics and Information Technology Laboratory) in Grenoble is the CEA's micro and nanoelectronics laboratory. It is notably at the origin of the SOI wafer technology that led to the creation of SOITEC. Leti is focused on CMOS electron spin qubit engineering. The project is coordinated by Maud Vinet and federates the efforts of several CEA, CNRS and UGA laboratories.



The **IRIG** (Grenoble Institute for Interdisciplinary Research) is the counterpart of Institut Néel in fundamental research at CEA. It includes the Laboratory PHotonique ELectroneRique et Ingénierie QuantiqueS (PHELIQS), which works on the physics of condensed matter.



**Institut Néel**<sup>1675</sup>, launched in 2007, is a CNRS laboratory specialized in condensed matter physics with a critical mass of researchers in quantum physics. Its researchers are exploring the possibilities of electron spin qubits (Tristan Meunier), superconducting qubits (Nicolas Roch), topological matter (Adolfo Grushin) and photonics. It also works on thermodynamics and the energetics of quantum computing (Alexia Auffèves), cryogenics (Sébastien Triqueneaux) and quantum foundations (Cyril Branciard and also Alexia Auffèves).



The **LPMMC** (Physics of Condensed Matter) of the University Grenoble Alpes is a CNRS UMR focused on the theoretical physics of condensed matter and quantum physics, N-body quantum interactions, superconductivity and superfluidity, and on the temporal evolution of quantum systems under the effect of magnetic and electric fields.



The **IJF** (Institut Joseph Fourier) of the University of Grenoble is working on quantum dynamics and in particular on issues of decoherence and thermal quantum noise.

---

<sup>1675</sup> The institute takes its name from Louis Néel (1904-2000, French), a physician of Lyon origin who was awarded the Nobel Prize in Physics in 1970 for his studies on magnetism and the discovery of antiferromagnetism. He is at the origin of the creation of the Polygone Scientifique de Grenoble, which brings together numerous research institutes and companies in the peninsula between the Isère and Drac rivers. The place hosted the first CEA site outside the Paris region in 1956, launched by Louis Néel. The CNRS established a foothold there in 1962, and in 1967 CEA-Leti was created. CEA-Leti is one of the world's largest civilian laboratories for applied research in nanoelectronics and nanotechnology. The Grenoble Science Park is also home to several international research organizations, the Institut Laue-Langevin, the European Synchrotron Radiation Facility and one of the branches of the European Molecular Biology Laboratory. In 2005 the CEA-Liten was created, a branch of the DRT specialized in new energies (photovoltaic solar, batteries, fuel cells, complete management of the carbon cycle, mixed energy management, innovative materials). In 2006, Minatec was launched, a nanotechnology commercial development center, later complemented by the Minalogic competitiveness cluster. In 2012, the Clinatec research center, founded by Alim-Louis Benabid, was launched, which is at the origin of the first complete exoskeleton for tetraplegics.



The **LIG** (Laboratoire d'Informatique de Grenoble) is interested in quantum algorithms in general. One of its members is the researcher Mehdi Mhalla, who works on the quantum resolution of graph problems.

Research in quantum computing in Grenoble is currently structured around three initiatives: **QuEnG**, **QuantECA** and **QuCube**, which are not on the same level.



**QuEnG** (Quantum Engineering Grenoble) is an ecosystem ranging from philosopher to industrialist. It is a trans-laboratory, trans-disciplinary and trans-sectoral umbrella initiative. The teams are working in physics on many other fields: in photonics, on superconducting qubits, electron spin qubits and qubits based on molecular magnets. They also delve into questions of thermodynamics. Alexia Auffèves, from the Institut Néel of the CNRS, is a great specialist in this field and is the coordinator of QuEng. Teams also make the link between quantum physics and philosophy with Vincent Lam. The initiative also includes training engineers in physics and quantum computing with various courses, including a project with Ensimag, Grenoble's leading computer science school. In 2021, it is evolving into **QuantAlps**.

**QuantECA** or Quantum Electronic Circuits Alps is an initiative launched in 2019 covering the large-scale integration of qubits in chips.

It brings together CEA-Leti, the physics department of IRIG and Institut Néel. Their field of action is the creation of stable, scalable qubits.

They are also working on quantum information storage and transport technologies. They rely on three technological branches (superconducting/photonics/electron spin/flying electrons). In particular, they master a technology integrating optomechanics in CMOS circuits. CMOS is part of the effort. It is within Quanteca that the team of Maud Vinet, Tristan Meunier and Silvano De Franceschi is located, having obtained an ERC Synergy Grant for the QuQube project.

**QuCube** is the initiative that got a €14M ERC Synergy Grant funding at the end of 2018. Its goal is to create a quantum computer with more than 100 qubits in less than 10 years in CMOS / electron spin technology.

### *Lyon*

Research in Lyon is well balanced between the physical part and the mathematical and software part of quantum.



The **Physics Laboratory of ENS Lyon** studies condensed matter. The Quantum Circuit Group of Benjamin Huard is working on superconducting qubits and their error correction codes. He was notably joined by Audrey Bienfait in 2019, who works on electron spin resonance and its applications in quantum sensing. It was also there that Théau Peronni finalized his thesis in 2020 while creating the startup Alice&Bob with Raphaël Lescanne.



The **INL** (Lyon Nanotechnology Institute) is located at Centrale Lyon (Ecully). They work on semiconductors and photonics. They have a technological platform for component prototyping, particularly in photonics.



The **iLM** (Institut Lumière Matière) of Lyon is specialized as its name indicates in photonics.



The **Camille Jordan Institute** in Lyon is a research laboratory in mathematics that works in particular on quantum probabilities. It is distributed on several sites: Villeurbanne, Saint-Étienne and on the Centrale Lyon campus in Écully.

The **LIP** (Laboratoire de l'Informatique du Parallelisme) of ENS Lyon associates CNRS, Inria and Claude Bernard Lyon 1 University. Its MC2 team works on theoretical computer science and complexity theory. It includes Omar Fawzi, CNRS 2019 bronze medalist and specialist in quantum information theory. He leads his work in the MC2 team at LIP.

### *Occitanie*

Quantum research in Toulouse is very focused on fundamental physics and quite far from quantum computing with the exception of **LPTT**. There are also two laboratories in Montpellier, one of which is associated with IBM. Let's mention the **QuantUM Hub** initiative launched by IBM Montpellier, the University of Montpellier, and the Occitanic Region.



The **Institute for Quantum Technologies in Occitanie** was created in January 2021 to consolidate all the Occitan research and industry organizations, including the research labs below from Toulouse and Montpellier.

The **CEMES** (Centre d'Élaboration de Matériaux et d'Etudes Structurales) in Toulouse is specialized in physics and optronics. It is interested in light-matter coupling at scale and the creation of sensors oriented more towards connected objects than quantum applications.

**LCAR** (Laboratoire Collisions-Agrégats-Réactivité) of the Paul Sabatier University of Toulouse works on Rydberg atoms. It is in the team of Juliette Billy and David Guéry-Odelin.

The **LPCNO** (Laboratory of Physics and Chemistry of Nano-objects) of INSA Toulouse is specialized in photonics and quantum electronics. They study electron and nucleus spins, quasi-particles and quantum dots. They aim at applications in quantum computing. Their research is looking at applications in the health sector.

The **ITM** (Institut de Mathématiques de Toulouse) of the University of Toulouse studies statistical and quantum physics. It is home to Clément Pellegrini who studies quantum information theory and quantum state measurement.

The **LPTT** (Laboratoire de Physique Théorique de Toulouse) works on superconductors and SQUID Josephson effect loops. Small peculiarity, they are involved in the Quantware project which has been co-funded among others by the NSA!



Laboratoire de Chimie et Physique Quantiques



The **LCPQ** (Laboratory of Quantum Chemistry and Physics) of the Paul Sabatier University of Toulouse develops generalist quantum chemistry codes, contributing to molecular simulation efforts.

The **L2C** (Charles Coulomb Laboratory) of the University of Montpellier is working on quantum metrology, spin dynamics and graphene, with applications in magnetic microscopy.

The **University of Montpellier** is an IBM partner in the setting up of a joint laboratory on quantum which actually aims to evangelize customers on the general principles and tools of the IBM Q quantum platform.

The **LIRMM** (Montpellier Laboratory of Computer Science, Robotics and Microelectronics) focuses in particular on the creation of quantum algorithms. It collaborates with IBM, Total and CERFACS.

Aida Todri-Sanial is one of their Research Director and works on quantum algorithms used for classical integrated circuits routing and on classical algorithms improving qubits gates mapping taking into account calibration data<sup>1676</sup>.

#### Nouvelle Aquitaine

The Nouvelle Aquitaine ecosystem is specialized in sensing and enabling technologies like lasers, with its industry ecosystem comprising **Muquans**, **Azur Light Systems** and **ixBlue**. Since March 2021, this ecosystem is federated under the umbrella **Naquidis**, as part of the AlphaLRH cluster and with the support of the Region.

Besides the local branch of IOGS (Institut d'Optique Graduate School), here are two quantum research labs in the region.



The **LP2N** (Laboratoire Photonique, Numérique et Nanosciences) of the Institut d'Optique de Bordeaux does research in photonics and metrology based on cold atoms (microgravitometry). This is where the startup Muquans started.



The **LOMA** (Laboratoire Ondes et Matières) from CNRS works on quantum matter and is investigating, among other things, nanomechanical qubits based on carbon nanotubes.



The **XLIM** (Limoges) does among other things photonics. They are notably partners with Thales TRT. They are working on applications in polariton metrology, in particular SPR (Surface Plasmon Resonance).

#### Sud

There are also a few quantum physics laboratories in Marseille, three of which are directly related to the needs of quantum computing. And one laboratory in Nice.

<sup>1676</sup> See [A Hardware-Aware Heuristic for the Qubit Mapping Problem in the NISQ Era](#) by Siyuan Niu, Aida Todri-Sanial et al, October 2020 (14 pages).



The **Fresnel Institute** of Marseille is involved in photonics, so inevitably, it can contribute to advances in photon-based qubit management and QKD-based quantum cryptography.

The **CPT** of the Universities of Marseille and Toulon is working on quantum dynamics and wave diffusion in optical fibers and light guides. They are partners of various foreign universities: Aalborg University (Denmark), Pontificia Universidad Católica de Chile, Karlsruhe Institute of Technology (Germany), Kyoto Institute of Technology and the Moscow Institute of Physics and Technology.

The **PIMM** (Physics of Ionic and Molecular Interactions) laboratory at the University of Marseille does research in plasmas, more related to the ITER nuclear fusion project than to quantum computing.

The **Laboratoire d'Informatique Fondamentale** de Marseille is particularly interested in quantum computing. Their Discrete Time Quantum Simulator project was launched in 2018. They are working on Quantum Walks and the Quantum Cellular Automata.

**INPHYNI** (Institut de Physique de Nice) of the Université Nice Côte d'Azur is interested in cold atoms, wave transport, interactions between light and atoms. It deploys a QKD test network between Nice in Sophia-Antipolis since 2019 in partnership with Orange. The quantum laboratory is directed by Sébastien Tanzilli.

### Burgundy Franche-Comté

Besançon is home to three quantum laboratories and Dijon to a fourth.



The **LmB** (Laboratoire de Mathématiques de Besançon) of the Université Bourgogne Franche-Comté studies quantum groups and probabilities.

The **UTINAM** Institute of the University of Besançon studies quantum decoherence, control, diagnosis, processing and transport of quantum information in the field of quantum sensing.

**Femto-St** is a research institute in Besançon focused on nanosciences, optics and optoelectronics. They work in particular on optical telecommunications, non-linear optics, optics-based Ising machines and quantum imaging.

**Icb** (Interdisciplinary Carnot of Burgundy) of the University of Burgundy, based in Dijon, includes a team studying quantum and nonlinear dynamics (DQNL).

### Great East

The region includes three quantum laboratories located in Strasbourg, Nancy and Troyes.



The **Quantum Matter Theory Group** from the University of Strasbourg is involved in condensed matter physics and also works on the interactions between light and matter, with Rydberg atoms. Run by Shannon Whitlock, the lab is developing cold atom-based quantum systems.

The **L2n** (Lumière Nanomatériaux Nanotechnologies) of the Technology University of Troyes is specialized in optoelectronics and photon sources.

The **Loria** (Lorraine Laboratory for Research in Computer Science and its Applications) is based in Nancy. Two teacher-researchers are interested in quantum computing and algorithms: Simon Perdrix and Emmanuel Jeandel. The first is one of the main contributors of ZX Calculus. Since 2021, Simon Perdrix is a PI at Inria Nancy.

### Elsewhere in France

And finally, here are a few quantum physics laboratories located in other regions, in Rennes, Lille, Bordeaux and Limoges, but with no apparent direct link to quantum computing.



The **IPR** (Institut de Physique de Rennes) is attached to the University of Rennes. They are interested in quantum dynamics, the evolution of quantum states over time.

The **LARIS** (Laboratoire Angevin de Recherche en Ingénierie des Systèmes) based in Angers deals with various IT subjects. Within it, François Chapeau-Blondeau and Etienne Belin are interested in the impact of noise on quantum algorithms.

The **PhLAM** (Laboratoire de Physique des Lasers Atomes et Molécules) in Lille is interested in photonics and cold atoms.

The **IEMN** (Institute of Electronics, Microelectronics and Nanotechnology) is a laboratory located on four sites in Lille, Villeneuve d'Ascq and Valenciennes. They specialize in the design of quantum nanostructures.

### International collaborations

International partnerships are very common in research. Many of the works of French researchers are carried out with researchers from other countries, including the USA, the UK, Austria, the Netherlands and Germany, Japan and Singapore (notably with joint international units of the CNRS IFLI and Majulab).

CEA-Leti is a partner of **IMEC**, its counterpart in Belgium, based in Leuven, covering AI and quantum computing<sup>1677</sup>. Like CEA-Leti in Grenoble, they have a clean room for etching up to 28 nm on 30-cm wafers and another on 20-cm wafers for MEMS.

Since 2017, the **Grenoble University Space Center** has been collaborating with the Austrian **IQOQI** on sending quantum keys via satellite in the Nanobob project.

<sup>1677</sup> See [Partners Double-Team AI & Quantum Computing](#) by Mathew Dirjish, November 2018.

And there is another international collaboration on quantum involving France, the Netherlands (QuSoft) and Latvia.

### ***Government funding***

After Atos launched in 2015/2016 its venture in quantum computing emulation, the French government started to look at the opportunity to launch a quantum plan. Back then, it was involved in the European Quantum Flagship which was announced in October 2018.

Things really started with the creation of a parliamentary investigation commissioned by the Prime Minister in March/April 2019 and led by **MP Paula Forteza**, accompanied by **Iordanis Kerenidis** (CNRS researcher specialized in quantum machine learning) and **Jean-Paul Herteman** (former CEO of Safran). The parliamentary mission submitted its report on January 9, 2020, titled "Quantum: the technology disruption that France will not miss". The report made fifty proposals, 37 of which were made public. The government then created a national quantum strategy that included some but not all of the parliamentary mission's proposals. All this during the early stages of the covid pandemic. It was finally announced a bit late, in January 2021, but by President Emmanuel Macron, a premiere in the western world.



The ambitions of the strategy and its roadmap revolve around rather classical themes : NISQ quantum computing, Fault Tolerant Quantum Computing (FQC, with a potential bet on silicon qubits), algorithms and software, quantum telecommunications overall (including quantum cryptography and distributed quantum computing), quantum sensing, and at last, enabling technologies. This includes cryogenics, cabling, control electronics, vacuum control, lasers and photon sources.

The plan is spread over 5 years from 2021 to 2025 with 1B€ public funding and an additional 850M€ funding expected from European funds and the private sector (industry and startups funding).

### ***Quantum industry***

On the startup scene, the country has a handful ventures in quantum computing hardware front with **Alice&Bob** (cat-qubits), **C12** (carbon nanotubes electron spins qubits), **Pasqal** (cold atoms qubits) and **Quandela** (single photon sources and photons qubits).

In the software side, we have **Qubit Pharmaceuticals** (healthcare), **QuantFi** (finance), **VeriQloud** (quantum telecommunications) and **Prevision.io** (quantum machine learning) plus a bunch of companies specialized in cryptography, mostly PQC with **CryptoNext**, **CryptoExperts**, **Ravel** and **Secure-IC**.

In quantum sensing, we have **Muquans** (microgravimeters, acquired by **iXblue** in 2021) and **Thales** (NV centers, SQUIDs and cold atoms sensing, lightweight cryogeny).

In addition to **Bpifrance** and the investment fund **Quantonation**, the **Deep Tech Founders** trains entrepreneurs/researchers in deep techs. It is an international program created by the Hello Tomorrow team. All these are behind the creation of a structure to support the quantum ecosystem in partnership, the **Lab Quantique**, launched officially in April 2020.

The Lab Quantique is a think tank for the development of talent, particularly at the crossroads between science and entrepreneurship. From a practical point of view, Lab Quantique organizes regular meetings that bring together mainly quantum technology entrepreneurs from France and abroad. These meetings took place in the form of videoconferences on Zoom during the covid-19 pandemic period in 2020 and 2021. Its objectives are to connect industry players, startups and researchers, to build bridges with the international community, to launch a program to accelerate quantum startups and to organize a major annual high-level conference bringing together all the stakeholders in the ecosystem, as well as an International Prize (attracting talent). In the end, it will also take the form of a trade association mixing the quantum industry (large organizations, small businesses and startups) and its users (mainly, large companies like EDF, Airbus and the likes).

One France specificity in Europe is its large corporations directly invested in quantum technologies and quantum enabling technologies : **Atos** (software, emulators, quantum accelerators), **Thales** (sensors), **Air Liquide** (cryogenics), **Orano** (isotopes production like silicon 28), **Radiall** (cabling) and many in photonics (like **iXblue**, **Azurlight Systems**, **Aurea Technology**, **Lumibird** and **Cailabs**) and even semiconductor manufacturing machines with **Plassys Bestek** and **Riber**.



Of course, France also hosts **Atos** which started its venture in quantum computing in 2016 under the leadership of Thierry Breton with creating emulation tools including a server QLM and development tools. They plan to become integrators of quantum accelerators and classical supercomputers to build hybrid solutions.

## Netherlands

The Netherlands is also active in quantum, mainly around the University of Delft (TU Delft).

It has long been a historical melting pot of quantum physics research in Europe. We have thus cited many great names at the beginning of this ebook: **Hendrik Antoon Lorentz** (1853-1928), **Heike Kamerlingh Onnes** (1853-1926), **George Uhlenbeck** (1900-1988), **Hendrick Casimir** (1909-2000) and **Samuel Goudsmit** (1902-1978).

In 2015, the government launched a 10-year, 135M€ plan to create a quantum computer<sup>1678</sup>. The investment was made in **QuTech**, TU Delft's quantum research center launched in 2014 with a 10-year budget of 145M€, half of which comes from TU Delft University and the other half from the NWO, the national funding agency<sup>1679</sup>. QuTech employs more than 180 people in all, of which only 37% are Dutch, with 25 permanent researchers.

The Netherlands government then announced a 7 years 615M€ plan in April 2021. This public funding should drive private sector investments of 3.6B€, a very ambitious goal in comparison with the similar 565M€ expected in France. It is managed by the non-profit foundation **Quantum DELTA NL** that was created in 2020<sup>1680</sup>. The Netherlands plans to create 30.000 high-tech jobs and create a cumulative economic impact of at least 5B€ with quantum technologies. The country plan is organized around the creation of three technology demonstrators, four generic action lines and shared cleanroom facilities.

- **Quantum Inspire**, their cloud superconducting computer service that is already available and got a funding of 90M€.
- **Quantum Network** project on quantum telecommunications and cryptography, connected to the related European projects, with a funding of 62M€. They expect to quantumly connect three quantum computers by 2023 and five by 2026.
- **House of Quantum** is a startup ecosystem facility to open in 2024 with a budget of 182M€. It would accelerate part of the 100 startups the country wants to consolidate by 2027. Within this house, the **Living Lab QT** that will focus on ethical, legal and societal aspects of quantum technology with research collaborations between universities, the public and private sector, with a funding of 20M€. They will open two related interdisciplinary university positions, create a desk and a toolkit for responsible innovation and entrepreneurship and create a covenant to be signed by private and public stakeholders promoting sustainable and safe use of quantum technologies.
- **LightSpeed** is a program connecting startups with investment funds. It's overselling a bit its value touting access to 13.6B€ in investment capital, representing the totality of the various funds managed by these investors.
- They also plan to invest 150M€ in the 5 cleanrooms from **NanoLabNL**, have a quantum sensors plan with 23M€ funding and a training program that should create 2000 PhDs and engineers by 2027 with a funding of 41M€.

QuTech is also associated with **Intel** and **Microsoft**. QuTech has received \$50M in funding in 2015 from Intel as part of a partnership on their superconducting and electron spin qubits.

Microsoft has also been a partner of QuTech since 2010, which they have also depleted by hiring **Leo Kouwenhoven** in their Microsoft Research laboratory which is on site and working on topological quantum and fermion of Majorana in liaison with a team of QuTech dedicated to the same subject. The Netherlands looks like a brain reservoir for the American quantum industry.

Collaborative research approaches are making good progress, particularly with a view to recovering European funding.

---

<sup>1678</sup> See the state of play of the Dutch National Quantum Plan in [National Agenda for Quantum Technologies](#), Quantum Delta Netherlands, September 2019 (51 pages).

<sup>1679</sup> See QuTech's [2018 Activity Report](#) (80 pages) as well as an [independent valuation report](#) published in 2019 and covering the period 2015-2018.

<sup>1680</sup> See the plan details in [Quantum Delta NL in a nutshell](#), 2021 (20 pages). Look also at the excellent [Economic Impact of Quantum in the Netherlands](#), Quantum Delta NL, May 2020 (60 slides) which contains a lot of interesting market data. DELTA stands for Delft Eindhoven, Leiden, Twente and Amsterdam, completed by Nijmegen, Maastricht and Groningen.

In October 2017, QuTech launched a partnership with the Institute of Photonic Sciences, the University of Innsbruck in Austria and the Paris Centre for Quantum Computer. QuTech is also a partner of the University of Aachen in the CMOS qubit. The University of Delft has also obtained for the European part of the QuNET project mentioned about Germany an ERC of 1,5M€ with a launch in November 2019 and an end planned for October 2024<sup>1681</sup>.

Other initiatives with blurred contours have been launched such as **Quantum Helix**, funded under the European Quantum Flagship Program and Horizon 2020. The **Quantum Software Consortium** runs for 10 years from 2017 and has received €18.8M in public funding from the country's Gravitation Program. It brings together various Dutch laboratories: **TU Delft**, **QuTech** (part of the latter), **QuSoft** (a research laboratory dedicated to quantum software, launched by CWI, UvA and VU in 2015), **CWI** (Centrum Wiskunde & Informatica), the **University of Leiden**, **UvA** (University of Amsterdam) and **VU** (Free University of Amsterdam) to conduct research in quantum software and cryptography.

Other companies include **Delft Circuits** (superconducting cabling), **Leiden Cryogenics** (high-power dilution cryostats), **Qblox** (electronics for controlling superconducting qubits), **Single Quantum** (single photon detectors), **QuiX** (photonic processor, a subsidiary of Lionix, a foundry capable of producing photonics wafers in nitrates on SiO<sub>2</sub>), **Qu&Co** (quantum software), **QuSoft** (quantum software), **QPhoX** (quantum computer interconnection) and **ipClock** (quantum clock).

In December 2020, the Dutch quantum industry created the **IMPAQT** consortium. The first members are Orange QS, Qblox, Delft Circuits, QuantWare BV (a new stealth spin-off from TU Delft creating superconducting QPUs) and Qu&Co. Their goal is to improve the coordination of how they are creating quantum computer enabling technologies.

At last, The Netherlands and France signed in September 2021 a Memorandum of Understanding to expand collaborations in quantum technologies, with Cédric O, the French Secretary of State for Digital and Electronic Communications and Mona Keijzer, the Dutch Secretary of State for Economic Affairs and Climate Policy. The bilateral collaboration includes research partnerships in silicon qubits as part of the European flagship project QLSI, research-industry collaboration involving companies like Atos and Qu&Co, the creation of a joint portal listing job opportunities in France and the Netherlands ([www.quantumjobs.fr](http://www.quantumjobs.fr) and [quantumjobs.nl](http://quantumjobs.nl)) and collaboration to increase EU venture capital in the domain (involving Quantonation).

## Belgium



Belgium is the host of the famous Solvay conferences created in the early 20<sup>th</sup> by Ernest Solvay. Their presence in the quantum science and technology scene is exemplified by **IMEC**, the international semiconductor and nanotechnologies research center based in Leuven, an equivalent to CEA-Leti in France, with 4000 employees.

**IMEC**'s quantum technology activities are centered on producing superconducting and electron spin qubits on behalf of various laboratories and vendors as well as some cryoelectronics systems. Among other projects, they participate to the European Quantum Flagship QLSI project that is co-ordinated by CEA-Leti. They announced in August 2021 a partnership with **Xanadu**, for the development of fault-tolerant photonic qubits chipsets based on silicon-nitride.

Let's also mention the **Centre for Quantum Information and Communication** from the Free University of Brussels (Vrije Universiteit Brussel). It works on quantum measurement, quantum entanglement, quantum communication, quantum cryptography and quantum algorithms.

<sup>1681</sup> See [A quantum network for distributed quantum computation](#), Cordis, 2019.

It has also worked on continuous-variable quantum cryptographic protocols, and developed quantum adiabatic algorithms.

In the vendor space, I have identified a company that was already mentioned, **QBee.eu**, a quantum accelerator and incubator created by Koen Bertels, who leads the Quantum Computer Architectures Lab in TU Delft and also works at Qutech.

## Austria



Austria's investment in quantum computing is concentrated in the **IQOQI**, the Institute for Quantenoptik und Quanteninformation in Innsbruck and Vienna. It focuses in particular on the design of qubits based on trapped ions. This led to the start-up **Alpine Quantum Technologies**, founded by Rainer Blatt of the IQOQI, to commercialize quantum computers based on trapped ions.

It has received €12.3M in public funding. It competes with the **IonQ** (USA), which is positioned in the same niche of ion-trapped qubits, as well as **Honeywell**. In June 2021, the Austria government announced a new 5-years funding of \$127 for research in quantum technologies.

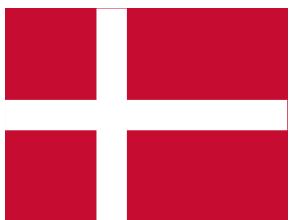
The Vienna Center for Quantum Science and Technology (**VQC**) is a partnership between the University of Vienna, Vienna University of Technology and the Austrian Academy of Sciences. It brings together a critical mass of about 20 quantum physics research laboratories.



Austria is also invested in quantum cryptography and is associated with China, with whom it has conducted experiments in sending quantum keys via the Micius satellite to set up secure video communication.

**IQOQI** is collaborating with the **Grenoble University Space Center** (CSUG) in the development of a CubeSat-type quantum key relay satellite, similar to the one in Singapore, in the **Nanobob** project ([presentation](#), 13 slides).

## Denmark



Quantum research in **Denmark** is organized around the Center for Quantum Devices (**QDev**) at the Niels Bohr Institute at the University of Copenhagen. It is a quality laboratory focused in particular on topological qubits, with its director Charles M. Marcus who also works for Microsoft Research in this field jointly with the MSR teams of Leo Kouwenhoven in the Netherlands.

QDev is a laboratory of physicists focused on the study of condensed matter, i.e. the physical lower layers of qubits, as can be seen in [their publications](#).

The team seems to be only a dozen people. Unfortunately, they cannot then rely on Danish or European industrialists to consider the transfer of their research into the production of quantum computers. This is a French but also a European problem!

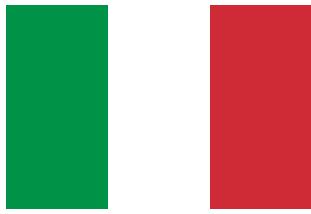
## Sweden



On the **Swedish** side, there is mainly the WACQT (Wallenberg Centre for Quantum Technology) which is part of the **Chalmers University** of Gothenburg and is co-financed by the Wallenberg Foundation. The WACQT has been funded under a 12-year plan with over \$100M. As in all countries, the center targets all quantum technologies domains (computing, communications and sensing).

In particular, they are invested in superconducting qubits as well as in continuous variable qubits. They plan to create a 100 qubits superconducting computer. WACQT is also working on cold atom qubits from Rydberg... named after a Swedish physicist! Finally, it has launched a "Women in WACQT" initiative to develop gender diversity in quantum science. In March 2021, the Wallenberg budget nearly doubled to \$9M per year, allowing the hiring of 40 more researchers.

## Italy



Italy has a very active research in place in various technologies in quantum computing. Photon qubits are explored by **Fabio Sciarrino** at Università La Sapienza in Rome. He is an European pioneer of boson sampling experiments and wants to make it programmable. And the **Università di Padova** launched its own Quantum Technologies Research Center that works on trapped ions computing.

**Francesco Tafuri** from the Università Federico II in Naples works on superconducting qubits. The Italian National Institute for Nuclear Physics (INFN) is also working with the US DoE on superconducting quantum materials at the FermiLab in Chicago, which happens to be run by Anna Grassellino, an Italian.

In the quantum communication realm, **Paolo Villoresi** from the Instituto Nazionale di Ricerca Metrologica in Turin pioneered photons polarization encoding with a satellite in 2015. Italy also deployed its **Italian Quantum Backbone** (IQB) with a total of 1,850 km fiber link based on commercial fibers. It connects INRIM's premises in Turin to Milan, Bologna, Firenze, Rome, Napoli, Pozzuoli and Matera. From Turin, a 150 km fiber reaches Modane in France, and connects to Grenoble, Lyon and Paris, then Europe.

The big shortcoming of Italy is its weak private sector with not many industry vendors and startups engaged in quantum technologies.

As part of its recovery plan announced in April 2021, the Italian government allocated a budget of 1.6B€ to fund 7 new research organizations, one of these being focused on quantum technologies<sup>1682</sup>.

## Spain



On the research side, most of Spain's efforts are concentrated in the **ICFO** (Instituto de ciencias fotónicas) of Barcelona, which is mainly specialized in photonics. Other research in quantum is carried out at the Quantum Information and Computation Laboratory (GIC-UB) of the **University of Barcelona** as well as the **Autonomous University of Barcelona**<sup>1683</sup>.

<sup>1682</sup> See [Italy's quantum scientists jostle for a superposition](#) by Francesco Suman, April 2021.

<sup>1683</sup> See [Quantum Technologies in Catalonia](#), July 2019 (43 slides) which describes very well the quantum ecosystem of this key region of Spain.

The **IFAE QCT** is the Quantum Technology Group from the IFAE (Institut de Fisica d'Altes Energies) from the Autonomous University of Barcelona opened its new lab and fab in October 2020.

On the startup scene, they have a startup, **Qilimanjaro** already mentioned, which develops mainly a cloud-based quantum software platform and a superconducting quantum annealer. Their chipset is manufactured at the IFAE. And they have **Entanglement Partners**, a service provider that is clearly succeeding in selling quantum-related cybersecurity services.

They also animate the country's ecosystem, do evangelization and organize events. In 2017, the open innovation platform **Open Trends** launched **The Carrot Cake** to encourage projects in the quantum field. This complements the **Barcelona QBIT** think tank launched in 2015 and the **Quantum World Association** launched at the MWC 2017, which brings together Switzerland, Canada, Australia and Catalonia with startups such as ID Quantique, evolutionQ, h-bar and Entanglement Partners. Spain is networking, having realized that it could not go very far on its own.



## Portugal



Portugal's key investment in quantum technologies sits with **QuantaLab**, a collaborative research center launched by **International Iberian Nanotechnology Laboratory** (INL) and the **Universidade do Minho**, both in Braga, Portugal. It focuses on quantum materials and quantum technologies. Portugal is also participating to European quantum projects including the QCI (Quantum Communication Infrastructure).

## Poland

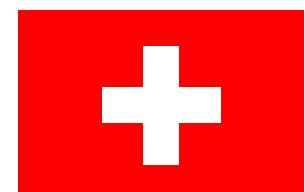


**Poland** has a Quantum Physics Research Center in Gdansk that focuses on quantum cryptography. It was launched in 2007. The University of Warsaw is also very involved in quantum research. The Polish National Science Centre also coordinates the international research network **QuantERA**, itself funded by the European Union's Europe 2020 budgets.

It does this in coordination with the French ANR. The countries involved, in addition to those of the European Union, are Switzerland, Israel (Bar-Ilan University) and Turkey.

About thirty research projects had been funded after a call for proposals in 2017, some of which were subsequently funded in the European Quantum Flagship, such as SQUARE. They are all quantum physics projects (photonics, cold atoms, ...).

## Switzerland



Switzerland is also mobilized on quantum technologies, particularly at **ETH Zurich**, which is collaborating with IBM and especially on quantum cryptography, notably with its startup **IDQ**, which is a leader in quantum random numbers generation used in quantum cryptography and elsewhere. And also with the Lausanne's **EPFL**.

The country has published a manifesto to promote its research and industrial efforts in quantum, [Switzerland: At the Quantum Crossroads](#). The **Swiss Quantum Hub** brings together the Swiss quantum ecosystem.

The **Quantum Science and Technology Initiative** (QIST), a joint initiative of ETH Zurich and the University of Basel, which also involves the University of Geneva and EPFL Lausanne, has 34 faculty members and 300 students. It has been funded with \$120M between 2010 and 2017.



It covers all the usual fields of quantum with, with a particular effort in quantum telecommunications. In August 2021, the EPFL launched through its own multidisciplinary Quantum Science and Engineering Center consolidating its research and academic efforts in all branches of quantum technologies.

The **Swiss Quantum Investor Club** was created in 2020 to link investors and quantum entrepreneurs and organize events in Geneva, Lausanne and Zurich, as well as the **Swiss Quantum Hub**, a think tank and accelerator for quantum startups, and the Quantum Computing Garage, a permanent hackathon.

In November 2020, Martin Haefner, an alumnus from ETH Zurich donated \$44M to the ETH Foundation to have them build a quantum research facility. We could wish more wealthy people would make such long-term investments for their community! In another similar initiative, ETH Zurich and the Paul Scherrer Institute (PSI) created in 2021 a joint quantum computing research center, focused on ion traps and superconducting qubits with the goal to host 30 researchers. ETH Zurich invested \$36M there<sup>1684</sup>.

## European Union



The **European Union** wants to consolidate its effort in quantum technologies. A "flagship project" germinated in 2016 and was formally launched in October 2018 to fund collaborative research on all aspects of quantum information: sensing, communications, computing and simulation<sup>1685</sup>. It is theoretically endowed with 1B€ to be used for the development and diffusion programs of quantum technologies, spread over 10 years.

In theory, because the budgets have not really been allocated at this level by the European Union. This Flagship is currently mainly focused on quantum computing fundamental physical. It has not yet looked at algorithms and software.

This **Quantum Technologies Flagship** is one of the three European "flagships" that aim to place Europe at the forefront of major technological breakthroughs with strong community investment in research. The two other flagships are the "Human Brain Project" led by the Swiss Henri Markram and the Graphene project in nanotechnologies. The first phase of the Flagship included €132M spread onto 20 projects selected out of 140 applicants and for a period of three years. 130 additional projects will be later selected.

---

<sup>1684</sup> See [ETH Zurich and PSI found Quantum Computing Hub](#), May 2021.

<sup>1685</sup> See the motivations behind the European Flagship: [The Impact of quantum technologies on the EU's future policies: Part 1 Quantum Time](#), 2017 and [Part 2](#).

Launched by the European Commission on October 29, 2018 in Vienna ([videos](#)), the program covers the four usual quantum domains: computing, simulation, communication and sensing<sup>1686</sup>.

Let's look at these projects. These projects involve an average of at least half a dozen countries, even partner countries like Switzerland and Israel.



It starts with three side projects related to quantum computing:

- **OpenSuperQ** (Germany, €10.33M) is a superconducting qubit computer project led by Saarland University that also involves Spain, Sweden, Switzerland and Finland and a total of 10 research laboratories. The ambition is to create a 100-qubit system. IQM is the probable vendor who will provide the quantum system for this project.
- **AQTION** (Austria, €9.57M) is trapped ions qubit computer project, planning to reach 50 qubits. Austria has a long history here and is quite legitimate. Atos is participating in this project.
- **MicroQC** (Bulgaria, €2.36M) plans to create another trapped ions computer.

Then we have four quantum simulator projects :

- **PASQuanS** (Germany, €9.25M) is a quantum simulator project based on cold atoms and trapped ions up to 1000 qubits. It also involves the UK, Atos and Pasqal.
- **PhoQuS** (France, 3M€) is a photonic based quantum simulator. It is led by a team of PSL researchers. It involves the use of polaritons.
- **Qombs** (Italy, €9.3M) is another photonics-based quantum simulator project.

<sup>1686</sup> See the [Press Kit](#) (28 pages), the [complete list of projects](#) and [Europe Accelerating the Industrialization of Quantum Technologies](#), October 31, 2018, the title of which is somewhat misleading in that the majority of projects funded are research projects and not industrialization projects. And then there is [The quantum technologies roadmap: a European community view](#), October 2017 (25 pages), which takes stock of the state of the art in Europe and around the world. See also [The EU Quantum Technology Flagship](#) by Elisabeth Giacobino, 2018 (41 slides and [video](#)).

- **SQUARE** (Germany, €2.99M) a quantum simulator project using trapped ions. It is led by the University of Karlsruhe and involves laboratories from Denmark, Sweden, Spain and France, including Thales. It seems that they are also seeking to create a quantum processor with universal gates.

Let's continue with projects in quantum communication and telecom security.

- **Quantum Internet Alliance** (Netherlands, €10M) (QIA) aims at deploying an Internet network protected by quantum key distribution (QKD) in mesh network mode and not just point-to-point. The quantum nodes or relays will be made up of systems using cold atoms. They will start with a three or four-node network. The project is led by TU Delft University. The CNRS participates in it, notably Eleni Diamanti, Elham Kashefi and Iordanis Kerenidis. The Sorbonne University also participates. Other participants include Swiss, Germans, Danes and Austrians ([complete list](#)).
- **QRANGE** (Switzerland, €3.87M) is a project to improve quantum random number generation techniques.
- **CiViQ** (Spain, €9.9M), or Continuous Variable Quantum Communications, is another QKD-based fiber telecommunications security project. The project involves 21 stakeholders covering the academic and industrial world, including CNRS, Institut Mines-Telecoms, Nokia Bell Labs France, Inria, Orange, as well as Mellanox.
- **Uniqorn** (Austria, €9.9M) is in the same niche and is working on a random number generator and a QKD system. It associates 17 organizations from 9 countries (Austria, Netherlands, Italy). The Israeli Mellanox is also involved there.
- **S2QUIP** (Netherlands, 3M€), Scalable Two-Dimensional Quantum Integrated Photonics, is another QKD-based secure communication project.
- **2D-SIPC** (Spain, €2.9M) is a project for the development of photoelectronic components made for networks secured by QKDs.
- **QMICS** (Germany, 3M€) or "Quantum Microwave Communication and Sensing" is about creating a microwaves-based links and networks between superconducting network nodes with applications in distributed quantum computing and also in quantum sensing.
- **NEASQC** (NExt ApplicationS of Quantum Computing) is a collaborative project launched in September 2020, to develop practical applications of NISQ (noisy quantum computers, an intermediate step before scalable quantum computers). It is an H2020 project that brings together European players including Atos, Total, EDF, the Loria laboratory from the University of Lorraine, AstraZeneca, HQS Quantum Simulations, HSBC and the University of Leiden (Netherlands).

Then we have five quantum sensing projects already seen in the section starting on page 661.

There is also the **QFLAG** project (Germany, €3.48M) which is managing the coordination for European Quantum Flagship projects.

At last, a new project was awarded in March 2020 to fund four years of fundamental research in silicon qubits. This **QLSI** project is being driven by the Grenoble team under the responsibility of Maud Vinet at CEA-Leti. The project funding is 14M€ spread over 19 organizations: Atos, STMicroelectronics, SOITEC, CNRS Institut Néel, TU Delft, University of Twente and TNO in the Netherlands, IMEC in Belgium, UCL and Quantum Motion in the UK, Infineon, RWTH Aachen, University of Konstanz, Fraunhofer and IHP Frankfurt in Germany, University of Copenhagen and University of Basel.

We note the strong predominance of projects piloted by German research laboratories (5), followed by the Netherlands (3), France (3), Spain (2), Austria (2), followed by Italy, the UK and Switzerland, all driving a single project. Large countries are present in many of these projects. As an example, France is involved in many of these projects. CNRS (France) alone is involved in 14 of the 20 projects<sup>1687</sup>. These projects do not yet include efforts in software, to create algorithms, development tools and business software solutions adapted to quantum computers. Such projects will probably be funded in subsequent phases<sup>1688</sup>.

But other European quantum projects are funded with other vehicles than the Flagship.



**QuantERA I** (2014) and **II** (2021) is an alliance of research funders from member states created to reinforce transnational collaborations in inspiring multidisciplinary quantum research. The QuantERA II Consortium assembles 38 Research Funding Organizations from 30 countries, some being extra-EU. It complements the Quantum Flagship in early stages, serving as an incubator of new ideas which then can get integrated in Quantum Flagship projects but comes from participating countries (45M€ for QuantERA I and 40M€ for QuantERA II) and the EU (11.5M€ for QuantERA I and 15M€ for QuantERA II). There were two calls for projects in QuantERA I and one in QuantERA II with a selection done late 2021 and projects funding starting in 2022.

**EQUIPE** (Enable Quantum Information Processing in Europe) project aims to advance the industrialization of the creation of quantum computing and telecommunications solutions for industry<sup>1689</sup>.

**EuroHPC** projects include quantum computing deployments in hybrid datacenters with deployments planned in Germany and France.

European research is federated under the umbrella of **QCN** (Quantum Community Network). Its industry counterpart is the **QuIC** (Quantum Industry Consortium) announced in June 2020 and formally launched in April 2021<sup>1690</sup>. Founding members are companies that were involved in at least two European Quantum Flagship projects.

They include Bosch, SAP, Atos, Thales, Muquans, Airbus and many others. The consortium has an extensive work plan covering market needs assessment, analysis of the quantum technology value chain, development of standards and regulations, sharing of best practices in intellectual property protection and market evangelization, access to infrastructure, linking startups and investors, skills development issues and coordination with public authorities.

---

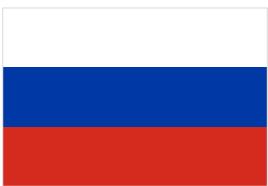
<sup>1687</sup> See [New Strategic Research Agenda on Quantum technologies](#), February 2020 (114 pages) which details the state of play of the European Quantum Flagship projects.

<sup>1688</sup> See [The Quantum Technologies Flagship: the story so far, and the quantum future ahead](#) by Thomas Skordas and Jürgen Mlynek, October 2020 which looks at the flagship progress two years after the program started.

<sup>1689</sup> See [Simulation on / of various types of quantum computers](#) by Kristel Michielsen (40 slides).

<sup>1690</sup> See [Announcing the creation of the European Quantum Industry Consortium](#) by Laure le Bars (SAP), the first President of QuIC, April 2021.

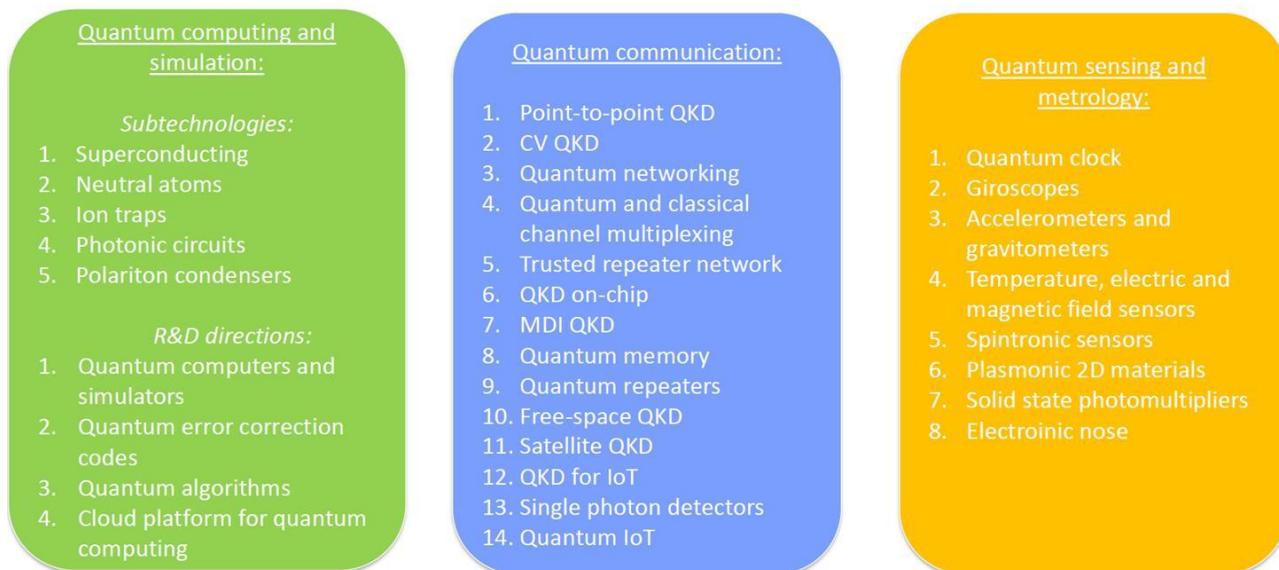
# Russia



Russia is not very visible in the quantum scene, maybe because they have not built the same research and industry partnership that are seen in the western world. But like with AI, its government realized that quantum technologies were critical for sovereignty. In December 2019, Russia announced its own plan of attack on quantum technologies, which seemed very focused on military, intelligence and cryptanalysis applications<sup>1691</sup>.

This plan got a five-year funding of \$790M. In practice, it covers almost all fields of quantum technologies<sup>1692</sup>.

## Data Economy: “Quantum technologies”. Main directions (2019-2024)



Source: roadmap draft “Data Economy: Quantum technologies”, 2019



Before all of that, the **Russian Quantum Center** was created in 2010, a private research center dedicated to the various application areas of quantum computing, including quantum cryptography. It employs over 200 researchers.

It covers many quantum computing branches: superconducting, trapped ions, photons and NV centers qubits, quantum sensing, QKD and a single photon detector. They collaborate with some international research organizations in the USA (MIT), Canada (University of Calgary), Germany (Max Planck Institute for Quantum Optics) and UK (University of Bath)<sup>1693</sup>.

The St. Petersburg **ITMO University** has a QKD research laboratory as well as the **Kazan Quantum Center** which has deployed a QKD on a 160 km network in Kazan. The country also plans to launch a QKD quantum key communication satellite in 2023. A few other laboratories are invested in quantum technologies such as the **NTI Center for Quantum Communications** at MISiS University and the **NTI Technologies Centre** at Moscow University.

<sup>1691</sup> See [Russia joins race to make quantum dreams a reality](#) by Quirin Schiermeier, December 2019.

<sup>1692</sup> Source: [Quantum communication in Russia: status and perspective](#) by Vladimir Egorov, 2019 (22 slides).

<sup>1693</sup> This information comes from [Evaluation Report of Russian Quantum Center](#), 2017 (7 pages). See also [Quantum technologies in Russia](#), October 2019 (9 pages).

Industry wise, they are mostly in quantum cryptography with only one startup, **Qrate Quantum Communications**, the others being established companies, such as **Infotecs**, **Scontel** and **Smarts QuantTelecom**<sup>1694</sup>.

## Near and Middle East

### Israel



**Israel** was relatively quiet about quantum technologies until 2018 apart from Gil Kalai from the Hebrew University of Jerusalem who, since 2013, has shown a deep-rooted skepticism about the future of quantum computers. They have a visible startup in the field, **Quantum Machines**, focused on qubit control hardware and software.

After a study carried out in 2017 by Uri Sivan (Technion) to evaluate the country's quantum technologies efforts, a first initiative to better fund its research was launched in 2018 by the country's government and endowed with €75M. It went mainly to Technion, the University of Haifa, which wants to design its own quantum computer and had also received a donation of \$50M. This Quantum Information Processing lab works on many tracks, in photonics and silicon qubits.

Quantum research is also on the agenda of the Quantum Information Science Center at the Hebrew University of Jerusalem, which was established in 2013 and focuses on secure quantum communication (QKD).

Bar-Ilan Nanotechnology University in Ramat Gan near Tel Aviv has its own quantum laboratory, the **QUEST** (Quantum Entanglement in Science and Technology), launched in 2017 and visibly invested in low-level quantum physics and especially quantum communication.

In July 2019, the **Ben-Gurion University of the Negev** (BGU) announced a partnership with the Israeli Ministry of Defense on quantum technologies, without specifying the targeted applications. The startup **Accubeat** (1993), which produces rubidium quantum atomic clocks, is a product of this university.

Google's R&D lab in Tel Aviv includes researchers in quantum computing.

In December 2019, a panel of specialists commissioned by the government proposed a plan to invest \$350M over 6 years in quantum technologies<sup>1695</sup>. In just a few months, the government approved this proposal. The plan is fairly standard with an investment in human capital (faculty hiring and launching training courses), research and scholarships funding, attracting foreign researchers and the likes. The emphasis is made on quantum computing hardware and components, quantum telecommunications and cryptography, as well as quantum sensing, particularly in its military applications. The plan is coordinated by the former Chief Scientist of the Ministry of Industry between 1996-2000, Orna Berry.

As in the USA, this plan was born thanks to a well-orchestrated lobbying campaign, since we often see a certain David Malits, the CEO of DM Communications, a public relations company, advocating quantum technologies in various media<sup>1696</sup>.

---

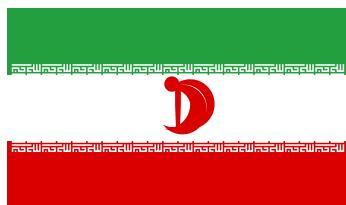
<sup>1694</sup> Here are some elements on this ecosystem: [Quantum communication in Russia: status and perspective](#) by Vladimir Egorov, 2019 (22 slides).

<sup>1695</sup> See [Israel joins the quantum club](#) by Uri Berkovitz, December 2019 and [Israel joins the race to become a quantum superpower](#) by Anna Ahronheim and Maayan Hoffman, Jerusalem Post, December 2019.

<sup>1696</sup> See for example [Israeli Government To Allocate \\$350 Million For Quantum Computing](#) by Analytics India Magazine, December 2019.

In March 2021, Israel announced it planned to create its own quantum computer, allocating a budget of \$60M taken out of the \$350M national plan launched in 2019. The goal is to create a 30- to 40-qubit quantum system. It will take bids from both local players and international companies. Meaning creating can lean on build or buy depending on the outcome.

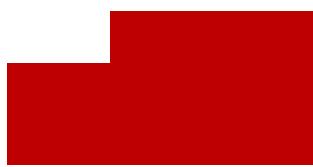
## Iran



Israel is not the only country in the Near and Middle East that seems to be invested in quantum research. Iran is also involved with at least two research laboratories, **Sharif University** which is working on quantum physics in partnership with Canada and the **Quantronics Lab** of the Iranian Technological University which is dedicated to quantum communication (QKD)<sup>1697</sup>.

The country even organizes its conference on quantum computing, the **IICQI**, since 2007<sup>1698</sup>.

## Abu-Dhabi



Each and every country wants « its » quantum computer. Even the emirate Abu-Dhabi got the quantum virus and decided to “build” its own quantum computer, even if “build” or “buy” are interchangeable in such a situation since it is a quantum annealing superconducting system coming from Qilimanjaro.

Still, it comes after the establishment of a Quantum Centre at the Technology Innovation Institute (TII) which hosts about 20 researchers coming from the Emirates and from various countries: Italy, Spain, Brazil, Greece, UK and Germany. This lab complements other labs in robotics, cybersecurity and energy. It even has some qubits manufacturing tooling.

Jose Ignacio Lattore is the chief scientist of this quantum research laboratory. He is a professor of theoretical physics at the University of Barcelona currently on leave, cofounder of Qilimanjaro and the director of the Singapore CQT since July 2020. Their key partners are Qilimanjaro, Universitat Catania in Sicilia and INFN, an Italian research network.

The QC-TII organized a webinar conference in June 2021, Atomtronics@Abudhabi with about 500 participants.

## Asia-Pacific

### China



As in many technology sectors, **China** is loudly and clearly asserting its ambitions and power in quantum technologies<sup>1699</sup>. As in the UK, this investment was taken in hand early on by the executive and as early as 2013 with the involvement of Xi Jinping, the Chinese president, during a visit to the Anhui laboratory, focusing on quantum cryptography, combined with a training session.

<sup>1697</sup> Source: [Iranian research in quantum information and computation](#), June 2016.

<sup>1698</sup> See <http://iicqi.sharif.edu/>.

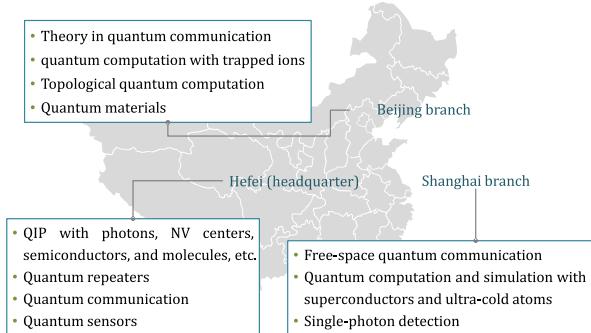
<sup>1699</sup> See [Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership](#), CNAS, 2018 (52 pages) and [Quantum information technology development in China](#) by Yuao Chen, June 2019 (25 slides).

## Government funding

In 2015, Xi Jinping integrated quantum communication into the country's scientific priorities, in 13th plan covering 2016-2020. Maybe was it a benefit from having a government comprising a majority of politicians with some scientific background and also the result of Snowden's revelations on NSA's spying capabilities in 2013.

The amounts invested in quantum were respectively \$160M in the 11th plan covering the period 2006-2010, \$800M in the 12th plan covering 2011-2016 and \$320M in the 13th plan starting in 2016, supplemented by \$640M in funding from the regions<sup>1700</sup>. Later on, the Chinese government communicated an amount of \$34B corresponding to several scientific priorities including quantum. In practice, this represented probably less than \$1B between 2016 and 2020 and a total of \$1.76B over 10 years. Other [estimates](#) are lower, in the \$1.5B range for the 2006-2020 period. So, all the impressive billion dollars figures related to China's quantum technologies investments have to be taken with a grain of salt. In 2021, China announced its new five year research plan, with a 11% global funding increase but with no details regarding quantum investments.

Operations jointly supported by the CAS and the Ministry of Education



These investments are mainly spread over Beijing, Shanghai and Hefei (500 km west of Shanghai). They specialize respectively in quantum communications, trapped ion computing, topological qubit computing and quantum materials for Beijing, silicon qubit computing, NV centers and photons, quantum communications and metrology in Hefei, and communication, superconducting and cold atom qubit computing and photon detection in Shanghai.

The Chinese plan is coordinated by the **USTC** (University of Science and Technology of China) of the Chinese Academy of Sciences (CAS) and under the leadership of Jian-Wei Pan<sup>1701</sup>. The most ambitious project is the “\$10B” research center that partially opened in 2020, the **NLQIS** (National Laboratory for Quantum Information Sciences) of Hefei. This laboratory is focused on quantum computing and metrology for military and civilian applications.



It will employ 1800 research people, including 560 full-time researchers spread across two labs, three universities and a fab ([source](#)).

<sup>1700</sup> The 2016 quantum roadmap is available in "Quantum Leap: The Strategic Implications of Quantum Technologies by Elsa Kania and John Costello ([part 1](#) and [part 2](#)). See also [Chinese QC Funding](#) by Xiaobo Zhu, 2017 (35 slides).

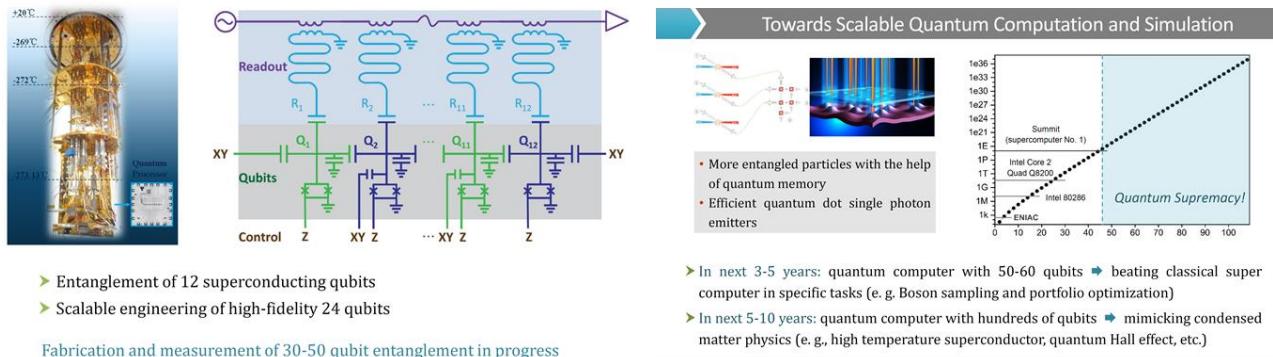
<sup>1701</sup> See [The man turning China into a quantum superpower](#) by Martin Giles in MIT Technology Review, December 2018.

But it seems this research center is also dedicated to research in artificial intelligence. So, again, the related investment amounts are certainly not entirely dedicated to quantum technologies.

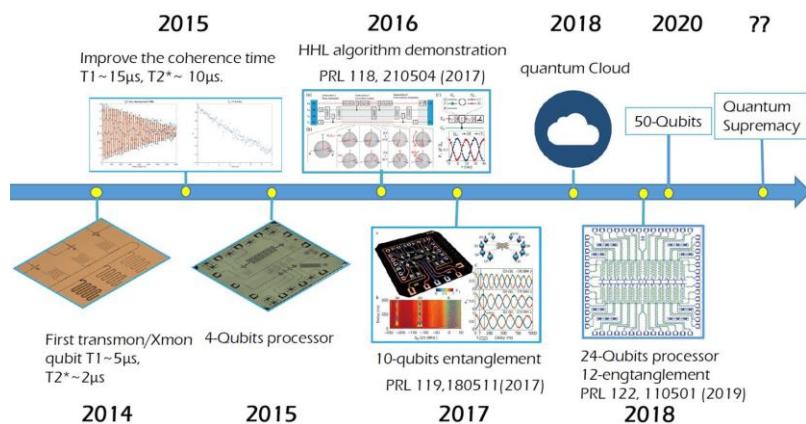
## Research

On the quantum computing side, Chinese laboratories are testing all imaginable qubit technologies and regularly announce technological progresses. They seem to be rather ahead in photon qubits as we have seen about their boson sampling experiments but not really with other qubit types.

In 2017, the Hefei laboratory announced the realization of a test system of 10 superconducting qubits in aluminum and sapphire<sup>1702</sup>. The two qubit gates error rate of 0.9% was not best in class.



They were at 24 superconducting qubits in 2019. Their fidelity is 99.9% on single-qubit gates and 99.5% on two-qubit CZ gates, is much better<sup>1703</sup>. Their T1 duration, which defines the coherence time of the qubits is 40 μs, equivalent to what IBM obtains with its Q System One at 20 qubits. The Jian-Wei Pan team planned to reach 50 superconducting qubits by 2023.



It delivered on this promise in May 2021 with 62 superconducting qubits, implementing quantum walks, which makes comparisons difficult, for example with IBM's 65 superconducting qubits system launched online in September 2020. They followed with the announcement of a 66 superconducting qubits system quantum advantage, being seemingly a copycat of Google's Sycamore processor architecture and benchmarking.

The Chinese scientific level is good but not yet stellar. They mostly improve technologies developed in Western countries and do not generate many new ideas. On the other hand, they create experiments like boson sampling or QKD deployments at a large scale.

China does not seem to have any influence in the academic world on quantum algorithms and programming tools. We must never forget the strategic role of software and platforms in the digital economic battles! It looks like History is repeating itself in China for this respect.

<sup>1702</sup> See [10-qubit entanglement and parallel logic operations with a superconducting circuit](#) by Chao Song et al, 2017 (16 pages).

<sup>1703</sup> Source: [Superconducting Quantum Computing](#) by Xiaobo Zhu, June 2019 (53 slides).

## **Quantum industry**

Public-private partnerships have been put in place, such as with **Alibaba**, who invested in the USTC to launch in 2015 the Shanghai [Alibaba Quantum Computing Laboratory](#). It focuses on quantum cryptography and quantum computing. Quantum cryptography could be used to secure e-commerce transactions and data centers connections. In January 2018, Alibaba even launched a cloud-based 11 qubits system developed by USTC.



We can also mention the involvement of **ZTE** and many telecom operators and manufacturers in the deployment of secure fiber networks by QKD (**China Telecom**, **China Cable**, **China Comservice**, **China Unicom**) as well as various banks that use them.

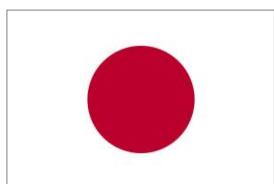
**Baidu** launched in 2018 its **Institute for Quantum Computing**, which is being deployed in their Technology Park in Beijing with around ten people as of September 2019. It is led by Runyao Duan, a specialist in quantum information theory, with Artur Ekert as board member. For the moment, they are working on software stacks, with no ambition to build their own quantum computer. They also have a quantum emulation offering in their cloud resources named Quantum Leaf<sup>1704</sup>.

**Tencent** also launched a Quantum Lab in 2018, led by Shengyu Zhang and based in Shenzhen. They plan to offer quantum computing resources in the cloud. The lab publishes work in quantum simulation and machine learning algorithms.

Chinese startups are not very numerous at this stage, one of the reasons being that public research laboratories are well funded and have less incentive to create companies. These include **QuantumCTek** and **Qasky Science**, which specialize in quantum cryptography. The latter two have joined with the Swiss company ID Quantique and the American company Battelle to form the **Quantum-Safe Security Working Group**, which federates the **quantum** cryptography industry. China is therefore putting the emphasis on quantum in all its dimensions, but especially in quantum cryptography!

## **Japan**

Let's move to the rest of Asia, starting with **Japan**. The country stands out for its very active and long-term oriented fundamental research initiation of two key technological waves in quantum computing.



It started with the creation of the principle of quantum annealing by **Hidetoshi Nishimori** in 1998<sup>1705</sup>. Then, there was the creation of the first superconducting qubits in 1999 by **Yasunobu Nakamura**, **Jaw Shen Tsai** (both then at NEC) in liaison with **Yuri Pashkin** (Lancaster University, UK). Unfortunately, this was not turned into some industry lead.

<sup>1704</sup> See [Introduction to Baidu Quantum Program](#) by Shuming Cheng, June 2019 (9 slides). They notably propose the Paddle Quantum library, released on GitHub, which supports neural network QML, quantum chemistry and optimization tools. All this in quantum emulation on classical data centers.

<sup>1705</sup> See [Quantum annealing in the transverse Ising model](#) by Tadashi Kadowaki and Hidetoshi Nishimori, 1998 (9 pages) and [Quantum Annealing by Hidetoshi Nishimori](#) where he explains the foundations of quantum annealing, used by D-Wave.

## Research

Japan's public research is conducted by several independent agencies attached to various ministries that fund public laboratories, university laboratories and research partnerships with companies<sup>1706</sup>:

- **JST** (Japan Science and Technology Agency) funded by the Ministry of Research and which funds deep techs research projects and also promotes science to the general public and international scientific collaboration. In 2016, JST launched a project by Yasunobu Nakamura of "Macroscopic Quantum Machines" to assemble 100 superconducting qubits.
- **RIKEN** (Institute of Physical and Chemical Research) also funded by the Ministry of Research (MEXT), with a total of about 3000 researchers. It includes a laboratory in theoretical quantum physics, headed by Franco Nori, and another in photonics, headed by Katsumi Midorikawa. They work in particular on silicon qubits. It collaborates with Fujitsu since 2020 to build a supercomputing qubits computer.
- **ICT** (National Institute of Information and Communication Technologies) includes the Quantum ICT Advanced Development Center, which specializes in quantum cryptography. In July 2017, the institute carried out a demonstration of quantum telecommunications using a microsatellite, reminiscent of the Chinese experiment with the Micius satellite carried out the same year.
- **NII** (National Institute of Informatics) includes a hundred or so researchers and focuses on research in theoretical quantum computing but also works on superconducting and silicon qubits.

The Japanese-French Laboratory for Informatics ([JFLI](#)) created in 2009 is based in Tokyo and hosted at both the NII and the University of Tokyo. It brings together researchers from the Universities of Tokyo, Keio, NII, CNRS, Sorbonne University (LIP6), Inria and Université Paris-Sud. This multidisciplinary team ranges from fundamental physics to algorithms and studies the feasibility of large-scale quantum computing as well as quantum cryptography. The laboratory is co-directed by **Kae Nemoto**, from the NII, one of the few women in this whole panorama. Damian Markham from CNRS LIP6 has been working there since the beginning of 2020.



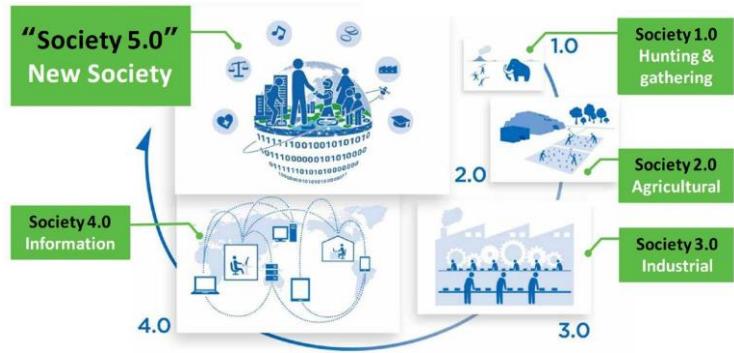
- **NEDO** (New Energy and Industrial Technology Development Organization) which is attached to the Ministry of Economy and Industry, METI. It is particularly invested in quantum annealing with a project running from 2018 to 2022 with \$4.5M per year.
- **AIST** (National Institute of Advanced Industrial Science and Technology) also funded by METI. It employs about 2300 researchers in all. Several laboratories appear to be dedicated to nanomaterial sciences. There is also a research group on precision measurement.
- **QST** (National Institutes for Quantum and Radiological Science and Technology) was launched in April 2016 with an annual budget of \$487M. This impressive amount is not exclusively allocated to quantum technologies. It mainly covers the vast field of quantum sensing and in particular medical imaging.

The Japanese government had launched various quantum initiatives such as **PRESTO** (since 2016) or the **CREST** cross-cutting program (also since 2016) as well as the **ERATO** projects in 1981 (Exploratory Research for Advanced Technology).

---

<sup>1706</sup> The most active quantum laboratories are located at the universities of Tokyo, Kyoto, Tohoku, Osaka, Nagoya, Keio, Tsukuba and Hokkaido. See [Activities on Quantum Information Technology in Japan](#) by Akihisa Tomita, June 2019 (19 slides). This is the source of the diagram in the following pages.

The country's quantum initiatives are currently part of its Fifth Science and Technology Plan, running from 2016 to 2022. In a typical Japanese way, this plan is linked to a societal goal "Society 5.0" to bring cyberspace and physical space closer together to solve society's social problems and create a human-centered society. All this with AI, quantum sensors and cybersecurity.



Here are a few leading researchers in Japan in addition to those mentioned above<sup>1707</sup>:

**Akira Furusawa** of the University of Tokyo has the ambition to create a large-scale quantum computing solution with photon-based qubits.

**Yoshihisa Yamamoto** (1950), a Stanford alumni and director of the NTT Physics and Computer Science Laboratory, who worked in photonics, QKD and quantum dots. He is very influential in Japan on the country's technological choices<sup>1708</sup>. He is the pilot of the Quantum Information Project (QIP), one of the national research program projects from FIRST selected in 2009 and which covered all branches of quantum applications ([source](#)).

**Kohei Itoh** of Keio University has been managing the Q-LEAP project since 2018, which focuses on assembling different silicon isotopes into CMOS components and on NV center based quantum magnetometry ([video](#)). He is also a partner of IBM's Q Lab in Tokyo.

**Yasuhiko Arakawa** (1952) of the University of Tokyo specializes in semiconductor physics and optoelectronics, at the origin of new processes for the exploitation of quantum dots in sensing.

**Yasunobu Nakamura** (1968) who specializes in superconducting qubits and serves at the RCAST (Research Center for Advanced Science and Technology) of the University of Tokyo and at the CEMS (Center for Emergent Matter Science) of RIKEN<sup>1709</sup>.

**François Le Gall** (1959) is a French researcher based at Kyoto University who specializes in quantum computing theory, mathematics, quantum algorithms and cryptography. He is also interested in distributed quantum computing ([video](#)). He has been living in Japan for more than 20 years.

**Masahito Hayashi** of Nagoya University was originally a mathematician who then became a specialist in theoretical quantum computing. He coordinated the ERATO project on theoretical quantum computing.

**Masahiro Kitagawa** of Osaka University specializes in atomic nucleus spin-based quantum sensing in nuclear magnetic resonance with notable applications in medical imaging.

**Mio Murao** who created and manages the Quantum Information Group at the University of Tokyo that bears his name (Murao Group). This group specializes in distributed quantum computing, quantum systems simulation algorithms, quantum telecommunication protocols and quantum algorithms. She is very fluent in English, which has enabled her to serve as a connecting point between Japan and research teams in the USA ([video](#)).



<sup>1707</sup> Source: [Q2B 2019 - International Government Panel](#), December 2019.

<sup>1708</sup> He is notably the co-author of the briefing note [Quantum information science and technology in Japan](#), February 2019 (8 pages).

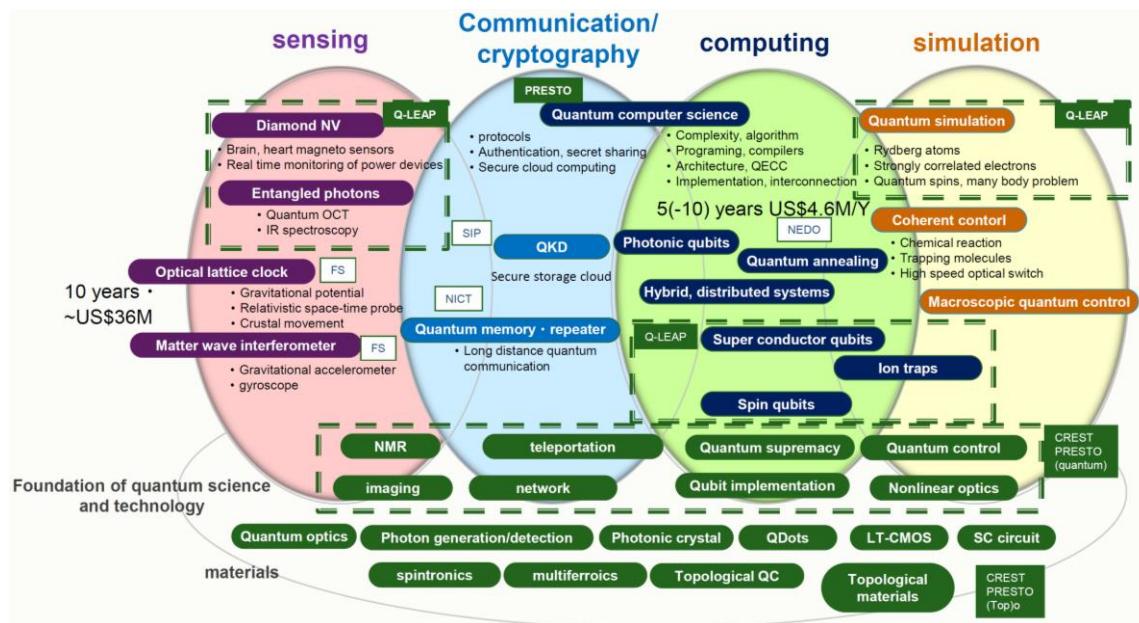
<sup>1709</sup> See his presentation of the state of the art of quantum computing [Development of quantum hardware towards fault fault-tolerant quantum computing](#) by Yasunobu Nakamura (19 slides).

**Nobuyuki Imoto** of Osaka University is leading research in quantum cryptography and telecommunications.

**Masahide Sasaki** of NICT leads much of Japan's quantum cryptography efforts. In particular, he has contributed to the SOTA project for quantum key communication using satellites<sup>1710</sup>.

### Government funding

The *flagship* project **Q-LEAP** launched late 2019 by the Ministry of Research (MEXT) seems the most ambitious and aims to catch up with both China and the USA, even if an alliance with the USA also seems to be on the agenda<sup>1711</sup>.



The roadmap extends to 2039 with \$200M spread over 10 years. The program targets quantum computing, quantum sensing and next-generation lasers. Most qubits technologies are funded: superconducting, cold atoms, trapped ions and electron spin. This "Flagship" will run until 2027.

### Quantum industry

Japanese startups are rather specialized in software and in particular for quantum annealing computing running either on D-Wave quantum annealers or on Fujitsu digital annealers. We have **A\*Quantum** (2018, QA software), **D Slit Technologies** (2018, software), **Groovenauts** (2012, QA software), **Jij** (2018, QA software framework), **MDR** (2008, chemical simulation), **QunaSys** (2018, healthcare), **Sigma-I** (2019, QA software) and **Tokyo Quantum Computing** (2017, QA software).

<sup>1710</sup> See [QKD from a microsatellite: the SOTA experience](#), October 2018 (10 pages).

<sup>1711</sup> See [Japan plots 20-year race to quantum computers, chasing US and China](#) by Noriaki Koshikawa, November 2019, [Japan plots 20-year race to quantum computers, chasing US and China](#) by Noriaki Koshikawa, November 2019, [Land of the Rising Qubit: Japan's Quantum Computing Landscape](#) by James Dargan, December 2019, and [Japan, U.S. unite to counter China in quantum computer race](#), December 2019.

**Softbank's** investment fund abounded with Saudi family's money up to \$100B is also to invest in quantum technologies ([source](#)).

However, four years after its announcement, the fund does not seem to have a single stake in quantum technologies.

#### key research orgs



#### key industry players



In the private sector, Japan's major industry groups are mainly focused on quantum telecommunications and cryptography, as well as on quantum and non-quantum annealing-based computing.

**Hitachi** also has a research laboratory located at the University of Cambridge (UK) that works on quantum key distribution, quantum computing and the creation of SQUID components for superconducting qubits.

**Toshiba Corporation** has been involved in quantum cryptography since 2003. They are working on it with the Quantum Information Group (QIG) at the University of Cambridge, UK. They performed a first demonstration of quantum communication in 2014, sending 878 Gbits/s of secure data over a 45 km fiber between two areas in the Tokyo area over a cumulative period of 34 days, at a rate of 300 kbits/s. They were continuing the experiments in 2019 and beyond and with British Telecom in the UK<sup>1712</sup>.

NTT maintains four applied quantum research laboratories, focused on quantum telecommunications and quantum cryptography, all with about 40 researchers<sup>1713</sup>.



In 2017, telecom operator **NTT** launched a prototype photonics-based Quantum Neural Network (QNN) in collaboration with the **National Institute of Informatics** and the **University of Tokyo**. It was available on the cloud at [qnncloud.com](http://qnncloud.com) ([video](#)) but the service was discontinued in March 2019<sup>1714</sup>. This was done with Toshiba, NEC and the NICT in Tokyo with three nodes and 45 km apart<sup>1715</sup>. They also work in the CMOS quantum dots qubits. NTT also developed LASOLV, a photonic based coherent Ising system with 2000 nodes<sup>1716</sup>.

Finally, several non-quantum annealing optimization computation projects on CMOS components have been launched. There is the **Fujitsu** offering, and also the NEDO project led by Masanao Yamaoka and Masato Hayashi at **Hitachi** in partnership with the AIST, RIKEN and NEDO (New Energy and Industrial Technology Development Organization, the equivalent of the energy branch of the CEA) laboratories<sup>1717</sup>.

<sup>1712</sup> See [Performance Limits for Quantum Key Distribution Networks](#) by Andrew Shields, June 2019 (16 slides).

<sup>1713</sup> This leads to raising wages inflation for the most talented people, a bit like in Silicon Valley. See [NTT offers researchers \\$1 million salaries in bid to lure top talent in cryptography, quantum computing](#), November 2019.

<sup>1714</sup> See [Japan launches its first quantum computer](#) by Walter Sim, November 2017.

<sup>1715</sup> See [Tokyo QKD Network and its application to distributed storage network](#) by Masahiro Takeoka, June 2019 (22 slides).

<sup>1716</sup> See [LASOLV Computing System: Hybrid Platform for Efficient Combinatorial Optimization](#) by Junya Arai et al, 2020 (6 pages),

<sup>1717</sup> See [CMOS Annealing Machine - developed through multi-disciplinary cooperation](#), November 2018, [Overview of CMOS Annealing Machines](#) by Masanao Yamaoka, Hitachi, (4 pages) and [A 2 x 30k-Spin Multi-Chip Scalable CMOS Annealing Processor Based on a Processing-In-Memory Approach for Solving Large-Scale Combinatorial Optimization Problems](#), November 2019.

And then the NEC project in quantum annealing led by **Yuichi Nakamura** in liaison with Waseda University, those of Yokohama and Kyoto, AIST and Titech (Tokyo Institute of Technology). They are optimizing the classical part of annealing processing with NEC vector processors. The quantum part seems to be managed on D-Wave machines. NEC is also versed in quantum keys (QKD).

IBM announced at the end of 2019 the opening of a Q Lab in Tokyo in partnership with the University of Tokyo. IBM's investment in Japan follows a model already inaugurated in France in Montpellier in 2018, in Germany in September 2019 and in Canada with the Institut Quantique in June 2020: a partnership with a university, investments in training and above all, a technical and marketing investment to evangelize quantum among major customers<sup>1718</sup>.

Finally, **Recruit Communications Ltd** (1960), a large \$16B CDN company specializing in HR, communications and marketing, distinguished itself by launching a partnership with D-Wave in 2017 to develop quantum annealing-based solutions for the operational optimization of marketing, communications and advertising. In particular, they have developed the PyQUBO open-source library, which simplifies the development of quantum annealing software applications<sup>1719</sup>.

## Singapore



The small state of **Singapore** is known for its economic and entrepreneurial dynamism. Within the **National University of Singapore** (NUS), quantum research has been consolidated since December 2007 in the **Center for Quantum Technologies** (CQT) with funding of approximately \$15M annually. It was created thanks to some real political leadership, coming from the then Defense Minister of Singapore<sup>1720</sup>.

It is vested in both quantum computing (cold atoms in Berge Englert's group, photons and superconductors in Dimitris Angelakis' group, trapped ions in Dzmitry Matsukevich's group), quantum cryptography (Kwek Leong Chuan's group) and quantum metrology (notably atomic clocks in Murray Barrett's group).

The CQT was led from its inception until July 2020 by Artur Ekert. Since then, it's run by José Ignacio Latorre. It brings together about twenty teams representing 22 permanent researchers, 60 research fellows and 60 PhD students, covering the four usual fields of quantum technologies. This represents a total of 300 people in all. Of the 22 research supervisors, about a quarter are Singaporeans who have usually done a thesis abroad. Singapore is doing well to attract talented foreigners and to ensure that they settle permanently in this country of five million people.

---

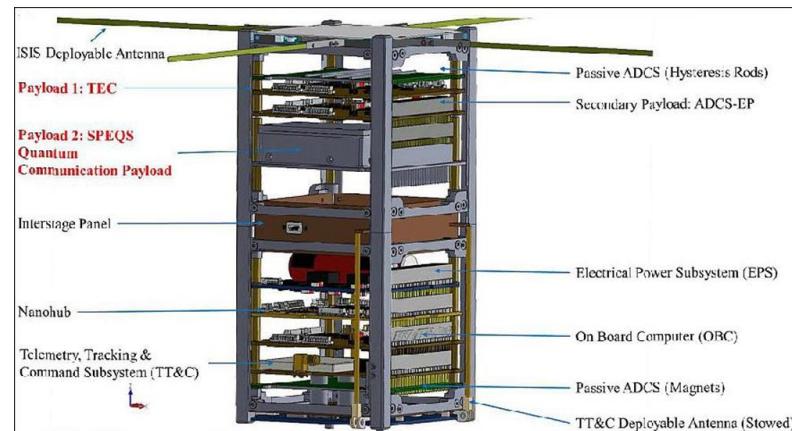
<sup>1718</sup> See [IBM Takes Its Quantum Computer to Japan to Launch Country-Wide Quantum Initiative](#) by Anthony Annunziata, December 2019. In partnership with the University of Tokyo and [IBM and the University of Tokyo Launch Quantum Computing Initiative for Japan](#) by IBM, 2019. In August 2020, IBM embellished this partnership by announcing the creation of a consortium for the adoption of quantum technologies in Japan. See IBM [Launches Global Consortium for Quantum Innovation](#) by Chris Duckett, August 2020, which refers to an announcement that is really only about Japan: [IBM and the University of Tokyo Unveil the Quantum Innovation Initiative Consortium to Accelerate Japan's Quantum Research and Development Leadership](#) by IBM, August 2020.

<sup>1719</sup> See [Recruit Communications and D-Wave Collaborate to Apply Quantum Computing to Marketing, Advertising, and Communications Optimization](#), May 2017.

<sup>1720</sup> Artur Ekert says he was persuaded to join Singapore in 2000 by Tony Tan, who was then the country's defense minister. He had met him at a conference where his visionary speech, for a politician, had impressed him. In 2005, Tony Tan took charge of the sovereign wealth fund Singapore Investment Corporation and then Singapore's National Research Foundation. He was at the origin of the strategy of targeted investment in cutting-edge research fields, which today we call deep tech. This Tony Tan then became the President of Singapore between 2011 and 2017. The CQT was launched in 2006. The story is told in the book [50 years of science in Singapore](#) pages 362 to 387, February 2017. His personal credo: to be successful, you need to attract the right people, original ideas and then funding. Too often, this happens through funding.

Six startups emerged from CQT with **Entropica Labs** (quantum algorithms), **Horizon Quantum Computing** (software), **Innovatus Q** (hybrid algorithms), **S-Fifteen Instruments** (quantum cryptography) and **SpeQtral** (satellite QKD).

Singapore is notably associated with China. In 2015, Singapore launched its Galassia-2U nano-satellite, created by CQT and used to experiment encrypted QKD based quantum communications. Galassia is integrated in a two-unit CubeSat format (two cubes on top of each other, see *opposite*). It weighs only 3.4 Kg in total. It was sent to space with 5 other satellites including the telecommunications satellite TeLEOS-1 (400 kg) at the end of 2015 by an [Indian launcher](#).



source: <https://directory.eoportal.org/web/eoportal/satellite-missions/g/galassia>

The lifetime of this type of satellite is six months<sup>1721</sup>. These experiments led to the creation of the S-Fifteen Space Systems. However, solutions have yet to be found to ensure that these satellites last longer in their low orbit and do not contribute even more to low orbit pollution.

Since 2016, CQT has also been associated with the laboratory launched by the telecom operator **Singtel** and the **National University of Singapore** for the deployment of QKD on optical fibers with repeaters.

Also in the QKD field, at the end of 2019, a team from **Nanyang Technological University** (NTU) developed a 3 mm-sided chipset capable of integrating a CV-QKD, a continuous variable quantum key-based encryption system<sup>1722</sup>. It is not without reminding what the English startup Kets Quantum Security wants to do.

In terms of international partnerships, we should also mention the association of a CQT research group leader in charge of studying noise and error correction codes, **Hui Khoon Ng**, with **Alexia Auffèves** of the CNRS Institut Néel and Atos on the evaluation of the thermodynamics of quantum computing. The CQT welcomes several researchers from France, including **Miklos Santha** (CNRS) and **Christian Miniatura** work at NTU University, this last one leading **Majulab**, the joint CNRS-NTU research laboratory on quantum science. NUS is also partnering with the **Thales TRT** research lab based in Singapore, in security and sensing ([source](#)).

## South Korea



In South Korea, the telecom operator **SK Telecom** is investing in quantum telecommunications<sup>1723</sup>. They are partners with Florida Atlantic University. They have also invested in 2016 in the Swiss startup ID Quantique. SK Telecom is also partner since 2017 with Nokia in the QKD field as well as with Deutsche Telekom with whom they have established a "Quantum Alliance" to create secure telecommunications.

<sup>1721</sup> See [Quantum Tech demos on CubeSat nanosatellites](#) (41 slides).

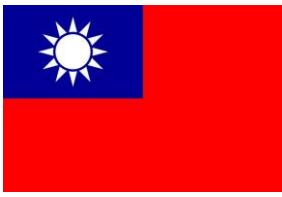
<sup>1722</sup> See [Quantum chip 1,000 times smaller than current setups](#), November 2019.

<sup>1723</sup> See [SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies](#), March 2019.

SK Telecom has deployed a QKD network in the backbone of its 4K network in the city of Sejong on two links of 38 and 50 km respectively<sup>1724</sup>.

**Samsung** is also investing in QKD and cryptography. They integrated a quantum random number generator in a dedicated version of a Galaxy smartphone for the Korean market in April 2020, with a component from ID Quantique, the Swiss startup acquired by SK Telecom in 2018. A new version was launched in April 2021.

## Taiwan



**Taiwan** is very advanced in semiconductors with TSMC, the leader in CMOS fab and the only one with Samsung that is able to go down to an integration level of 5 nm, soon 3 nm and with plans to reach 1 nm. It is also still very present in the PC components market. This is particularly the case with motherboards (MSI, Asus, Gigabyte) and PC manufacturing (Quanta, ...).

It was logical in these conditions that the country becomes interested in quantum computing.

We can identify initiatives in students training and with a conference organized in September 2019<sup>1725</sup>. **Quantum Design** provides measuring instruments but does not seem to exploit technologies of the second quantum revolution<sup>1726</sup>. Finally, IBM has established a foothold in the country to help it adopt quantum technologies.

In December 2020, Taiwan launched a \$282M quantum plan over 5 years. It will consolidate its investments in the Southern Campus of Academia Sinica, the national academy of Taiwan, in Tainan. They plan to create a research laboratory between 2022 and 2024. On top of that, Hon Hai (FoxConn) created a Quantum Computing Research Center in January 2021.

## Australia



The Australian [National Innovation and Science Agenda](#) announced in 2015 included 24 initiatives and \$820M in funding over 4 years, of which \$19M were allocated to the Center for Quantum Computation and Communication Technology (CQCCT) over 5 years in quantum computing.

The country is prolific in public-private partnership projects associating Australia with other countries<sup>1727</sup>.

In 2017, the University of New Wales (UNSW), the Commonwealth Bank of Australia and telecom operator Telstra provided \$52M in funding for the creation of a silicon quantum bit processor. One could hope that Orange will do the same in France with the CEA and/or a startup!



An investment fund of the Ministry of Defence, the **Australian Next Generation Technologies Fund** allocated \$730M to 9 areas including one on quantum technologies over 10 years<sup>1728</sup>.

<sup>1724</sup> See [Quantum Safe Communication - Preparing for the Next Era](#) by Dong-Hi Sim, June 2019 (21 slides).

<sup>1725</sup> See [Quantum Computer: Envision the New Era of Computing](#), a conference in September 2019 and [Quantum tech summer program in Taiwan a success](#), Taiwan News, July 2019.

<sup>1726</sup> See [Quantum Design Taiwan](#).

<sup>1727</sup> See [Charting the Australian quantum landscape](#), February 2019 (5 pages).

<sup>1728</sup> See [Next Generation Technologies Fund](#), 2016.

Assuming that these funds were distributed evenly among the 9 initiatives, this gives us \$8M of additional funds per year on quantum technologies for military uses, including sensing.

In February 2019, **CQC2T** (Centre of Excellence in Quantum Computation and Communication Technology) was created at UNSW, headed by Michelle Simmons. The goal was to create an electron spin quantum computer. With federal funding of \$33.7M, it brings together a community of 200 researchers<sup>1729</sup>.

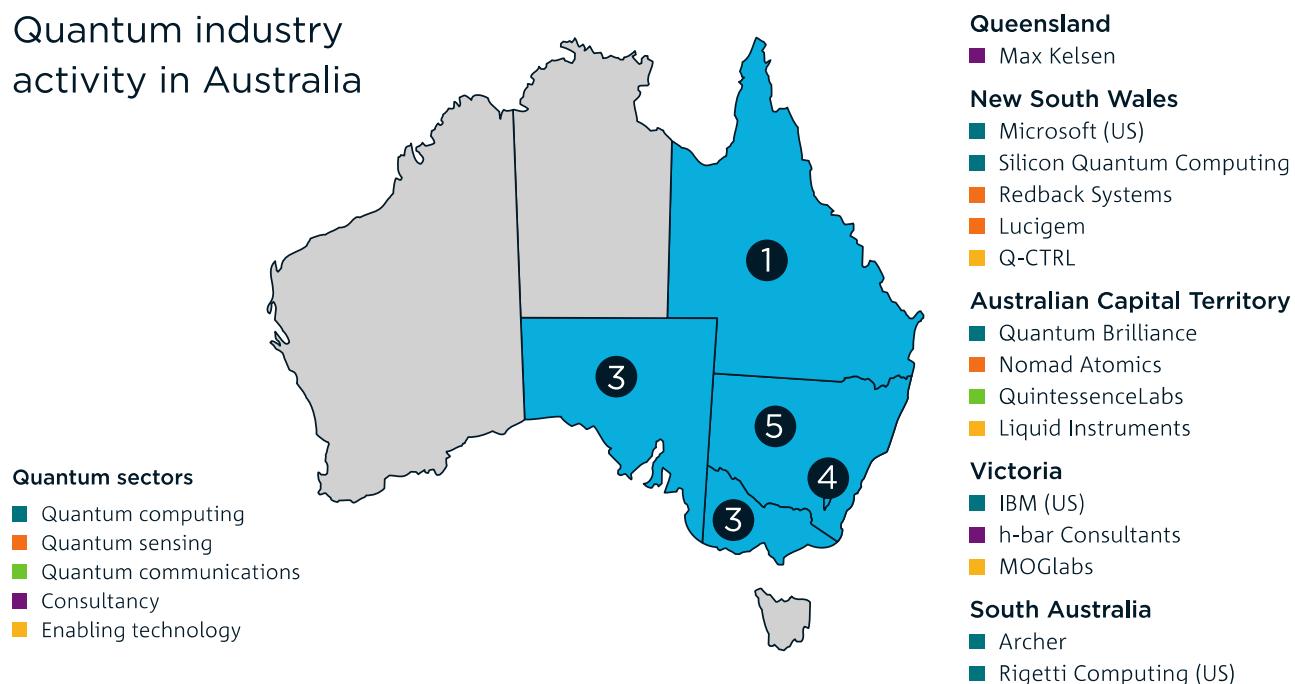
Australia also has **EQUS** (Arc Center of Excellence for Engineered Quantum Systems), a national quantum sensing research center. It partners with Microsoft, Moglabs and Lockheed Martin, among others.



On the entrepreneurial side, there are three startups in the field of quantum technologies with **QuintessenceLabs** (QKD optical keys), **QxBranch** (software and consulting, an American startup with an office in Australia, acquired by Rigetti in July 2019), **Silicon Quantum Computing** (silicon qubits), **Quantum Brilliance** (2019) on top of which should be added **Archer** and their carbon electron spins qubits.

In May 2020, Australia put its quantum strategy in order with the publication of a plan by CSIRO<sup>1730</sup>. Their ambition is to turn it into a \$4B industry creating 16,000 jobs by 2040 out of a projected global total of \$86B. The projected breakdown is \$2.5B and 10,000 jobs for computing, \$900M and 3000 jobs for sensing and \$800K and 3000 jobs for telecommunications. The goals? To define a coordinated strategy, to finance research and business creation, to train talents and to create a coherent industrial value chain.

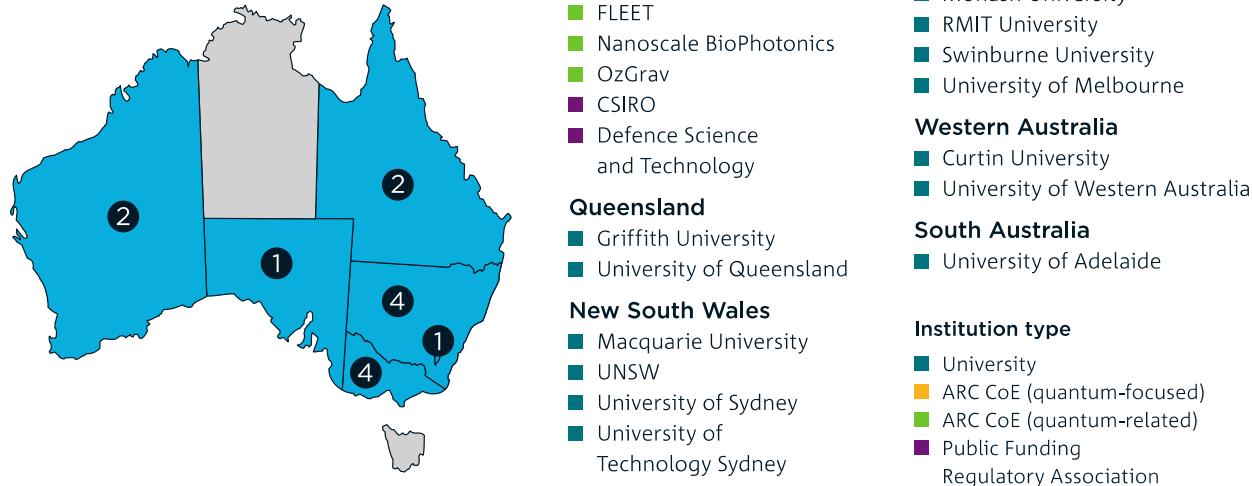
A relatively new point in such a plan, is to explore the ethical, social and environmental issues that could be raised by quantum technologies. The subject has been growing in importance since 2020. They also address the question of the supply chain of key components and materials for quantum technologies.



<sup>1729</sup> In early 2019, UNSW's CQC secured an additional \$33M in funding at its official launch. See [Federal govt funnels \\$33.7 million towards UNSW's quantum research](#) by Matt Johnston, February 2019.

<sup>1730</sup> See [Growing Australia's Quantum Technology Industry](#) by CSIRO, May 2020 (56 pages) and [Australia could lose its quantum computing lead, CSIRO warns](#) by John Davidson, May 2020.

## Quantum R&D institutions in Australia



As for companies and startups, they have some of them shown in this map. They highlight Microsoft and IBM. So be it. Rigetti because they have acquired the local startup QxBranch. And a few other startups, some of which are specialized around diamonds.

In terms of international partnerships, the country is associated with the University of Singapore for the creation of quantum telecommunication satellites.

The University of Sydney is also part of an international consortium integrated in the US IARPA LogiQ program.

In 2018, CQC2T initiated a partnership with CEA-Leti for applied silicon qubit research but without any real follow-up<sup>1731</sup>.



In December 2020, Australia launched the **Sydney Quantum Academy**, a joint effort from Macquarie University, UNSW Sydney, the University of Sydney and UTS. It consolidates training offerings implemented by the partner Universities for undergraduates, PhDs plus some fellowships programs.

## India



At the beginning of 2020, India launched an investment plan in quantum technologies, the **NMQTA** (National Mission on Quantum Technologies & Applications). This plan is well funded as a proportion of the country's GDP, with \$1.12B over 5 years, at the same level as the American Quantum Initiative Act of 2018 or the European Flagship launched the same year<sup>1732</sup>. This should be checked in practice.

<sup>1731</sup> It was even signed in May 2018 in the presence of Emmanuel Macron and Australian Prime Minister Malcolm Turnbull. The partnership also involves the UNSW-based Silicon Quantum Computing (SQC) company, created by Michelle Simmons, whose shareholders include the Australian government and the operator Telstra. It focuses on the development of CMOS quantum technologies. It also involves Andrew Dzurak, a UNSW physicist specializing in silicon qubits. This being said, this partnership seems at this stage to be a declaration of good intentions, especially concerning the industrialization part. In particular, the question of patents is not entirely clear-cut. In 2020, it seemed to be in a deadlock.

<sup>1732</sup> See [India finally commits to quantum computing, promises \\$1.12B investment](#) by Ivan Mehta, February 2020.

The plan covers the usual suspects: quantum computing, quantum telecommunications and quantum sensing. Ironically, the CEOs of IBM, Google and Microsoft are all... Indian (Arvind Krishna, Sundar Pichai and Satya Nadella)!

This plan has accelerated the creation of startups in India, some being king in overselling their technology advances. This is the case of **QPI** and their projects of a one million silicon qubits and hybrid processor.

Many of their new startups are multi-domains, such as:

- **QRLAB** (2020, India) is a contract research, education and consulting company focused on quantum computing. They develop quantum inspired software, QML and also work on quantum Internet and cryptography.
- **Qulabs.ai** (2017, India) builds quantum networks and has some expertise in QML in finance and for new drug discovery. That's quite broad in scope! Their QuAcademy facilitates students training.

## What industry strategies?

**Why:** governments are motivated to invest in quantum for strategic reasons: both in the idea of being able to decrypt existing or past telecommunications in the context of the activities of their intelligence services (DGSE Technical Directorate in France, NSA in the USA, GCHQ in the UK, etc.) and to protect their own via quantum or post-quantum cryptography. More than almost any other digital technology, quantum is therefore a tool for the states strategic sovereignty<sup>1733</sup>.

**Partnerships:** they are different in nature, between research laboratories within countries (as in the UK hubs), between particular labs across various countries, and between public and private research within the same country (CEA and Atos) or between different countries (Intel with Qutech). The raison d'être of all these partnerships can be identified: quantum computing is a complex scientific subject that cannot be mastered by a single laboratory or company. Collaboration is necessary to bring together talent from different specialties, between condensed matter physics, sensor and control technologies, optronics, cryogenics, semiconductor production, algorithmics and software development.

**Industry development:** beyond this strategic aspect are questions about the speed at which the private sector could and should take over from public basic research. This is a long-term technological issue that involves a risk almost as great as scientific risk and uncertainty. What would be the best timing for private investment and the ability to do so with very high technological uncertainty? There are some "best practices" such as ID Quantique, launched in Switzerland by researcher Nicolas Gisin.

**Funding:** despite the beautiful dynamics around deep techs that we feel in Europe and in France, this type of financing seems for the moment accessible only in North America. We need to invent entrepreneurial and financing models that allow us to conduct long-term adventures in the private sector, in the image of D-Wave's long history.

---

<sup>1733</sup> See the forum [Europe: Keys to Sovereignty](#) by Thierry Breton, August 2020. He cites three pillars of this sovereignty: computing power, data control and secure connectivity. Quantum technologies have a key role to play in the first and third! However, the means cited to obtain this sovereignty are classic and relate to public funding for R&D. We know that this is clearly insufficient.

**Startups:** as usual, many countries are asking themselves how to encourage the creation of startups by researchers or the exploitation of their work by entrepreneurs who are not researchers. Countries also have the opportunity to create a software ecosystem with development tools and business applications. A new industry is likely to emerge, even if it starts as a modest submarket of the current enterprise classical computing market.

### Quantum technologies around the world key takeaways

- The quantum startup scene has seen its peak company creation in 2018. A small number of startups like D-Wave, IonQ, Rigetti, PsiQuantum and Xanadu collected about 70% of the worldwide quantum startups funding. The investors FOMO (fear of missing out) and the “winner takes all” syndrome explain this situation.
- Most developed countries now have their “quantum plans”. The first ones were Singapore in 2007 and the UK in 2013. Investment comparisons are not obvious since these plans accounting are not the same from country to country (incremental funding vs legacy+incremental, private sector included or not, European Union investments included or not). All these plans invest a lot in fundamental research.
- China’s quantum investments have been overestimated for a while, both because of the ambiguity of China’s communication and since various lobbies in the USA were pushing for increased federal investments to counter China’s perceived threat. This worked particularly well during the Trump administration and will persist with the Biden administration.
- Europe and the USA are the greatest investors in quantum science so far. The USA has bigger investments than Europe due to its large IT vendors investments (IBM, Google, Microsoft, Honeywell). The USA also has a leading edge in startups funding, and, certainly, with its domestic market size and dynamics.
- Many countries did put quantum technologies in the critical field of “digital sovereignty” like if it was some sort of nuclear weapon equivalent.
- Each country has its own strengths and specialty although most of them invest in all the fields of quantum technologies (computing, telecoms/cryptography and sensing).
- Some analysts are wondering whether we’ll get soon into a quantum winter, like the ones that affected artificial intelligence in the 1970s and the 1990s. One way to avoid it is to limit overpromises.

# **Corporate adoption**

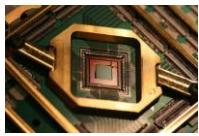
This book is intended for a wide audience interested in quantum technologies. In particular, it includes companies that may wonder what to do when facing such a deluge of hype, information, complexity and uncertainty. And this comes in addition to other technological waves to assimilate such as artificial intelligence, Blockchain, IoT and 5G, not to mention cloud deployments and the classical business applications backlog.

The wave of quantum technologies is unique in that it is even more unpredictable and difficult to grasp than the other digital technologies waves. And yet, it is worth the attention, particularly in certain key verticals such as finance, healthcare, utilities and transportations. We are clearly in a technology push situation, meaning, here it is and it's up to us to imagine what to do with it. And quantum technologies, particularly computing, are not replacing legacy systems, but complementing them.

It's still a fairly green field and not only because scalable quantum computers are not yet available. It's also linked to having only a few people understanding how quantum computers are used and benchmarked. Innovation is still well ahead of us. And quantum technologies are not just about computing. It also deals with telecommunications, cryptography and sensing. This last domain might be underevaluated and could be strategic for many industries.

I propose here a relatively simple and, all in all, fairly classic approach, which I will present here, in a dozen points, some of which come from the experience of major large companies.

## **technology screening**



- understand quantum technologies
- concepts and wording
- decipher vendor's messages and hype
- understand the news
- what can quantum algorithms do?
- case studies applicability and range



## **education and training**

- some developers, IT architects and line of businesses R&D scientists.
- study the link between quantum computing and R&D unsolved problems.
- online training
- initial training

## **resources**

- «Understanding Quantum Technologies» ebook (free, >780 pages).
- ecosystem events (Q2B, QCB, Lab Quantique, ...)
- look at vendors quantum offerings (IBM, Amazon, Microsoft, D-Wave, Pasqal, Honeywell, IonQ, ...)
- independant software vendors offerings.

## **needs analysis**



- existing unsolved problems or problems that are too lengthy or costly to solve?
- create an internal community
- involved security specialists
- security protocols mapping



## **evaluation**



- test some quantum algorithms at small scale
- on universal gates qubits as well as on quantum annealing or quantum simulators

## **Technology screening**

- Understand the **technology dimensions** of quantum computing and related telecommunications and cryptographic matters.
- Also look at the potential of **quantum sensing**. It may be enormous in various industries where precision is mandated. Quantum sensing helps measure with greater precision nearly any physical dimension: time, gravity/acceleration, magnetism, electro-magnetic waves and the likes.

- Learn how to **decode** analysts, research labs and suppliers lingua, particularly in the field of overpromises. I provide a few examples in this ebook, about the fact that quantum computing is not a miracle solution that can speed up all computer processing. Also, it is not adapted for big data applications. One important aspect here is the timing of innovations given the analysis timeframe is quite large, sometimes accounted in decades.
- Understand what can be done with **quantum algorithms** by looking at the parts of this ebook on [algorithms](#) (page 442) and [business applications](#) (page 538) sorted by vertical market. If your market is not there, it doesn't necessarily mean that you shouldn't care.
- Attend **ecosystem events** such as the QC Ware Q2B conference, Lab Quantique meet-ups, or conferences organized by researchers all around the world. Real-life events seems to be back after the long covid lockout period of 2020/2021.

## Customer needs analysis

- Identify **intractable problems** in the company's applications and business needs portfolio. This is a question that developers and data scientists can sometimes answer. For example, these are complex optimization problems involving the orchestration of many resources. You have also to look at your current existing or potential usage of high-performance classical computing. What if scenarios can also be built on the power quantum computing can bring. For example, what if we could solve this complex business problem that was never addressed?
- Create an **internal community** of engineers and business specialists interested by quantum technologies, as Goldman Sachs, Morgan Stanley, BMW, Volkswagen, Airbus, EDF and Total have done, for example. It can be fed with presentations from research labs and vendors and also sharing the understanding inside engineers have about quantum technologies, identify key questions to ask, brainstorm about business needs where quantum technologies could help.
- Launch a mapping of **security protocols** threatened by quantum computers and the infamous Shor integer factoring algorithm. What data in the present that could be intercepted now could have some value in the future for an attacker? If present data has some value more than 5 years from now, you need to start worrying and looking at QKD and PQC solutions or even revisit the way you implement applications in the cloud.
- Look at what your **peer companies** and those from your own ecosystem are doing with quantum technologies. Some may be vocal, like in the financial sector, some less. But there's now no lack of industry events where this topic is discussed.

## Training

- Train a **few developers** in quantum programming. This can be done by letting people interested in the matter spend time on it on their own. The information and tools are available online with IBM, Microsoft, Atos, D-Wave and many other places. Open-source cloud-based tools are already there. The youngest and most curious developers will probably be the ones who will best adapt to quantum computing programming paradigms, which are difficult to assimilate when being trained for classical programming. These must also have a stronger mathematical background than the average developer. Analog electronics engineers can also be interested with quantum programming giving the analog nature of the underlying processes like interferences between qubits.
- Understand the links between **quantum computing and artificial intelligence**. Quantum machine learning is a new sub-discipline of quantum algorithms that deserves to be explored and understood.

- The small hidden advertising in this book is here: I propose a **one or two days customized training** for corporate engineers who are curious to discover the whereabouts of quantum computing and other quantum technologies.

## Evaluation

- Talk to the many quantum computing **independent software vendors**, particularly with those who are specialized in your vertical.
- Test **some algorithms** in the cloud with universal quantum computers (IBM, Amazon and Microsoft cloud, Xanadu, etc) or quantum annealer (D-Wave) or with emulators (Atos, IBM, Microsoft, Amazon, Google). The available case studies are discussed in this ebook in the section on algorithms and applications by market, page 543.
- Do not hesitate to test algorithms on D-Wave **quantum annealers** despite their relatively poor image among universal quantum computer purists. Quantum algorithms for these computers are suitable for solving complex optimization problems and represent a large part of what quantum computing can bring, whether in biology or finance, to take just two examples.
- Also keep an eye on **quantum simulations** which are useful for solving two main classes of problems: materials and chemical simulations, and complexity problems. Pasqal (France) and ColdQuanta (USA) are not far from delivering very interesting hardware here.
- Avoid the **do nothing approach**. Since quantum technologies adoption takes a while, you would be left behind against your competition. This may look contradictory with the need to avoid falling into the current quantum hype. Well no. Sort the hype and find what is useful! You'll find stuff!

Congratulations, you have saved yourself a McKinsey or BCG study!

# **Quantum technologies and society**

We will leave quantum physics, hardware, mathematics and algorithms to focus on the links between quantum technologies and society. We are still at the very beginning of this technology revolution. What will follow is a mixture of observations and interpolations. Like with any digital technology wave, the quantum wave will affect society and industries at several levels, some of which can be anticipated, others less easily.

I am interested in connecting the potential impact of quantum computing with regards to mankind ambitions, the role of science fiction in the buildup of quantum imaginary, the philosophy of quantum physics, the way in which religions and spiritual movements may embed quantum whatever in their thinking, quantum technologies ethics, education and training in quantum computing, the role of gender balance in the sector and, at last, quantum vendors marketing side effects.

## **Human ambition**

Quantum computing is easily presented to the general public, or understood, as bringing a computational power defying imagination, going beyond anything that has been done so far. Quantum computing would thus be a way to circumvent the current sluggishness of Moore's law. It would make it possible to maintain some sort of eternal technology growth exponentiality. This may give the impression that, with quantum computing, mankind will have a tool providing him with infinite power and total control of information, in the line of many myths built around artificial intelligence and its ultimate mythical destiny, Artificial General Intelligence (AGI). In 2018, the futuristic American physicist and author **Michio Kaku** predicted that quantum computers will be the ultimate computers capable of surpassing human intelligence<sup>1734</sup>. Here we go again with the Singularity!

Artificial intelligence and quantum computing seem to have no boundaries. They illustrate mankind's desire for power and omniscience, to shape matter if not minds, and to have the capacity to predict the future, making it almost deterministic. So much that it would be the abandonment of free will<sup>1735</sup>. Of course, not!



### **TECHNOLOGY**

## **Could Quantum Computing Be the End of Free Will?**

On the fear that too much processing power will make us cease to be human

RACHEL GUTMAN JUN 30, 2018

Quantum physics has generated its share of questions about the nature of the world. The indeterminism of quantum state measurement has become that of life. Quantum entanglement has given rise to pseudo-scientific explanations of telekinesis and the transmission of thought. We will see in the following section how quantum medicine mixes nano and macro worlds in a fancy way.

<sup>1734</sup> See [The World's Most Disruptive Technology \(That No One Is Talking About\), Part II](#) by Ian Connett, 2018.

<sup>1735</sup> As suggested by [this article in The Atlantic](#) of June 2018, the title of which has little to do with the content!

The mechanical nature or not of consciousness is at stake. For **epiphenomenalism** ([definition](#)), our consciousness is the result of physical phenomena in our body and brain but without direct external physical effects. Behavior is the result of the brain's action on the muscles.

For **mysterianism**, the understanding of consciousness is beyond the reach of Man. As consciousness depends at a low-level on quantum phenomena which govern a-minima the relations between atoms of the molecules of our brain, some people deduce a little quickly that quantum computing would allow AI to become general as in this [debate](#)! But these are at this stage fancy elucubrations.

Ambitious projects such as the European **Human Brain Project** led by Henri Markram aim to simulate the brain's behavior in a computer and thus to understand how it functions from start to finish, even if it is not possible to do so on even a molecular scale. In another fashion, the ability of quantum computers to simulate quantum phenomena has also sustained the idea that we are objects of a great simulation. An idea that ignores the constraints of dimensionality.

An exploration of the mysteries of quantum computing and complexity theories allows us to put our feet back on the ground. Complexity theories describe various limits to the nature of problems that can be solved with quantum computing. Computational omnipotence does not exist. We will always be obliged to use various forms of reductionism to simulate the world, i.e. we will only be able to do it correctly at "macro" scales and not at "micro" or "nano" scales for matters related to computational magnitude. A bit like predicting the weather thanks to the finite element method applicable to large portions of sky and not at the level of each water molecule.

The limits of the possible will be constantly pushed back, but they will remain. Just like those of understanding the world which are confronted with the temporal and spatial limits of the Universe. We will probably not be able to know what was happening before the big bang nor to evaluate the existence of multiverse. Being unverifiable, these interpretations of the world can only remain speculations and not become real science. In the same way, our physical means will probably never make it possible to simulate our world in-extenso.

Quantum physics also introduces a lot of chaos and randomness into biology that no computer will ever be able to fully simulate and control.

Finally, this quote from Scott Aaronson sums up the quest for quantum computing. This would be justified by the desire to counter those who say it is impossible. The rest is the icing on the cake<sup>1736</sup>. This is obviously some humor, not to be taken at face value!



*"For me, the single most important application of a quantum computer is disproving the people who said it's impossible.*

*The rest is just icing on the cake"*

**Scott Aaronson**

source : A tale of quantum computers de Alexandru Gheorghiu (131 slides)

## Science fiction

Science fiction and particularly movies and TV series have been great sources of inspiration and also of delirium about the potential of quantum technologies.

---

<sup>1736</sup> The quote comes from [A tale of quantum computers](#) by Alexandru Gheorghiu (131 slides, slide 31). Also see [Quantum Darwinism, Decoherence, and the Randomness of Quantum Jumps](#) by Wojciech Zurek, 2014 (8 pages), [The Combination Problem for Panpsychism](#) by David Chalmers (37 pages) and [Why Philosophers Should Care About Computational Complexity](#) by Scott Aaronson (59 pages) ?

They have created an imaginary world made of teleportation (**Star Trek**), supraluminal speed (**Star Trek**, **Star Wars**), various entanglements and miniaturization (as in **Ant Man**<sup>1737</sup>), states superposition (**Coherence**), parallel or multiverse worlds (**Fringe**, **Spiderman**, **Counterpart**, **Dark**) or time travel (**Interstellar**).



In some cases, the quantum term is used without any scientific connection to quantum physics, as in the 2013 James Bond **Quantum of Solace**, which means approximately "an ounce of consolation".

Or it plays the role of the "MacGuffin", popularized by **Alfred Hitchcock**, the gizmo that the protagonists will look after from the beginning to the end of a movie without us really understanding what's inside or all about. This is the case of the **Ronin** movie. We find another one in the movie **Hard Kill** with Bruce Willis released in February 2020. Bad guys are trying to get the "code" that will activate a "quantum AI", but its contours are quite blurred. All we know is that it could eventually do some "good" things just like hacking an airliner to crash it. In short, it's a banal "dual" civil-military solution. The bullets will rain down until the bad guy is dead without us really knowing what it's all about.

However, a small 11-page guide tries to explain quantum physics to screenwriters<sup>1738</sup>! It contains some language basics that can be used to create scripts. The usual scriptwriters do not hesitate to twist things, like **Christopher Nolan** with his elastic vision of time arrows in *Interstellar* or *Tenet*.

More recently, in March 2020, the eight-episode TV mini-series **Devs** was the first to be built around the prowess of a quantum computer capable of reconstructing the past up to Christ's crucifixion and predicting the future anywhere on Earth. With a video! Of course, this doesn't make any sense with today's technologies, but also with those of tomorrow<sup>1739</sup>.



<sup>1737</sup> See '[Ant-Man' science adviser explains the real-life physics behind the film](#)' by Denise Chow, July 2018, which explains the links between quantum physics and the scenario of the last **Ant Man**. Well, knowing that there is none to enlarge or miniaturize a character.

<sup>1738</sup> See [The Sci-Fi Writer's Guide to Quantum Physics](#) by Radha Pyari Sandhir, 2019 (11 pages).

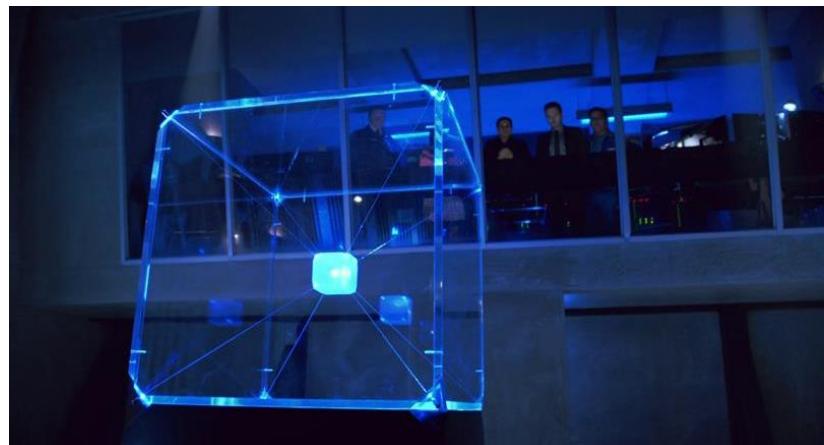
<sup>1739</sup> The stylized quantum computer features an elongated candlestick that resembles those of IBM and Google quantum computers. It is not connected to anything at all from the top, but that's okay! The whole thing is enclosed in a huge cube that is suspended and magnetically isolated. See this beautiful analysis of the series: "[Devs" by Alex Garland: a quantum thriller in Silicon Valley](#)" by Romane Mugnier in Usbek&Rica, May 2020.

It's a level of complexity problem and also about getting the training data. Even assuming that the Universe is totally deterministic, it is impossible to capture the precise position of all particles in space to determine their past and future. Moreover, this comes up against one of the key principles of quantum physics: Heisenberg's principle of indeterminacy.



Its derivative states that one cannot accurately capture the position and velocity of an elementary particle. From this point on, everything falls into place to model and simulate the world with precision!

In 2015, episode 11 of season 2 of **Scorpions** featured a quantum computer made of lasers and a large plexiglass cube capable of injecting ransomware into the US Federal Bank with just 4 qubits! This is quite a performance! The heroes hack the computer dressed as a cosmonaut by redirecting the beam of one of the lasers towards the luminous cube.



Science-fiction is fine when it stays in the science-fiction realm. The problem starts when pseudo-researchers present science-fiction as if it was actual science instead of classifying it in a rough “hard science-fiction” category that is looking for some form of scientific credibility although being most of the time heavily far-fetched. So, when some singularists tell you science and quantum physics could help resuscitate the dead using some fancy Dyson sphere and the likes, just forget it or just have some fun<sup>1740</sup>.

These science-fiction dreams are far removed from the science of today and probably tomorrow. Their benefit is to create vocations. Dreaming drives innovation. Even when a young person discovers that science does not allow them to realize the scenarios of these fictions, they can discover the infinite field of applications of quantum physics and still be creative. If real-world quantum technologies are less impressive than Star Trek magic, it still can do wonders and bring new generation of researchers and innovators.

---

<sup>1740</sup> See [A Dyson Sphere Could Bring Humans Back From the Dead, Researchers Say](#) by Stav Dimitropoulos in Popular Mechanics, March 2021. Which refers to [Classification of Approaches to Technological Resurrection](#) by Alexey Turchin (Digital Immortality Now, Foundation Science for Life Extension) and Maxim Chernyakov (Russian Transhumanist Movement), not dated (39 pages). It suggests a Dyson sphere, some quantum algorithm based on a QRNG and some weird magic with an Everettian parallel universe could help resuscitate the dead. The science-fiction, not science at all. It also suggests quantum physics could help read data from the past, a bit a la Devs.

The use of quantum physics in Hollywood movies can also be used to convey other messages. As is often the case, they can agitate the potential of an external threat against which the USA should respond with strength. It would not be surprising to see fictions emerge in which the quantum threat comes from China. These movies often illustrate the myth of the hero who can get through adversity, also illustrating an alternative to the centralized powers of governments<sup>1741</sup>.

In novels, fiction can also have pedagogical virtues. This is to some extent the case of **The Key of Solomon**, a novel by Portuguese author José Rodrigues Dos Santos published in 2015. In an affair mixing espionage and quantum computing, the hero spends his time teaching quantum physics to the other protagonists of the story. This gets the message across in a didactic way and without overly taxing science.

## Quantum foundations and the philosophy of quantum physics

Philosophy is a process of critical reflection and questioning about the world, knowledge and human existence. It creates a connection between all these dimensions. The discovery of quantum physics at the beginning of the 20th century created a real philosophical shock wave through the upheavals it brought to our understanding of the world at the microscopic level<sup>1742</sup>. It called into question key notions such as the links between reality and observations, or between ontology and epistemology. And the debates are still raging about it.

### Quantum physics and its missing ontology

Science has always been closely linked to philosophy. It is not by chance that a doctorate is a "PhD", or Doctor of Philosophy, whether in humanities or in so-called hard or exact sciences.

The great physicists and mathematicians of the 19th and early 20th centuries were also philosophers, which is less common now, due to a process of accelerating specialization.

The creators of quantum physics were constantly questioning the impact and meaning of their discoveries. **Niels Bohr** was also both a physicist and a philosopher, influenced in particular by **Søren Kierkegaard** (1813-1855, Danish). **Erwin Schrödinger** was even more of a philosopher than a physicist. He had studied Western and Indian philosophy before creating the famous wave function that bears his name<sup>1743</sup>. An assistant to Niels Bohr, **Werner Heisenberg** had also invested a lot of his time in philosophy and it related well with his work around the mathematical modeling of quantum physics and the famous indeterminacy principle.

---

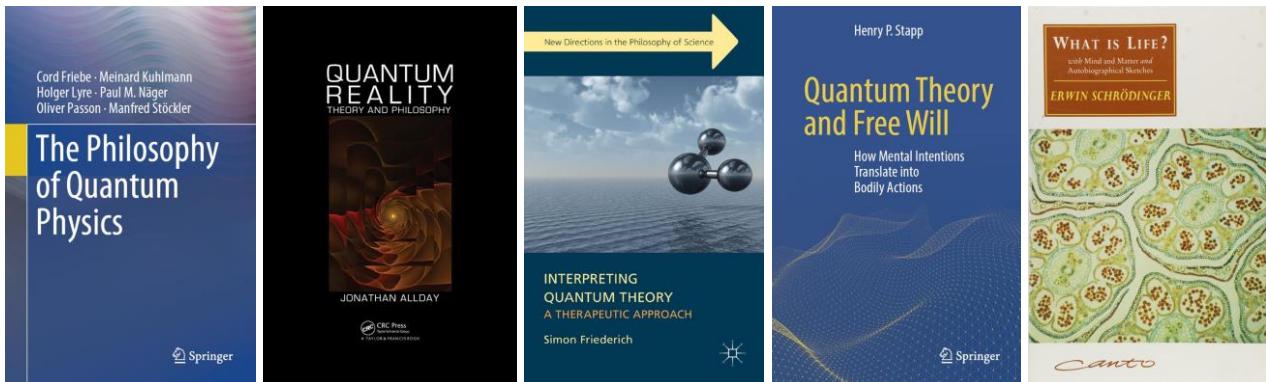
<sup>1741</sup> See [Quantum Computing, Hollywood and geopolitics](#) by Jean-Michel Valentin, March 2019. The author is a French specialist in strategic studies, sociology of defense and American strategy. The article relies heavily on the film Mortal Engines (2018), whose scenario only indirectly emphasizes quantum, with a past quantum war that ravaged the planet.

<sup>1742</sup> In practice, these upheavals occur mainly at the nanoscopic scale, that of atoms and their constituents, the nuclei and electrons. However, quantum effects can also be observed at the scale of large groups of particles that can be microscopic, as is the case with large molecules and their wave-particle duality, in Bose-Einstein condensates or superconducting currents. Knowing in all this that the frontier between quantum physics and classical physics has regularly evolved over the last century.

<sup>1743</sup> Michel Bitbol indicates that in the epilogue of "What is life? Mind and matter", Erwin Schrödinger wondered whether consciousness was singular or plural. If consciousness is only experienced in the singular, its extension to a global consciousness such as that of the Universe is only a risky extrapolation and difficult to prove experimentally. The thesis of a consciousness of the Universe is defended by some scientists. See for example [Is the universe conscious? It seems impossible until you do the math](#) by Michael Brooks, April 2020, which refers to the work of German mathematicians who try to define mathematically the notion of consciousness, allowing them to apply it then to the universe as a whole. Details are in [The mathematical structure of integrated information theory](#) by Johannes Kleiner and Sean Tull, 2020 (22 pages). It's cold and abstract!

The debates that agitated the physicists of quantum mechanics often took as much the form of philosophical jousting as of physical or mathematical debates, all the more so since the founders of quantum physics were not experimenters and were rather theoreticians<sup>1744</sup>. History has, moreover, forgot the names of the experimentalists<sup>1745</sup>.

Quantum physics has generated endless debates since its beginnings because its formalism is difficult to associate with the principles of reality usually applicable in classical physics. Intuitive classical physics understanding has historically been associated with an ontology. In Newtonian physics, the notion of state with position and motion of an object and the laws of evolution of these properties allow the prediction of phenomena such as the motion of planets. These evolutions are perfectly observable and deterministic.



Quantum physics was founded without such an ontology although it served to explain some known physical phenomenon like the blackbody radiation, the photoelectric effect or hydrogen's absorption and emission spectrum<sup>1746</sup>.

It was created as a set mathematical postulates that could help predict experimental results. You have mainly the Schrödinger wavefunction for non-relativist massive particles and others like Dirac and Klein-Gordon equations for relativist particles. In quantum physics, the prediction instrument is a probabilistic wave function that is difficult to apprehend. It is coupled with a whole host of new notions that have no equivalent in the macroscopic and classical world: energy quantification, wave-particle duality which applies to matter (electrons, atoms) and photons (all have a momentum  $p$  related to a wavevector  $k$  using Planck's constant  $\hbar$ , as  $p = \hbar k$ ), the influence of measurement on the quantities to be measured<sup>1747</sup>, measurement indeterminacy and the notion of chance.

Quantum physics is a predictive, not descriptive theory. It doesn't describe physically the electrons and other particles when they behave quantumly. It doesn't physically explain entanglement nor wave-particle duality.

<sup>1744</sup> The book [Fantaisies quantiques - dans les coulisses des grandes découvertes du xx<sup>e</sup> siècle](#) by Catherine d'Oultremont and Marina Solvay, 464 pages (2020) tells the story of the famous 1927 Solvay conference. It is a very beautiful history of quantum physics that tells touching stories of its various protagonists in the first half of the 20th century. It seems the book is not yet available in English.

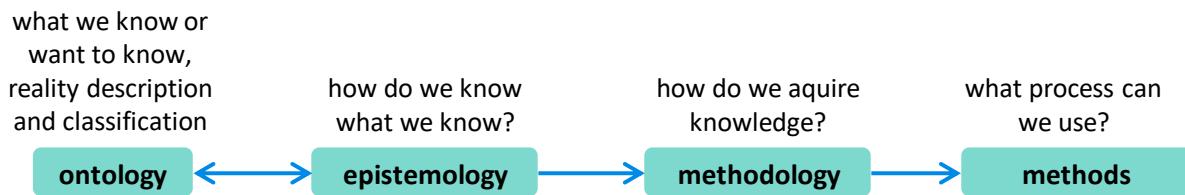
<sup>1745</sup> We mentioned many of them at the beginning of this ebook, such as Johann Balmer, Theodore Lyman, Friedrich Paschen, James Chadwick, Arthur Holly Compton, George Paget Thomson, Clinton Davisson and Lester Germer. The names of these experimental physicists generally do not ring a bell to the general public and scientists, whereas the general public has heard much more about Max Planck (with his constant more than for the black body radiation explanation), Albert Einstein (for the theory of relativity more than for the photoelectric effect explanation), Niels Bohr (for his model of the atom), Erwin Schrödinger (more for his cat analogy than for his wave equation) and Werner Heisenberg (for his indeterminacy principle, commonly called uncertainty, but not much for this huge work on quantum physics mathematical foundations). Among the founding fathers, Paul Dirac, Wolfgang Pauli and John Von Neumann were geniuses but are way behind in notoriety.

<sup>1746</sup> An ontology deals with what is, types and structures of objects, properties, events, processes and relationships in all areas of reality. It is usually opposed to epistemology, which covers how to obtain valid knowledge.

<sup>1747</sup> This is not valid only in quantum physics and the infinitely small. It works regularly at the macro scale, as in any survey with biased questions for example.

Einstein's position was that quantum physics was an incomplete theory. Werner Heisenberg even asserted in 1927 that quantum physics established the final failure of causality! The knowledge of the present no longer made it possible to predict the future from the application of the laws of physics, all the more so as the knowledge of the present with precision is also impossible<sup>1748</sup>.

Some like Niels Bohr concluded that it was useless and even counterproductive to create some quantum physics ontology. Many attempts were contradicting each other or weren't even realist per se. Some like Hugh Everett believed that reality was a universal  $|\Psi\rangle$  function, David Bohm devised some pilot waves explanations, Christopher Fuchs et al are focused on the role of agents actions and experiences in quantum Bayesianism and its derivative QBism, CSM's ontology argues that states pertain to systems and contexts, and so on. We end up having competing postulated ontologies frequently enabling the same predictions. These are hard to sort out.



The relationship between measured values, measurement and the observer is also debated. Would a true measurement be one that does not alter the quantity to be measured at all, a feat hard to attain in the infinitely small? In fact, quantum mechanics is contextual, the measurement depends on its context, which does not detract from its objectivity<sup>1749</sup>.

The mathematical formalism of quantum physics from 1900 to 1935 was not at all disconnected from the observable physical world. It made it possible to explain experimentally studied phenomena such as black body radiation, interference from Young's slits with light and matter waves, or spectral excitation lines of atoms under a wide range of conditions. We have seen how important they are in photonics, with trapped ions, cold atoms or NV centers. Electron spin explained the hyperfine energy levels of atoms observed in 1922 in the Stern-Gerlach experiment<sup>1750</sup>.

Relativistic quantum chemistry derived from Paul Dirac's equations explained spectral shifts of transitions involving low layer electrons of heavy atoms moving at relativistic velocities. The list is long.

If quantum physics explained experimental measurements, linking the observed reality and the theory, it was however insufficient to produce an unanimously accepted representation of reality. It is part of a history of science that described matter step by step, with nested Russian dolls. Atoms were initially abstract, theoretical entities before being embodied and accurately described and then directly observed as we do now with electron microscopes or cryogenic microscopy (Cryo-EM). The very existence of atoms was debated at the end of the 19th century between Ludwig Boltzmann who believed in them and Wilhelm Ostwald and Ernst Mach who opposed them.

---

<sup>1748</sup> "In the strong formulation of the causal law, 'If we know the present with exactitude, we can predict the future,' it is not the conclusion, but rather the premise that is false. We cannot know, as a matter of principle, the present in all its details. " vu dans [One Thing Is Certain: Heisenberg's Uncertainty Principle Is Not Dead](#) by Ava Furuta in Scientific American, 2012.

<sup>1749</sup> This approach is challenged by the Bayesian quantum interpretation (QBism) for Quantum Bayesianism) promoted from 2002 onwards by Carlton Caves, Christopher Fuchs, Rüdiger Schack and then David Mermin. See in particular QBism [The Future of Quantum Physics](#) by Hans Christian von Baeyer, 2016 (268 pages).

<sup>1750</sup> This one made a beam of heated silver atoms pass through a non-homogeneous magnetic field, which generated two distinct spots on a screen.

Protons and neutrons were then discovered. These were split into quarks and gluons with particle accelerators, turning the physical world into a maybe endless fractal. Obstacles to understanding it could simply be related to the enormous amount of energy that needs to be injected into particle accelerators, which is increasing the more elementary the particles are.

## Quantum Physics interpretations

Quantum physics philosophy belongs to the broad field of **quantum foundations**. It focuses essentially on the multiple possible interpretations of the same theory and their mathematical formalism. They all ask related questions such as: does reality exist independently of the observer? What is the physical meaning of the wave in the wave-particle duality? Is it a real wave of an indeterminate nature or is it a simple statistical and probabilistic mathematical model incomplete in its ability to describe physical reality<sup>1751</sup>?

Several interpretations of quantum physics have thus emerged to try to provide answers to these many questions.

**Copenhagen interpretation** is the canonical version of quantum foundations. It is essentially probabilistic. Quantum physics postulates and the wave function describe all that we can know about reality but not reality itself, which is neither accessible nor meaningful. It adopts the positivist approach according to which one sticks to observations, laws and phenomena, without seeking to know their intrinsic nature. It was the "Bohrian" side of the historical debate between **Niels Bohr** and Albert Einstein, mainly between 1927 (in the famous Solvay Conference in Brussels) and 1935 (the EPR paradox paper and subsequent discussions). Adopted by Werner Heisenberg, Max Born, Wolfgang Pauli, Paul Dirac, it is the classical and dominant interpretation of quantum physics that is still mostly taught like in the Cohen-Tannoudji/Laloe/Diu bible of quantum physics. It is satisfied with an essentially mathematical and probabilistic model that does not seek to physically describe the entire real world. There are, moreover, sub-branches in the Copenhagen interpretation, notably around the open and closed theories that had opposed Heisenberg and Dirac from 1929 onwards.

**Bohm interpretation** came from **David Bohm** (1917-1992, American then Brazilian and British). He proposed in 1952 a so-called deterministic version of quantum mechanics, called "De Broglie-Bohm theory". It was inspired by ideas initially promoted - but partly abandoned - by the French physicist and took up the idea of the existence of hidden variables, insinuated by Albert Einstein in the 1930s, and by Louis de Broglie, in the form of pilot waves<sup>1752</sup>. The existence of local hidden variables was disproved in 1982 with Alain Aspect's famous experiment. But the promoters of the therefore explicitly nonlocal Bohmian theory are still very active, including in France<sup>1753</sup>.

---

<sup>1751</sup> These different interpretations can be evaluated according to the criteria of scientificity of Karl Popper (1902-1994, Austrian/English), according to which a theory is scientific if it can be refuted by crucial experiments giving precise results. The theory cannot be shown to be irrefutable. A proven scientific theory is therefore always between two waters, in the state of a theory corroborated by facts, until proven otherwise. The history of physics has shown, however, that the "serious" theories of the past were mainly challenged by the broadening of their perspective and context: with large masses and high velocities (for relativity) and in the microscopic (for quantum physics). In their initial contexts, they remained perfectly valid. I like the very current example of the search for dark matter, which would represent 85% of that of the Universe. Its existence is not yet experimentally demonstrated but is assumed by the application of the laws of gravity and relativity applied to the cohesion of galaxies. It can be refuted or partially verified at present in at least three ways: by discovering elementary particles associated with dark matter (quantum detectors are built in this sense, and have so far given nothing), by modifying the laws of general relativity as the Israeli Morchedai Milgrom is trying to do, or by discovering hidden matter such as the dust of galaxies that could explain all or part of their cohesion without using dark matter. Belief in God and many areas of metaphysics are not part of science because they are neither demonstrable nor refutable. See on this subject the interesting debate between André Comte-Sponville and Jean Staune in [André Comte-Sponville - Jean Staune: Will science refute atheism?](#), June 2007, where some allusions are made to quantum physics.

<sup>1752</sup> The Bohmian approach is well popularized in [Quantum Physics Without Quantum Philosophy](#) by Detlef Dürr, Sheldon Goldstein and Nino Zanghi, 2013 (304 pages).

<sup>1753</sup> With Aurélien Drezet from Institut Néel, Grenoble.

**Everett interpretation** and its Universe wave function was proposed in 1957 by **Hugh Everett** (1930-1982, American) and after being almost forgotten, revived by **Bryce DeWitt** in 1970. It then became the multiple worlds or multiverse interpretation in an article published in Physics Today<sup>1754</sup>. It is said to be realistic in the sense that the Universe is a huge wave function with a (immensely) large number of parameters. It never collapses and the world is deterministic, but split in parallel branches. DeWitt's interpretation transforms quantum probabilities within this universal wave function into parallel worlds that exist simultaneously. Since it is impossible to verify that parallel worlds exist, the theory is not refutable. It's the case with all interpretations based on the same formalism.

	Copenhagen	Bohm	Everett / DeWitt
world entities	macroscopic quantum objects	wave function and particles position	wave function with quasi-classical world
determinism	indeterminism	determinist	deterministic
probabilities interpretation	objective	epistemic	objective
theories predictions goal	measurement results	particles position	agents bet
locality	non-locality	non-locality	locale
theory mathematical formalism	Schrödinger equation, projections, probabilities	Schrödinger equation and pilot waves	Schrödinger equation

We are therefore far from an experimentally supportable interpretation<sup>1755</sup>. This theory has also been promoted by David Deutsch, also known for his quantum algorithms. It feeds a many science fiction drams and mad mysticism, everything being linked to everything and vice versa, especially souls and consciences<sup>1756</sup>.

**GRW theory** published in 1986 by the Ghirardi-Rimini-Weber trio proposes a different formulation of Schrödinger's equation with a spontaneous reduction of the wave function that is not simply related to the notion of measurement. This is a rare formalism that could experimentally validated.

**QBism** is a derivative from quantum Bayesianism, starting with some ideas by **Edwin Jaynes** (1922-1998, American) and pushed by **Christopher Fuchs, David Mermin** et al. It interprets quantum physics through the eye of the observer agent actions and experiences.

**Relational Quantum Mechanics** (RQM) was crafted by **Carlo Rovelli** in 1994. This relational ontology considers that a quantum state is defined by the relation between any pairs of systems. One of them can be an observer. It is inspired by special relativity principles and its observer reference model.

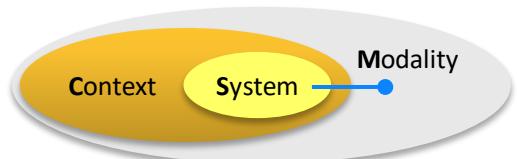
<sup>1754</sup> See [Quantum mechanics and reality](#) by Bryce S. DeWitt, 1970 (6 pages) as well as [The Many-Worlds Interpretation of Quantum Mechanics](#) by Bryce DeWitt and Neill Graham, 1973 (146 pages) which contains "The theory of the universal wave function" by Hugh Everett, 1957. DeWitt's interpretation is also called EWG for Everett-Wheeler-Graham. John Wheeler was supervisor of Hugh Everett's thesis and Neill Graham, a student of DeWitt. Seen in Everett's [pure wave mechanics and the notion of worlds](#) by Jeffrey A. Barrett, 2011 (27 pages).

<sup>1755</sup> See [Making Sense of the Many Worlds Interpretation](#) by Stephen Boughn, 2018 (36 pages) which dismantles a bit the model of parallel universes, especially in terms of dimensioning. By calculating the number of bifurcations of the Universe since its birth, and taking Planck's time as a basis, we end up with a number of parallel worlds that is beyond comprehension and all imaginable analogies. As for Schrödinger's cat, the dead cat and the living cat cohabit in two parallel worlds and the matter is settled!

<sup>1756</sup> Source of the diagram, the excellent thesis [The plurality of interpretations of a scientific theory: the case of quantum mechanics](#) by Thomas Boyer-Kassem, 2011 (289 pages).

**CSM ontology** was proposed in 2015 by **Alexia Auffèves** and **Philippe Grangier** in order to reconcile the Copenhagen interpretation with realistic models<sup>1757</sup>. CSM is a minimalist ontology designed to pacify somewhat these old debates. In this model, the properties that are measured, called **modalities**, are attributed to a **system** (studied system, as isolated as possible) within a **context** (completely specified measurement device like a photon polarizer or Stern-Gerlach experiment). Modalities are jointly associated to the system and its context, not just the system, building a contextual objectivity<sup>1758</sup>. In CSM, randomness doesn't just come from Heisenberg's indeterminacy principle but is a direct consequence of the quantization postulate and the contextual nature of reality. CSM can also help explain the origin of probabilities, non-locality and quantum-classical boundary.

Non-locality, aka the EPR paradox, has nothing to do with an action at a distance, but appears because a modality belongs to both a system and a context. It also solves the Wigner's friend thought experiment paradox based on a recursive observer of a measurement agent.



There are many more interpretations of quantum physics than qubit types around! Let's mention them without any details: **Quantum Coherentism** from Claudio Calosi and Matteo Morganti, **Foundationalism** (there must be a source of being), the **Geometrodynamic Model of Reality** from Shlomo Barak and the **Quantum Conceptual Turn** from Diederik Aerts and Massimiliano Sassoli de Bianchi<sup>1759</sup>. Other ontologies abound like **Structuralism**, **Perspectival Objectivity**<sup>1760</sup>, **Pluralism** (atomism), **Monism** and **Infinitism**, but their scope goes beyond quantum physics.

### Other interpretations

Among the physicists who have contributed to the field of quantum physics philosophy. **Pascual Jordan** (1902-1980, German) built a theory of free will according to which one is not freer by acting randomly or in a determined way, breaking the idea that quantum non-determinism would be a

<sup>1757</sup> CSM results from the creation with Nayla Farouki of the CEA of a group dedicated to the foundations of quantum mechanics in Grenoble. In 2013, they form a group with Philippe Grangier, who has long defended contextual objectivity. CSM is documented in several papers: [Contexts, Systems and Modalities: a new ontology for quantum mechanics](#), January 2015 (9 pages) lays out the key principles of CSM ontology, tying physical properties to the system, and to the context in which it is embedded. [Violation of Bell's inequalities in a quantum realistic framework](#), International Journal of Quantum Information, February 2016 (5 pages) reuses a lot of content from the first paper, commenting on observed "loophole free" violation of Bell's inequalities. [Recovering the quantum formalism from physically realist axioms](#), Nature, December 2016 (8 pages) derives Born's probabilistic rule and unitary transforms from CSM. Then [What is quantum in quantum randomness?](#), Philosophical Transactions of the Royal Society A, April 2018 (9 pages), [Extracontextuality and Extravalence in Quantum Mechanics](#), Philosophical Transactions of the Royal Society A, May 2018 (7 pages), [A generic model for quantum measurements](#), July 2019 (8 pages) and [Deriving Born's rule from an Inference to the Best Explanation](#), October 2019 (6 pages). See one critic of CSM in [Comments on New Ontology of Quantum Mechanics called CSM](#) by Marian Kupczynski, 2016 (8 pages). And the more recent [Contextual objectivity : a realistic interpretation of quantum mechanics](#) by Philippe Grangier, 2001 (5 pages).

<sup>1758</sup> Within the usual quantum formalism, a modality is a pure quantum state and a context is a complete set of commuting observables (CSCO). For a given context, CSM defines N distinguishable modalities that are mutually exclusive. If one modality is "true", or "realized", the others are "wrong" (or "false"), or "not realized". The value of N, called the dimension, is a characteristic property of a given quantum system, and is the same regardless of the context.

<sup>1759</sup> See [Diederik Aerts and Massimiliano Sassoli de Bianchi - The quantum conceptual turn](#), May 2021 (48 mn) from the [International Workshop on Quantum Mechanics and Quantum Information, Quantum Ontology and Metaphysics](#), April 2021.

<sup>1760</sup> See [Perspectival Objectivity or: How I Learned to Stop Worrying and Love Observer-Dependent Reality](#) by Peter W. Evans, University of Queensland, 2020 (16 pages).

proof of human free will. **Henri Stapp** (1928, American) worked on consciousness and believes that it governs the world and reality and that it can only be explained by quantum physics<sup>1761</sup>.

**Roger Penrose** (1931, English) considers that consciousness results from the reduction of the wave packet and **Elizabeth Rauscher** (1931-2019, American) was a physicist who first became interested in philosophy and then moved on to parapsychology<sup>1762</sup>.

On the other hand, **Steven Weinberg** (1933-2021, American), Nobel Prize in Physics in 1979 for his work on the unification of the weak and electromagnetic forces, thought that philosophy is of little use in quantum physics other than to protect us against the errors of other philosophers<sup>1763</sup>. This view was shared by **Stephen Hawking** (1942-2018, English).

In France, in addition to the CSM ontology creators, **Michel Bitbol**, a biophysicist and philosopher of science, is interested in particular in the question of consciousness, **Etienne Klein**, originally an engineer and physicist, is specialized in the philosophy of science at the CEA, as well as **Alexei Grinbaum** and **Vincent Bontemps** who are both part of Etienne Klein's LARSIM laboratory.

Quantum physics raises other physico-philosophical questions such as does a total vacuum exist? Indeed, quantum physics describes the energy of the vacuum, which would always be crossed by various real and virtual particles. From a practical point of view, it is therefore difficult to create an empty space that is not crossed at all by electromagnetic waves or particles of all kinds. If therefore nothing exists, what was there before the big bang? And let's not talk about the nature of time, which is still a matter of debate.

## Beyond Quantum Foundations

The current philosophical approach to quantum physics baffled me a bit. Most of the writings in this discipline are full of mathematics and physics. They must break records in this respect compared to any other subject covered by the field of philosophy. Above all, they do not deal much with human sciences per se.

What are the human consequences of these different interpretations of quantum physics? Are there philosophical questions other than those related to the interpretation of realism at low-level? There is much to be done in this area. The notions of uncertainty and indeterminism inevitably lead to the notion of free will and destiny (as seen by Pascual Jordan). The quantum philosophical focus on the microscopic and nanoscopic scale of physics could also be a form of reductionism preventing a wide-angle view of its societal impact.

---

<sup>1761</sup> See [Mind, Matter and Quantum Mechanics](#) by Henry P. Stapp, 2009 (303 pages). This is the kind of book that makes non-testable hypotheses that then become gospel for the quantum medicine quacks we are talking about in the dense section dedicated to quantum fumbling. And yet, the basic idea is nothing extraordinary: brain chemistry, like all chemistry, is based on many facets of quantum physics. This becomes complicated when the hypothesis is put forward of an implementation of entanglement in consciousness. Quantum medicine goes out of the scientific game when it claims that these mechanisms can be controlled from the simple will, without counting the action on the other organs (preferably sick ones) of the human body.

<sup>1762</sup> Elizabeth Rauscher is co-author with Richard Amoroso of [The Holographic Anthropic Universe](#), 2009 (510 pages). They discuss a model for creating a scalable quantum computer called "Universal Quantum Computing" that is difficult to grasp between real science and crackpot science and is based on a theory called "Unified Field Mechanics" that is difficult to evaluate. The subject is detailed in [Brief Primer on the Fundaments of Quantum Computing](#) by Richard L Amoroso, 2017 (140 pages). Richard Amoroso is Director of the Noetic Advanced Studies Institute in Oakland, California. Noetics is interested in the links between quantum states and consciousness. And this goes well beyond the realm of science with Pragmatic Proof of God ([Part I](#) & [Part II](#), 2017 by Richard L. Amoroso (34 and 13 pages).

<sup>1763</sup> See the chapter "Against Philosophy" in "Dreams of a Final Theory", 1994, Steven Weinberg, which is contradicted in [Physics Needs Philosophy / Philosophy Needs Physics](#) by Carlo Rovelli, 2018. Carlo asserts that saying that science does not need philosophy is to be doing some sort of philosophy of science! See also [The Trouble with Quantum Mechanics](#), 2016.

Also, is the extension of the scientific field infinite? What are the limits of human knowledge that seeks to explain and interpret everything about the way the Universe works? What do we miss and why? What links can be made with our humility? What are the structural limits to our insatiable curiosity? I am only reformulating the very notion of Kantian metaphysics, the "*science of the limits of human reason*".

The philosophical question thus concerns the notion of the feasible and the unfeasible and its evolution over time, a perspective provided by the history and philosophy of science. What are the limits of human ingenuity? What is superhuman? Will we be able to create ultra-reliable and *scalable* quantum computers? The theories and classes of complexity, discussed in this book, should also serve as tools for this kind of thinking.

How to extend the interpretation of quantum physics to the metaphor of quantum computation: highly rich and complex inside but simple after measurement is done? Could it be used to simulate the living and create it in silico? This will then raise questions about man's power over nature and the associated responsibilities. We will also see the resurgence of debates on scientism, the "*science-led society*", as well as on technology solutionism, a concept promoted by **Evgeny Morozov**, which could provide answers to all problems, especially environmental and health problems, which cannot be treated properly with the required urgency.

These questions arise more and more at a time when precaution prevails over everything, when there are fears of technological blunders in almost every field (nuclear, GMOs, fertilizers, vaccines, artificial intelligence and 5G), when the very notion of scientific progress is no longer accepted and when cognitive relativism no longer allows us to distinguish between the serious and the far-fetched, leading to a collective mistrust in science. In the following section, we will precisely study a question that belongs to the field of philosophy, the question of the ethics of quantum computing.

Are these questions really specific to physics and quantum computing? Aren't they recurrent as soon as a major new technology shows up? Perhaps, but these questions deserve to be asked, like those raised by the commoditization of artificial intelligence since 2012.

The interpretations of quantum physics are in any case there to remind us that in all matters, we must multiply the angles of view of problems to better analyze them. This is obviously full of lessons from a metaphorical point of view.

I wonder about all these questions by observing that, if they are not dealt with, they tend to become the field of esotericism and charlatanism as we will see in a following section dedicated to quantum fake sciences. It is a bit as if the philosophy of quantum physics had remained at the stage of fundamental research without moving on to the stage of applied research. In a way, it is in line with the level of market maturity of the technologies of the second quantum revolution. Let's bet that as quantum technologies will mature, the more this applied philosophy will develop and allow us to write a new chapter in this exciting history of science.

## Ethical quantum

Artificial intelligence ethical concerns became a real political issue in 2018. This was very apparent in France in the **Villani Mission Report on Artificial Intelligence** published in March 2018 as well as in a **Report of the House of Lords** published the same month and on the same subject in the UK<sup>1764</sup>. It highlighted the need to ensure, at least morally, but if possible, practically, that AI-based solutions respect society and avoid generating or perpetuating training data-originated discriminations. Hence two salient topics such as the explicability of algorithms and the limits of the manipulation of our emotions, particularly via more or less humanoid robots and voice agents.

---

<sup>1764</sup> See [AI in the UK: ready, willing and able?](#), March 2018 (183 pages).

The difficulty to explain how deep learning algorithms work has been exaggerated. If it is true that multilayer neural networks are somewhat abstract. But it is equally abstract for almost any software, with or without AI, that can affect our daily lives. But we've forgotten that a little. When a software from the Visa group rejects your credit card payment abroad, we almost never get an explanation of the whys and hows it was rejected and how to avoid it. Bayesian fraud and machine learning based detection techniques are not explained to consumers.

Quantum computation is likely to amplify this quest for explicability. It is even less obvious to satisfy with quantum algorithms, which follow a logic that few developers can grasp. Quantum algorithms are likely to be even more complicated and less understandable than those of today's AI. This is amplified since we cannot observe their inner working and intermediate quantum states. Only the "classical" result is measured at the end of the operations. Moreover, from about fifty qubits, it becomes impossible to emulate a quantum algorithm on a classical computer.

Their possible biases will not necessarily come from the data that feeds them because, for a certain period of time, quantum computers will probably not exploit large volumes of data. We can therefore speak literally of the term algorithm bias, whereas when we talk about AI, we are dealing more with training data bias rather than algorithms bias.

But this will be judged on a case-by-case basis. Depending on whether the applications of quantum computing optimize automobile traffic, manage energy distribution, create new molecules in chemistry or biology or help the NSA break the codes of private communications, the stakes will not be the same.

An ethical question will undoubtedly emerge before others. It will be associated with a whole range of applications of quantum computing: the simulation of the dynamics of organic molecules. It will probably be limited at the beginning to the simulation of relatively simple molecules. The simulation of complex proteins folding is a hypothesis that has not yet been validated. In a distant hypothetical future, we may be able to simulate larger biological ensembles.

When this is simulated and then altered, for example to create new therapies, the rejection of GMOs or vaccines will seem like distant memory. New fears will show up and scientists will have to get involved to prevent them from spreading. These irrational fears will emerge because of exaggerations about the capabilities of quantum computers. We already hear about "quantum robots", which means nothing, but can impress and drive wild thoughts.

**MOTHERBOARD**

ROBOTS | By Jason Koebler | Oct 8 2014, 9:25pm

## Quantum Robots Will Do Your Job Better Than You Can

Quantum computing will be powerful enough to create artificial intelligence that can learn and react in real time.

**International Business Times**

Technology

## Quantum Robotics will Create Artificial Intelligence 'Capable of Creativity'



By Anthony Cuthbertson  
October 9, 2014 11:46 BST



The example *above* is eloquent from this point of view with two titles in 2014 when quantum computing was nearly just about D-Wave and which, in practice, are only relaying a rather banal scientific publication, [Quantum speedup for active learning agents](#) (15 pages) describing quantum algorithms for the execution of agent networks used in robotics bringing a so-called "quadratic" performance gain, therefore... not exponential, therefore, not extraordinary<sup>1765</sup>. Each time, we will have to decode and take a step back.

A good approach for the quantum scientific community would be to pre-empt these fears by analyzing them as early as possible and defusing them if possible, so as not to be in a situation that would block scientific progress and innovation useful to society because of these irrational fears.

Various initiatives started to pop-up in 2021 around quantum ethics in Australia, the UK, the Netherlands, Canada and the USA. It's following a similar pattern than with artificial intelligence but earlier given the maturity of the sector. So far, contrarily to what's happening in the AI field, it has not yet been hijacked by large industry vendors or even regulators. Most initiatives were born out of the research community.

Still, there are already some similarities and overlaps between the AI and quantum ethics frameworks that are showing up.

On the AI side, many AI charters have been published since 2018. One of these comes from the **GPAI** (Global Partnership on AI<sup>1766</sup>) launched by 15 countries in June 2020 including France and Canada. Its goal is to foster the development of responsible and inclusive IAs based on human rights, favoring diversity, while driving innovation and economic growth. The GPAI did set up experts run working groups on responsible AI, data governance, the future of work and at last, on innovation. OECD launched its **AI Policy Observatory** ([OECD.AI](#)) in February 2020, an online platform consolidating information to help states craft their public AI policies. OECD defined its own AI principles ([OECD AI Principles](#)) that were adopted by 42 countries in May 2019. Also in 2020, the **AI Rome Call for AI ethics** gathered the Vatican, Microsoft, IBM and others to whitewash about the same goals as GPAI.

And these are just a couple initiatives among many others, frequently driven by industry vendors who are lobbying for self-regulation instead of tight government-based regulations.

In the quantum space, **Australia** was the first country that launched a quantum ethics initiative. Early on, in 2019, **CSIRO**, the Australian scientific research agency, mentioned the need to explore and address any unknown ethical, social or environmental risks that may arise with the next generation of quantum technologies<sup>1767</sup>. It was followed in 2021 by a white paper published by Elija Perrier from the Centre for Quantum Software and Information at the Sydney University of Technology<sup>1768</sup>.

It was spun out of the Association for the Advancement of Artificial Intelligence ([www.aaai.org](#))

<sup>1765</sup> See [Article 1](#) and [Article 2](#).

<sup>1766</sup> With Canada, Germany, Australia, South Korea, USA, Italy, India, Japan, Mexico, New-Zealand, UK, Singapore, Slovenia and the European Union.

<sup>1767</sup> See [Growing Australia's Quantum Technology Industry](#), CSIRO, 2019 and [The 'second quantum revolution' is almost here. We need to make sure it benefits the many, not the few](#) by Tara Robertson, June 2021.

<sup>1768</sup> See [Ethical Quantum Computing: A Roadmap](#) by Elija Perrier, Centre for Quantum Software and Information, Sydney University of Technology, February 2021 (10 pages).

#### Ethical Quantum Computing: A Roadmap

Elija Perrier<sup>1,2</sup>

<sup>1</sup>Centre for Quantum Software and Information  
University of Technology, Sydney  
Sydney NSW 2000

<sup>2</sup>Humanising Machine Intelligence Program  
The Australian National University, Canberra  
elija.t.perrier@student.uac.edu.au

##### Abstract

Quantum computing is among the most significant technologies to emerge in recent decades, offering the promise of paradigm-shifting computational power and significant ethical consequences. On a technical level, the unique features of quantum computation have technical consequences for the imposition of fairness and ethical criteria on computation. Despite its significance, little if no structured research has been undertaken into the ethical implications of quantum technology. In this paper, we fill this gap in the literature by presenting the first roadmap for ethical quantum computing setting out prospective research programmes. In doing so, we inaugurate the cross-disciplinary field of the ethics of quantum computing.

how computing is undertaken in quantum systems and (b) the consequences of quantum computing which distinguish research programmes into quantum ethics.

At the technical level, the distinct (by contrast with classical computing) characteristics of quantum computation, including its inherently probabilistic nature, the availability of superposition states and resources such as entanglement have distinct implications for the technical implementation of computational ethical regimes reliant on classical features of computation, including proposals regarding the implementation algorithmic governance, fair machine learning, cryptography and representational justice. These technical characteristics of quantum technologies are the basis upon which such technologies offer the promise of

The paper starts with defining the quantum physics postulates<sup>1769</sup>, then cover ethical quantum computation and asks many ethical related questions that could be asked for any kind of classical computing. They mention the complicated question of quantum algorithms auditing. Quantum algorithms indeed may become black box similarly to deep learning, leading to some explainability issues. So, on top of the various XAI (explainable AI) initiatives like the one launched by DARPA in the USA, will we see emerging the field of XQC for Explainable Quantum Computing?

It also mentions the need for some Quantum Fair Machine Learning (QFML). It may not be such of a problem since QML may not be used to process huge volumes of personal data due to quantum computing limitations in data loading techniques, which may last for a long time. They even go as far as asking whether quantum interferences implemented in quantum algorithms are ethical in nature. They also cover privacy and cryptography matters. Is Shor going to kill our private life? How could some differential privacy be implemented with quantum computing? Other topics involve distributional ethics and fair distribution which are classical economical questions arising with any new technology. At last, they wonder about the impact of quantum simulations and whether it could be implemented to simulate people's personal behavior.

The paper seems highly influenced by the works on ethical AI and sometimes mixes science-fiction with real state of the art understanding of what can and will be done with quantum computing. But it asks good questions.

In the **UK**, ethical quantum computing became a topic promoted by the media TheQuantumDaily starting in December 2020. They released a short video documentary trying to explain what quantum computing is and the related ethical issues involved with researchers like John Martinis and entrepreneurs like Ilana Wisby<sup>1770</sup>. They are highlighting the need for democratizing quantum technology skills, mention the risks on privacy and security and the need to address quantum AI bias. They also pinpoint the “Hype-Fear-Disappointment Cycle” and recommend to set realistic expectations to avoid triggering fears and biases.

Other ethical issues to be addressed cover the potential harmful manipulation of the human genome fears, the (positive) quantum use cases to find environmental solutions and the energetic footprint of quantum computing.

In **The Netherlands**, the government 615M€ initiative launched in April 2021 includes a 20M€ plan on quantum ethics and societal impact research run out of the Living Lab Quantum and Society spun out of Quantum Delta NL, the foundation established to run the Netherlands quantum program. They also create ethical, legal and societal standards for quantum technologies and their applications.

The **World Economic Forum** launched its [Quantum Computing Governance](#) initiative in February 2021. It wants to standardize an ethical framework enabling the responsible design and adoption of quantum computing. They ask the ever-lasting question: will the public trust technologies which they cannot understand and whose results they cannot verify as if they could do it with existing digital technologies. They advocate the use of preemptive involvement in technology design to make sure ethical issues are addressed as early as possible. With that, they are assembling a “*global multistakeholder community of experts from across public sector, private sector, academia and civil society to formulate principles and create a broader ethical framework for responsible and purpose-driven design and adoption of quantum computing technologies to drive positive outcomes for society*”.

---

<sup>1769</sup> They define only the first 4 quantum physics postulates and not the whole 6, and their fourth postulate doesn't correspond to the canonical Born rule related principle.

<sup>1770</sup> See [Quantum Ethics documentary](#), December 2020 (13 mn) published by TheQuantumDaily as part of a series of “conversations”. It was followed by several posts like [Quantum Ethics Series: Understanding the Issues and Expanding the Conversation](#) by Matt Swayne, 2021.

They will frame the conversation, drive quantum ethical issues awareness, study quantum related risks, design quantum computing ethics principles and framework and test it with some case studies.

In **Canada**, **Q4Climate** is an initiative for using quantum technologies in climate research, an initiative coming from the Institut Quantique, the University of Waterloo and Zapata. It looks like a small think tank. It explains how some quantum chemistry algorithms could potentially solve some environmental problems.

In the **USA**, some spare initiatives are launched by academics like Chris Hoofnagle from Berkeley, or a while ago, by Scott Aaronson<sup>1771</sup>.

Interestingly, none of these initiatives mention the field of quantum sensing, which could also have some underlying ethical issues to be addressed, particularly when used in the military. Quantum radars, quantum imaging, precision gravity measurement and its impact on underground resources exploitations are a couple examples.

## Religions and mysticism

In recent millennia, the human race has developed the habit of devoting a cult to one or more higher divine powers of an imprecise nature, but explaining everything and everything else.

Mankind probably began to attribute this power to natural phenomena that he could not explain like the Sun or the stars. Mankind then went from multiple systems of gods to a single all-powerful God. In a way, the monotheistic religions realized before time the theory of unification so much sought after by physicists. This story is told with hindsight by **Yuval Harari** in Sapiens and with cynicism by **Richard Dawkins** in “The God Delusion”.

For some scientists or believers in an afterlife, quantum physics renews the desire to explain the inner works of the Universe by some divine power. It gives the impression of providing an ultimate scientific explanation for everything, of God, and of his ability to control and supervise everything<sup>1772</sup>. The quantum function most often emphasized in these explanations is entanglement.

It makes it possible to envision a Supreme Being who, thanks to this physical phenomenon, can control all the particles of the Universe and at a distance. It would also explain strange synchronicity phenomena. The wave-particle duality also makes it possible to imagine or explain many magical scenarios such as remote healing, telekinesis or telepathy<sup>1773</sup>.

Some of the protagonists of these theories are themselves quantum physics scientists. One of the best-known is **David Bohm** (1917-1992), already mentioned in the quantum foundations section, page 744, who came closer to Indian spiritualism in the 1960s, simultaneously with the Beatles! He was convinced that the laws of the Universe were governed by some spirit<sup>1774</sup>. He is one of the initiators of the theories of **quantum cognition**, a field of cognitive theories based on the mathematical formalism of quantum mechanics, and relying on analogies.

---

<sup>1771</sup> See [Law & policy for the quantum age : a presentation](#) by Chris Hoofnagle, February 2021 (58 mn). Berkeley Professor. See [Why Philosophers Should Care About Computational Complexity](#) by Scott Aaronson, 2011 (53 pages).

<sup>1772</sup> On this subject, see the Wikipedia fact sheet that briefly describes [quantum mysticism](#).

<sup>1773</sup> A good inventory of these different debates can be found in [The Quantum God An Investigation of the Image of God from Quantum Science](#), 2015 (81 pages) which evokes the notion of consciousness of the Universe. See also the almost parodic [Nothing is solid "All is energy"](#).

<sup>1774</sup> See [Lifework of David Bohm - River of Truth](#) by Will Keepin, 2016 (22 pages).

The literature on quantum derived spiritualism is sometimes mind blowing, such as [Google's Quantum Computer May Point People to God](#), from 2013. According to the (anonymous) author, a perfect quantum computer could attempt to simulate the appearance of life on Earth and demonstrate through absurdity that it would not be possible without divine intervention. But who says that the result would not be the opposite? Quantum computing could invalidate classical theories of evolution.

They do not specify the number of zillions of entangled qubits that would be required to support this. Of course, because they have no idea which algorithms to use. And who care about quantum error corrections !

All of this is religion-science fiction and can generate heated debates with people who will never be on the same wavelength, some adopting a classical scientific approach and others a mystical and more emotional one.

## Public education

Quantum computing will amplify a situation observed with artificial intelligence: a huge gap between those who understand it and those who use it, coupled with a shortage of skills.

Quantum computing is right now definitely a world of specialists, and it is even harder to grasp than most other digital-related disciplines. Today, this world is balanced between specialists in condensed matter physics and quantum algorithms and software<sup>1775</sup>.

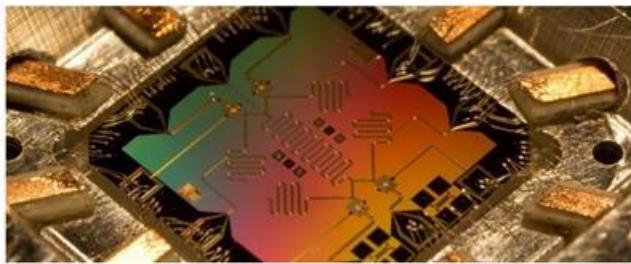
By extrapolating a little and drawing inspiration from the history of computer science, we can anticipate that software will gradually take over when quantum computing becomes commonplace, especially if it leads to applications in all sectors of industry.

In today's digital economy, there are many more software specialists than there are with semiconductors. The economies of scale are actually much greater with the latter between producers and users. Quantum will probably not escape this, even if initially the market for quantum computers will not be a volume market.

In the short term, there is a great need to popularize the field and also avoid its technical jargon. You have to proceed step by step, broadening the audience step by step in a progressive way from the techie to the non techie<sup>1776</sup>. The next step is training and extension to decision-makers in companies and institutions. It is becoming even more important as the quantum technologies hype is peaking with the flurry of vendors and research labs announcements that are regularly showing up.

## Google's Quantum Computer May Point People to God

In Featured, In the News, Videos by JD Rucker / October 11, 2013 / 9 Comments



<sup>1775</sup> See [Eleven risks of marrying a quantum information scientist](#) by Nicole Yunger Halpern, 2020. A second degree but realistic inventory of the life of a quantum scientist in the USA.

<sup>1776</sup> See for example [The Quantum Prisoner, a free scientific and technological video game is now available online](#), CEA, October 2020.

In that category, let's mention **QuantumShorts**, a [film festival](#) organized by the CQT from Singapore, a video creativity contest around the topic of quantum science and technologies. That's fun. They benefit from partnering with Scientific American and Nature and various research centers beyond CQT in the USA, Australia, Canada, UK and Netherlands.

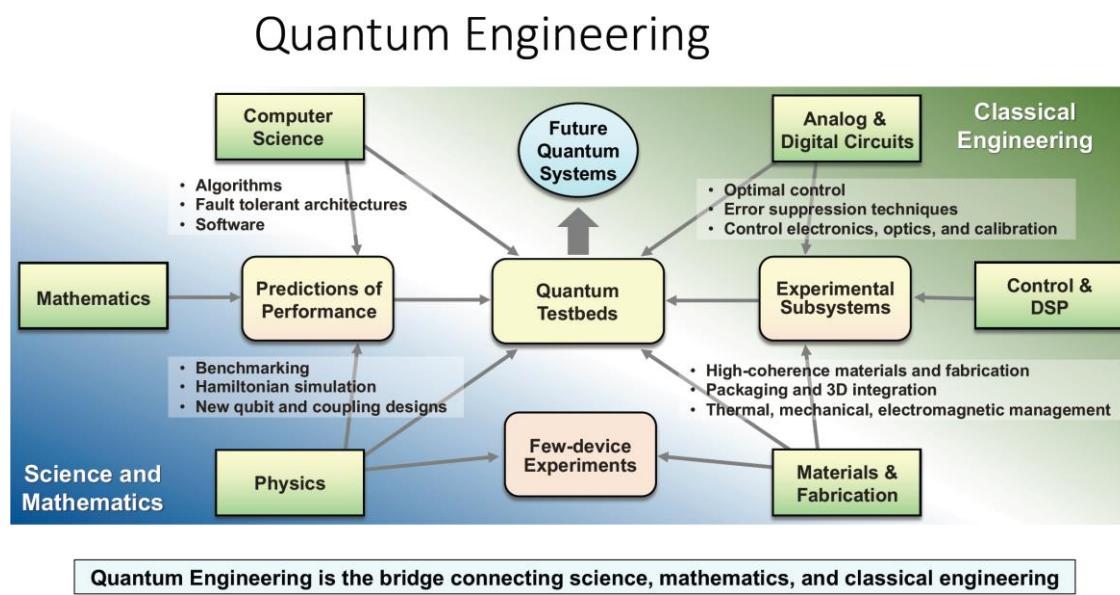
## Scientific education

All these countries launching well-funded quantum plans create a significant challenge with scientific education along the whole cycle from bachelor to doctorate. Before being an industry competition, quantum technologies are a talent one. We can expect that there will be more money to spend than talent to hire with it.

On top of the many existing available quantum physics programs, there are a couple new disciplines where more and more people will need to build knowledge and skills on:

Quantum systems engineering create real machines that work from start to finish. This requires de-compartmentalizing disciplines and bringing together physicists and engineers.

The technologies involved are varied and include photonics and lasers, analog and digital electronics, thermodynamics, fluid mechanics, various components manufacturing techniques, and the design of complete systems. Quantum engineering involves many complementary disciplines<sup>1777</sup>. With AI, it is a new challenge for higher education that is being prepared.



In the purely mathematical and software fields, very important disciplines come into play for creating end-to-end quantum solutions: algorithms design, software tools design and applications software development. Added to this is the field of post-quantum cryptography.

The creation of business applications also requires skills at the crossroads between the above and vertical markets, which are often themselves scientific as in life sciences (organic chemistry, protein folding, photosynthesis, ...), materials sciences (battery chemistry, superconducting materials) or other branches such as portfolio management and risk assessment in finance or optimization problems in logistics, transport and marketing.

---

<sup>1777</sup> The schematic comes from the [Introduction to Quantum Computing](#) presentation by William Oliver from MIT at Q2B in December 2019.

Quantum technologies will be found with many different professions:

- **Fundamental physicists** (solid-state physics, condensed matter physics, light-matter interaction, quantum optics) who combine theoretical and experimental approaches to understand low-level phenomena.
- **Quantum technologies researchers** who turn fundamental discoveries into first proofs of concept in the laboratory. These research teams combine physics, technology and engineering researchers.
- **Design engineers** who create technical subsets of quantum computers to complete finished products. They essentially do the "D" of "R&D" by relying on the R of physicists.
- **Research engineers**, who participate in the development of new materials and new technologies in semiconductor fabs, or process engineers who design the manufacturing processes for these integrated circuit systems supporting qubits.
- **Technicians** for certain components manufacturing and/or for the deployment of technologies such as quantum cryptography in the telecom space. But only once this technology is deployed on an industrial scale, probably by generalist or specialized telecom operators.
- **Software tools developers** who must be associated with previous researchers and engineers. Indeed, for the time being, the design of these tools still has to take into account the physical characteristics of quantum calculators/accelerators.
- **Application developers**, whose numbers will increase as the computing power of quantum computers grows.
- **Project managers** who manage projects and teams that combine these different professions.
- **Business strategists**. Brian Lenahan goes as far as defining the job of “quantum business strategist” which looks like an equivalent of the chief digital officer for quantum technologies related projects, creating the link between IT and business managers. This role is about crafting a quantum plan with mission, vision, goals, strategies, KPI’s and tactics. In other words, it’s an old-fashioned consultant<sup>1778</sup>!

As in many disciplines, researchers and engineers are increasingly required to be versatile. Teams must be structured around a strong interdisciplinarity and transversality. They need "technological polyglot" teams that link all these professions and skills. In particular, physicists will have to be increasingly interested in engineering and engineers in physics.

Finally, when you turn to the business side with actual products that can be marketed and sold, you need the whole mix of skills usually found in technology marketing and sales: product marketing, operational marketing, business development and partnerships, creating ecosystems and, above all, pure and simple B2B sales for a starter.

This is completed by the generic skills associated with deep techs startups creation (organization, business planning, recruitment, funding, etc.) and with intellectual property attorneys who must grasp the specificities of the quantum vocabulary.

Quantum sensing products are beginning to be marketed, and in a market that is currently niche.

---

<sup>1778</sup> See [What is a Quantum Business Strategist?](#) by Brian Lenahan, April 2021 and his related book [Quantum Boost: Using Quantum Computing to Supercharge Your Business](#) by Brian Lenahan, May 2021. Brian Lenahan also created in September 2021 the Quantum Strategy Institute with various people from Spain, UK, France and the USA with the goal to bridge the gap between quantum science and businesses.

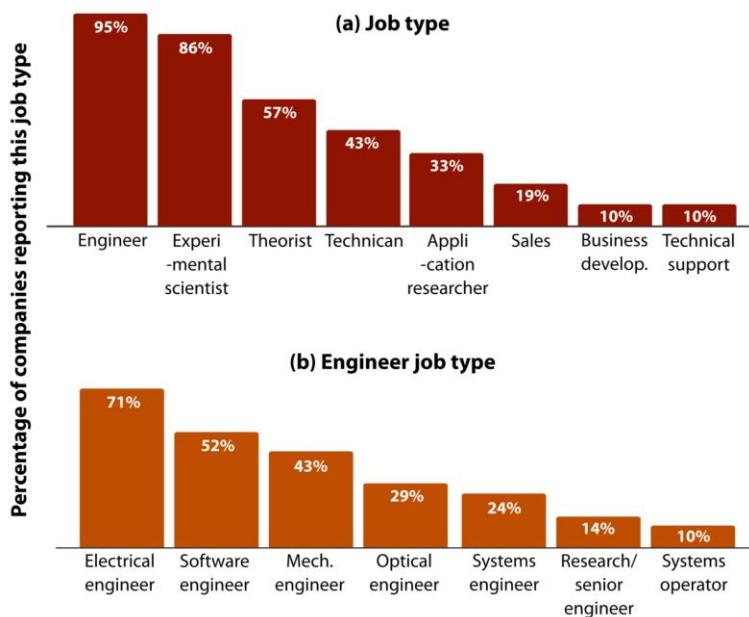
Quantum cryptography systems are in the experimental field phase and could be deployed on a larger scale in the coming decade.

Quantum communications with the objective of leading to quantum communications networks will develop in a second phase, combining fiber and satellite networks with quantum ground relays. This is a complementary field to the development of quantum computers.

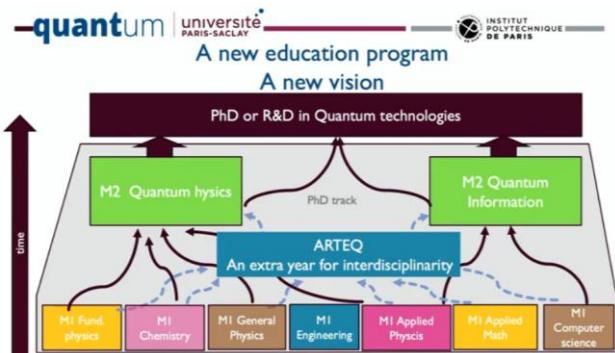
Finally, quantum computing and simulation will progressively evolve and see their field of application widen as the qubits number and quality in quantum computers grows. It will be a process of continuous innovation.

As in the case of classical computing, the weight of software is bound to become dominant in skills requirements. This explains why many publications insist on the need for quantum application developers. This is what the major players such as IBM, Google and Microsoft, not to mention D-Wave, Rigetti and IonQ, are "evangelizing" about<sup>1780</sup>.

Nevertheless, in parallel with the software market development, an intermediate phase will require a lot of skills in engineering and in the different branches of quantum technologies. In some cases, training can be shared between universities, particularly when teachers are scarce. That's what is implemented in the Université Paris-Saclay with the ARTEQ interdisciplinary year positioned before masters M1 and M2, to feed M2 masters in quantum physics and quantum information science.



here is an American inventory of engineering jobs and skills in quantum technologies<sup>1779</sup>



ARTEQ – Interdisciplinary education on quantum technologies	
October – January Lectures + Personal project	Alain Aspect (LCF), Philippe Grangier (LCF) et Jean-François Roch (LUPIN-F)
February – July Internship in QT Entrepreneurship training	Pablo Arrighi (LMF) Benoit Valiron (LMF) et Romain Alléaume (LTCI) Pascale Senellart (C2N) et Jean-Damien Pillet (LSI) Jacqueline Bloch (C2N) et Marc Olivier Goerbig (LPS) Filippo Miatto (LTCI) et Julie Grollier (CNRS-Thales)

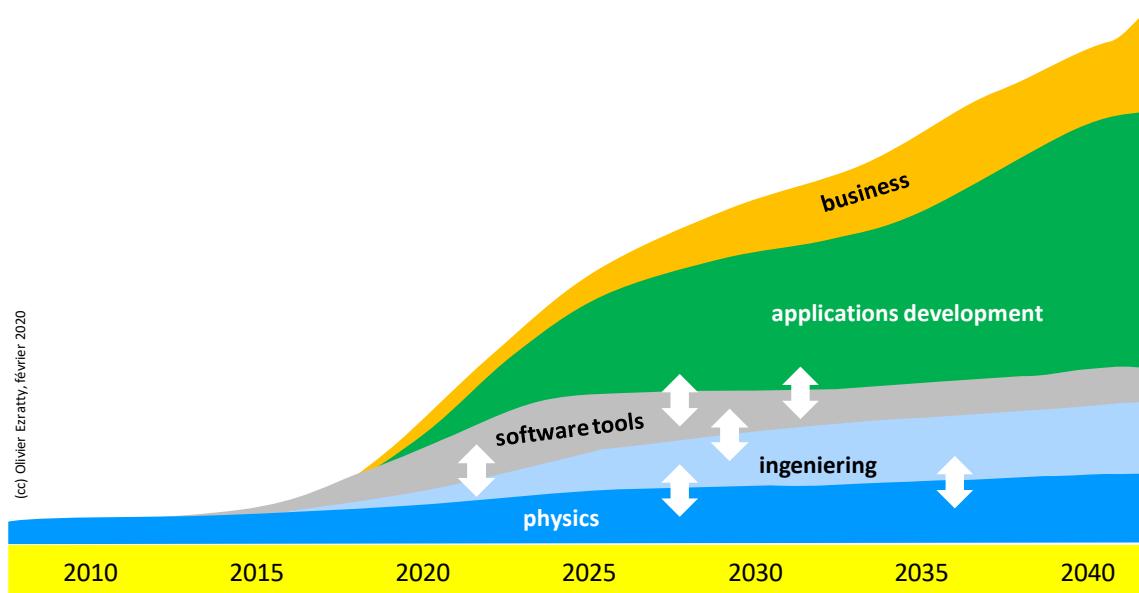
Training in public higher education should introduce quantum science and technology as early as possible in the bachelor's and master's degree programs. It will also be necessary to create master's degrees in quantum engineering, bringing the world of research and engineering closer together.

<sup>1779</sup> Source: [Preparing for the quantum revolution -- what is the role of higher education?](#) by Michael F. J. Fox, Benjamin M. Zwickl et H. J. Lewandowski, 2020 (23 pages).

<sup>1780</sup> Look at it this way: [Quantum Computing Demands a Whole New Kind of Programmer](#) by Edd Gent, May 2017 (slightly ahead of schedule), [The Hitchhiking Cat's Guide to Getting a Job in Quantum Computing](#) by Jay Gambetta, October 2019, [Building Quantum Skills With Tools For Developers, Researchers and Educators](#), IBM Research, September 2019 and [Some useful skills for quantum computing](#) by Chris Granada, January 2020, which also emphasizes mathematical and software skills.

The training offer will depend on several parameters: funding for teacher-researchers or teaching positions, the creation of vocations, the ability to attract teachers and students from wherever they come.

Continuing education may include both scientific and technological courses (quantum physics, quantum communications, quantum algorithms and software) and strategic courses (understanding of the issues, knowledge of the players, economics of the sector, good practices). This is probably the less well address market need so far.



It can or could be delivered by private organizations, by higher education organizations as well as via online courses offered by Coursera and the likes.

Self-training allows enthusiasts to discover these sciences and technologies by themselves, but it is not self-sufficient as it is sometimes the case in artificial intelligence.

It must be complemented by quality pedagogical support, if only to do and correct exercises. As far as the software part is concerned, this will perhaps change the day when development tools will be possible with higher levels of abstraction than today.

Scientific events organized by quantum hubs, research laboratories and companies serve to facilitate transdisciplinarity among researchers and engineers. They can be interdisciplinary symposia, thematic conferences or workshops.

It will also be necessary to attract as many women as men in these courses, otherwise there is a risk that a whole sector will develop, as in AI, which is far too masculine. Not to mention the increase in the diversity of students' social backgrounds, which remains a key means of republican promotion, despite its current decline.

Upstream of all these courses, the creation of vocations among young people is indispensable. Science fairs can also contribute to this. It is a long-term task, as is the creation of vocations in science in general and in the scientific and technical professions of the digital world in particular.

There are some pure players around in the quantum computing educational market, many of them offering open-sourced eLearning contents:



**Q-munity** (2019) is a training organization and community connecting young individuals in quantum computing. With its 1000 members, it organizes summer camps (well, outside pandemics), conferences and workshops.

It was created by Anisha Musti, a quantum computer scientist who worked on Shor's algorithm, quantum teleportation and quantum machine learning.



**QubitbyQubit** (USA) is a quantum programming online learning initiative from The Coding School, created by a Brown University undergraduate in 2014. It was created by Kiera Peltz and is sponsored by IBM and Google.

**Qplaylearn** (2020, Finland) develops an online visual quantum programming training tool targeting a broad audience including high school students. They collaborate with various universities in Finland as well as with IBM.

**Quantum Country** (USA) is a tutorial web site on quantum programming created by Andy Matuschak and Michael Nielsen. It contains “mnemonic medium” that makes it easy to remember what you read. These are long reads including some good story telling and some exercising. It starts with the basics of quantum programming, then covers key algorithms like Grover search.

**QuTech Academy** is offering free online courseware on quantum technologies for engineers<sup>1781</sup>.

CERN has a series of introductory conferences on quantum computing from **CERN** (7 x two hours tracks), broadcasted in November and December 2020, also targeting engineers<sup>1782</sup>.

**Qureca** (Spain) sells “Quantum for Everyone” courses for business people delivered by Araceli Venegas-Gomez, the founder of Qureca, Bruno Fedrici, a French consultant and lecturer on quantum technologies and Quantfi, a French Startup specialized in Finance applications.

**SpinQ Technology** (2018, China) announced Gemini in January 2021, a \$5K 2-qubit desktop quantum computer using the outdated NMR qubit technology, and their cloud quantum computing platform Taurus<sup>1783</sup>. It followed an initial version launched in 2020 and sold at \$55K. The computer weights 55 kg and works at ambient temperature. They plan to increase the number of qubits of this device in upcoming versions, up to a maximum 15 qubits. It would be nice since 2 qubits are nearly useless even for quantum programming training tasks. Meanwhile, you can test for free 15 real superconducting qubits on IBM Q Experience cloud systems.



## Jobs impact

Finally, what about the future of quantum-related employment, a question that Sophia Chen asked herself in Wired in June 2018? It's difficult to assess because we're thinking over several decades and about use cases that are still uncertain. There will be, as with AI, those who know and those who don't, those who code and those who use stuff, those who create wealth and those whose jobs are threatened.



# QUANTUM COMPUTING WILL CREATE JOBS. BUT WHICH ONES?

<sup>1781</sup> See [QuTech Academy Online Learning](#).

<sup>1782</sup> See [Online introductory lectures on quantum computing from 6 November](#), 2020.

<sup>1783</sup> See [SpinQ Gemini: a desktop quantum computer for education and research](#) by Shi-Yao Hou et al, 2021 (14 pages). It was updated with 3 qubits in September 2021 with their Triangulum version.

For the moment, quantum computing does not generate any specific jobs threats, because it will enable us to do things that mankind can't do today. There is no logic of replacement, at most optimization as for applications based on graph optimization like those of the traveling salesman.

## Gender balance

Gender unbalanced in all STEM jobs and particularly in computer science is a known fact and it has been so for a long time. You can look at all the statistics and they are not good. It started to go awry in computer science in the early 1980s when computing became mainstream. Many initiatives have been launched worldwide to rebalance gender in all these domains. They have mostly failed, or maybe did they just made things better than if nothing was done. Are quantum technologies different for gender balance?



## Problems

This domain is already highly male-dominated, in the lineage of computer science and artificial intelligence. The specialty is still too masculine as it stands. Quantum physics founder in History books are mostly men, particularly in the seven first quantum wave theoreticians narrow club with **Planck-Einstein-De Broglie-Schrödinger-Heisenberg-Dirac-Born**. You have to really dig into the History of science to recognize the role of **Emmy Noether** and **Chien-Shiung Wu**, the few female scientists of this era. Also, only three Nobel prizes were awarded to women with **Marie Curie** (1901), **Maria Goeppert** (1963, for her work on nuclear physics) and **Donna Strickland** (2018 for her work in pulse lasers). But besides Marie Curie, they don't yet have the recognition status of **Linda Lovelace**, **Grace Hopper** and **Margaret Hamilton** in computer science.

The statistics are depressing with only 20% women in STEM (in the USA) and it doesn't seem to be better in quantum science<sup>1784</sup>. Women's representations in culture, media and toys still play a leading role in crafting this unbalanced world.

<sup>1784</sup> See [The Quantum Computer Revolution Must Include Women](#) by Chandrakha Singh, Scientific American, January 2021 and [The Upcoming Women In Quantum Summit III And Its Secret 70 Year-Old Legacy](#) par Paul Smith-Goodson, December 2020. See also [Women in Quantum Technologies - What are the challenges](#), February 2020.

Only a few countries are faring better, like in Asia. Is the condition of women in universities and research labs different than in business organizations? It probably depends on their values, leadership and culture. The scientific world seems as competitive and tough than the private sector even if its rules are different, based on h-indexes, conference talks and the likes. Still, in most places, research is a longer term activity which may create better conditions for women.

On top of that, the language used in quantum science is very masculine<sup>1785</sup>. It evokes the notions of superiority (supremacy) and auxiliaries (ancilla), the former echoing a higher authority, and the current "white supremacy" resulting from South African Apartheid and which is still stirring the US political scene. The second notion takes up the notion of "female servant" in Latin, slavery and racial segregation, whereas the technical term was coined in 1995. These are symbolic items but they deserve to be corrected. One solution is to talk about quantum advantage even if the meaning is slightly different from quantum supremacy. It seems going on in the right direction.

## Hope

There's still hope. It seems easier to identify dozens of women who are real inspiring role models and play a key role in quantum science and technologies and anywhere in the world. Many of these were at the origin of key scientific advancements in quantum technologies. You may know the famous threshold theorem co-demonstrated by **Dorit Aharonov**! There are a few startups created by women like Silicon Quantum Computing (SQC, Australia), created by **Michelle Simmons**, Oxford Quantum Circuits that is led by **Ilana Wisby**, Quandela, co-founded by **Pascale Senellart**, VeriQloud co-founded by **Elham Kashefi** and Qureca, created by **Araceli Venegas-Gomez**. In the Corporate world, **Krysta Svore**, **Patty Lee** and **Anna Matsuura** play leading roles at respectively Microsoft, Honeywell Quantum Systems and Intel. In Europe, **Laure Le Bars** leads SAP's quantum research efforts on top of being the first President of the QuiC industry consortium.

Also, quantum tech is still a green field and it's not too late to attract young women in this emerging and promising discipline. There are already women playing leading technical and business roles in quantum startups on top of the cofounders mentioned above<sup>1786</sup>.

## Initiatives

Some initiatives have been launched around the world to promote and help women in quantum technologies. They are matching what has been done for a while in the computer science and information technology fields. Gender oriented actions are a mix of associations, events and media visibility initiatives. Too many of these are seasonal, and centered around the Woman's Rights day, on March 8<sup>th</sup>, each and every year.

Let's mention a few of these:

- **Women in Quantum** by **OneQuantum** is a think tank gathering quantum leaders worldwide in dedicated chapters, with the goal to influence government action, vendor relationships and the quantum ecosystem. It offers a resources, services and events platform for quantum startups to collaborate. Women in Quantum is one of the "chapters" of this organization, run by Denise Ruffner (also, VP IonQ Business Development), organizing quarterly Women in Quantum events, the last one being held online in June 2021<sup>1787</sup>.

---

<sup>1785</sup> As Karoline Wiesner of the University of Bristol points out very well in her succinct [The careless use of language in quantum information](#), 2017 (2 pages).

<sup>1786</sup> See [52 Wonder Women Working In Industry As Quantum Scientists & Engineers](#) by James Dargan, The Quantum Daily, August 2021.

<sup>1787</sup> See the [casting of the Fall 2020 edition](#).

- **Women in Quantum Development** is a professional network of quantum tech enthusiasts in the Netherlands, with events and mentoring programs. It belongs to a new trend, with national quantum plans containing specific initiatives around the ethics and social impact of quantum technologies. Netherlands is a good best practice for that respect. There's also a gender equality workgroup in the EU **Quantum Flagship** ([source](#)).
- The **University of Bristol** organized a two-day Women in a Quantum Engineering event in December 2019.
- Some research labs and organizations showcasing their women quantum scientists and engineers like at the **Lawrence Berkeley National Lab** from the DoE in the USA<sup>1788</sup>, at the **Harvard** Center for Integrated Quantum Materials<sup>1789</sup>, at **Yale**<sup>1790</sup>, with **IBM**<sup>1791</sup> and **Microsoft**<sup>1792</sup>.
- **SheQuantum** (2020, India) is an eLearning provider offering quantum computing education content targeting women.
- In France, the association **Quelques Femmes du Numérique!** promotes women in tech, particularly engineers and scientists using quality photography portraits with over 750 women in various fields (artificial intelligence, Blockchain, cybersecurity, IT, etc) and over a dozen in quantum techs<sup>1793</sup>. It launched many initiatives including promoting quantum science to female teenagers.

## Solutions

Like in any domain, particularly in social science, there's not yet a common agreement on what should be done to create a better gender balance in STEMs and in quantum science.

Should we encourage some affirmative actions or not? Some are worth the effort like the European Union ERC Grant program which extends since 2010 the age limit by 18 months per child plus other anti-bias measures. Paternity leaves are also taken into account<sup>1794</sup>.

In the way women scientists and entrepreneurs are promoted, I believe we should be more engaged but with subtlety. For example, it's more efficient to value scientists and entrepreneurs for their achievement and who happen to be women instead of doing this explicitly because they are women. An implicit communication is sometimes more efficient than an explicit one. Finding women talents should be a sort of backstage work. It requires some discipline. When organizing training and events, and with any media speaking opportunity, make sure gender balance is respected. It involves having some knowledge of the field ecosystem and of its female leaders. Don't say "there are only a few of them", but "where are they?" and look for them. Also, let them talk about their science.

We should also promote a broad range of role models in different fields and jobs to inspire young talents, particularly with young ones.

It's also about building inclusive and welcoming work environments in universities, research labs and commercial vendors.

<sup>1788</sup> See [Women of Quantum Computing Go Tiny in Big Ways](#) by Elizabeth Ball, June 2021.

<sup>1789</sup> See [Ask a Scientist: Women in Quantum Science and Technology](#), November 2020.

<sup>1790</sup> See [WIQI \(Women in Quantum Information\) Group](#).

<sup>1791</sup> See [Encouraging more women in quantum: four insights from four women](#), IBM UK, March 2021.

<sup>1792</sup> See Women of Microsoft Quantum [Part 1](#) and [Part 2](#), March 2020.

<sup>1793</sup> Disclaimer: I'm the cofounder and photographer of this association. Whenever I can in media and events speaking opportunities, I propose to create a duo with one the quantum scientists women I know well.

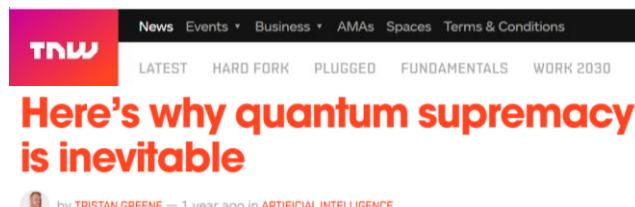
<sup>1794</sup> See [ERC Gender Actions](#), 2021 (14 slides). It provides some data on the share of women applicants vs men who get ERCs and H2020 grants based on the discipline. Across the board, women have about 20% less chance to get a funding.

Of course, in a broader scale, media and fiction play a key role. The geek in TV series and movies is too frequently an introverted male. We need more Felicity Smoak, the geek from the TV Series Arrow!

At last, do that all year long and not just on March 8<sup>th</sup>.

## Quantum technologies marketing

The last point to be mentioned here is the role of marketing and propaganda. Quantum technologies are the perfect spot to broadcast extraordinary and impressive claims that few specialists can fact-check. It's a world of superlatives and exaggerations. It started in 2019 with Google's supremacy claim.



News Events Business AMAs Spaces Terms & Conditions  
LATEST HARD FORK PLUGGED FUNDAMENTALS WORK 2030

## Here's why quantum supremacy is inevitable

by TRISTAN GREENE — 1 year ago in ARTIFICIAL INTELLIGENCE



The Register®  
Biting the hand that feeds IT

### Emergent Tech

## 'Quantum supremacy will soon be ours!', says Google as it reveals 72-qubit quantum chip

Don't panic: 'supremacy' is the point at which quantum kit trumps classical computers

By Richard Chirgwin 6 Mar 2018 at 08:36



Computing / Quantum Computing

## Google thinks it's close to "quantum supremacy." Here's what that really means.

It's not the number of qubits; it's what you do with them that counts.

by Martin Giles and Will Knight

Mar 9, 2018

We are going to be drowned in innovation propaganda that will blur things. Scientists in the field will no longer recognize their creations.

Popular news related to quantum computing will continue to start explaining qubits with their superposed states 0 and 1 and... stop there!

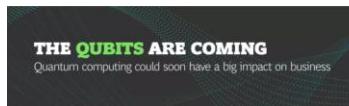
Marketing and communication are all about making fancy claims and simplifying facts with wild exaggerations.

Consulting firm will also strive in simplifications. This **BCG** set promoting quantum computing in the pharmaceutical industries is quite amazing although, hopefully a bit dated<sup>1795</sup> (*below*). They mention the ability of a quantum computer to solve an "*infinite number of problems simultaneously*", confusing, infinity and exponentiality, then superposition and problems.

They did estimate the quantum computing market in the pharmaceutical industries in the USA to sit between \$15B and \$30B with no precise date. Well, a market forecast dated from 2018 expected that global IT spending dedicated to drug discovery would have reached \$5.3B by 2020<sup>1796</sup>!

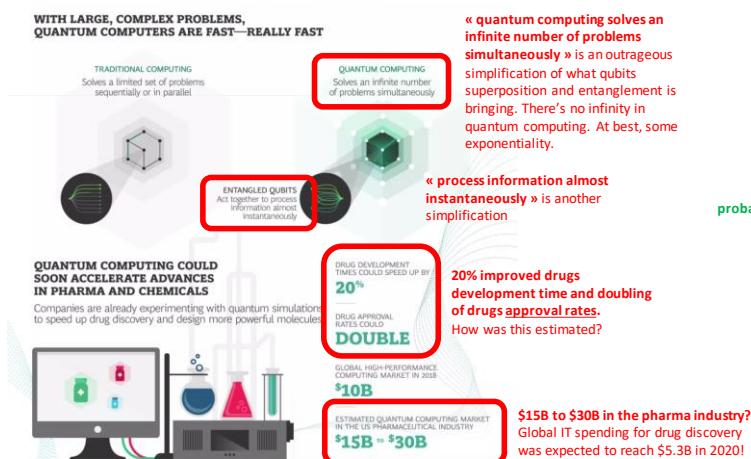
<sup>1795</sup> Source: [The Qubits are coming](#), BCG Henderson Institute, June 2018, extracted from the report The Coming Quantum Leap in Computing.

<sup>1796</sup> Source: [Growth Insights Report: Global Pharmaceutical Drug Discovery IT Solutions Market 2017-2020 - Key Initiatives by Big Pharmaceutical Companies](#), January 2018.

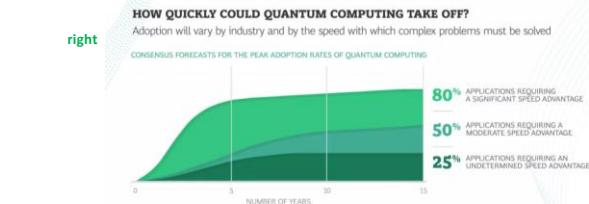


BCG

THE BOSTON CONSULTING GROUP



source : <https://www.bcg.com/publications/2018/qubits-are-coming-infographic.aspx>  
comments by Olivier Ezratty, September 2018, updated in 2021.



#### THE QUANTUM COMPUTING MARKET WILL EVOLVE IN THREE OVERLAPPING GENERATIONS

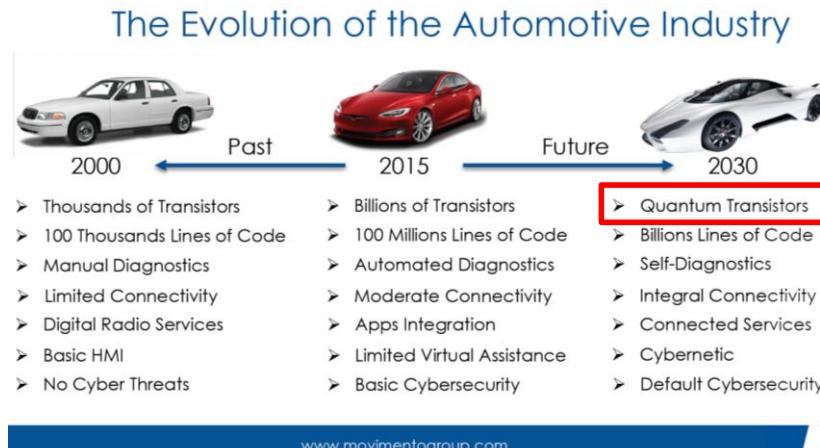


BIG EXPECTS A DECADE OF STEADY PROGRESS IN QUANTUM COMPUTING, FOLLOWED BY A SIGNIFICANT BOOST IN CAPABILITIES AFTER 2030



And yet I am the first to be convinced of the benefits of quantum computing in pharmaceutical applications, and in particular in simulating the behavior of organic molecules! These die-cut exaggerations are delirious and remind me of those that were made about the Internet of things a few years ago.

In the same vein, the **quantum transistors** evoked in this presentation by Movimento Group for the autonomous vehicles of 2030, stem from a lack of knowledge of the state of the art of quantum computing, its speed of progression and the physical nature of qubits ([source](#)). Bearing in mind that transistors have been using quantum phenomena since their creation!



Another phenomenon that is bound to become recurrent is the propensity of the media to get confused by vendors and research labs claims!

## Quantum technologies and society key takeaways

- Quantum technologies can become one of the artefacts of Mankind's technology ambitions, pushing the limits of what can be achieved in the line of some works done in artificial intelligence. It may give the impression that mankind's power has no limit. A sound scientific mind will however understand that quantum computing has its own limits. The world can't be simulated, the future can't be predicted and apparent free will will persist.
- Science fiction has built an imaginary of what quantum technologies could achieve, with teleportation, supraluminal traveling speeds, various entanglements and miniaturization feats, parallel or multiverse worlds and time travel. While none of these things are possible given our current scientific knowledge, it can create scientific vocations and drive new generations to solve actual problems.
- Quantum foundations is the branch of science philosophy that aims to build some understanding of the real world. Quantum physics' formalism is difficult to associate with the principles of reality usually applicable in classical physics. While classical physics understanding has historically been associated with an ontology with objects position and motion enabling the prediction of phenomena such as the motion of planets. Quantum physics lacks such an ontology describing the physical world. Beyond the canonical Copenhagen interpretation (psi and the wave equation), many scientists tried to create such ontologies and the debate is still raging.
- The quantum scientific community is starting to investigate the ethics of quantum technologies. Like with artificial intelligence, it will be questioned on algorithms explainability and auditability, on what it will do to simulate if not tweak matter and life and on how to handle public education. Some related initiatives have already been launched by scientists in Australia, The Netherlands, Canada and the UK.
- The education challenge around quantum sciences and technologies is enormous, both for the general public and with specialists. There's a need for better pedagogy, accessible educational content and also for sound fact-checking information.
- Gender balance is already an issue in quantum technologies with a low share of women in the field, particularly with vendors. Hopefully, there are many top women scientists and entrepreneur role models around who can inspire a new generation of women teenagers. Many initiatives around the world have been launched for that respect.
- At last, quantum technologies vendors marketing must be watched carefully. It is and will be full of exaggerations and approximations. The worse will happen with vendors outside the quantum technology sphere.

# Quantum fake sciences

One of the most fascinating topics in the mainstream impact of quantum physics is the way some people integrating it into alternative dubious scientific approaches. The vast framework of "quantum medicine" is a fairly coherent stream of thought and practice from this point of view. It has given rise to the proliferation of gurus of all kinds and to voluntary or involuntary scams based on miracle machines for detecting electromagnetic waves or vague energies, and restoring your body balance. It is at best a subset of the vast placebo effect industry!

Other fields took over quantum physics and long before quantum computing became a visible subject: management and marketing, not to mention politics<sup>1797</sup>. Quantum physics is essentially used there as a source of inspiration by analogy. But the "gurutisation" of these sectors is also quite common, linking together currents of thought that revolve a lot around magical thinking.

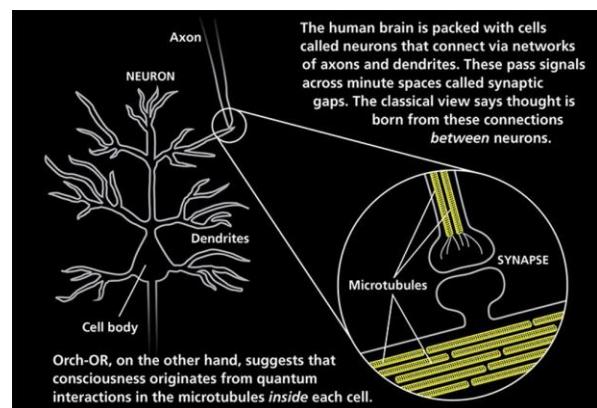
## Quantum biology

The starting point of quantum medicine is, however, scientifically relevant and interesting. Some low-level biological phenomena can be well explained at a low-level by quantum physics. Of course, since everything is quantum at this scale!

To mention just a few examples, this is obviously the case of **photosynthesis** in plants, which uses the photoelectric effect transforming a photon into electron displacement, leading after the Calvin cycle to the production of glucose that is used to store energy. The same applies to **retina cones and rods** which capture light. **UV-B rays** participate in the synthesis of Vitamin D3 precursors in the skin ([source](#)) again using the photoelectric effect but with a different wave length. Quantum physics also explains the **capture of terrestrial magnetism** in the brains of many birds via a special protein called cryptochrome. This mechanism relies on the protein's ability to detect magnetic variations through some electrons quantum entanglement ([source](#))<sup>1798</sup>. So far so good.

Then, some renowned scientists want to explain the origin of consciousness with quantum physics. Several major schools of thought are related to each other: the **Orch-OR theory**, the **holographic dimension** of DNA and **biophotons**. And then there are all the works around **structure of water** and **water memory**.

None of this work has obtained the agreement of a majority of scientists, but it still deserves a little review. If only to understand how they are quickly being misused.

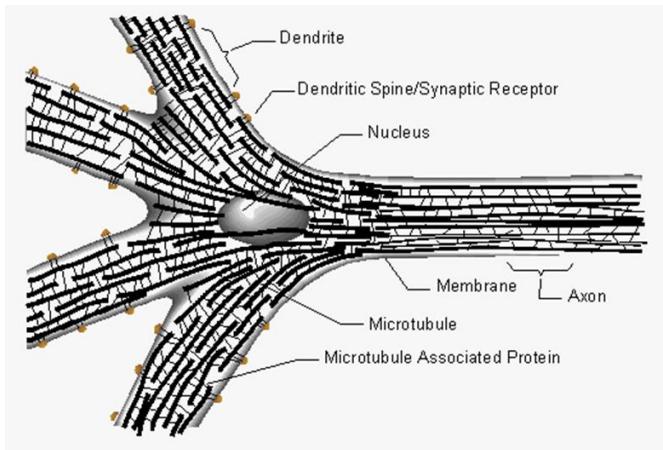


<sup>1797</sup> The concept of quantum politics is still in its infancy. Here is some literature from economic and social researchers on the subject. For example, [Quantum like modelling of the non-separability of voters' preferences in the US political system](#) by Polina Khrennikova, University of Leicester, 2014 (13 pages) seeks to model the choices of US voters and the entanglement or not of the choice of presidential candidate and congressional candidates showing that it can decouple under certain conditions. And [Quantum Politics: New Methodological Perspective](#) by Asghar Kazemi, 2011 (15 pages) creates a link with chaos theory and the butterfly effect. The paper was written just after the 2011 Arab revolutions. See also [Schrodinger's Cat and World History: The Many Worlds Interpretation of Alternative Facts](#) by Tom Banks, who uses Bryce DeWitt's Multiple Worlds Thesis to explain the election of Donald Trump in 2016 by a giant tunnel effect. That maaaayyy be a little far-fetched!

<sup>1798</sup> See [Resonance effects indicate a radical-pair mechanism for avian magnetic compass](#) by Thorsten Ritz et al, 2004 (4 pages), [Cellular autofluorescence is magnetic field sensitive](#) by Noboru Ikeya and Jonathan R. Woodward, January 2021 (6 pages) and [Magnetic sensitivity of cryptochrome 4 from a migratory songbird](#) by Jingjing Xu et al, June 2021.

## Orch-OR Theory

According to **Roger Penrose** (English, 1931<sup>1799</sup>) and **Stuart Hameroff** (American, 1947), consciousness is housed and managed by microtubules, the complex fibrous structures that, together with actin filaments and intermediate filaments, constitute the structure of neuron cells, called the cytoskeleton, and in the case of neurons, the dendrites, synapses and axons<sup>1800</sup>. In 1996, they proposed the Orch-OR (Orchestrated Objective Reduction) model according to which these microtubules were coherent quantum systems explaining consciousness.



For them, consciousness is managed in the neurons within these microtubules and not by their interconnections via dendrites/synapses pairs.

In 2011, Roger Penrose and Stuart Hameroff even suggested that these microtubules would be quantum nanocomputers capable of managing qubits and associated calculations<sup>1801</sup>. If this were true, the power of this computer in number of qubits would be immeasurable because a single neuron comprises about 100 million tubules, the brain 86 billion neurons and more than 600 trillion connections between neurons! These theories obviously do not specify how the entanglement between these qubits would work on this scale. Ironically, the indirect impact of this gargantuan sizing would be to push back even further in time a possible singularity, the moment when a computer would reach the computing capacity of a human brain in raw computing power<sup>1802</sup>. We are dealing here with another current of thought, promoted in particular by **Ray Kurzweil**.

The Orch-OR theory was revived in 2014 with the discovery of quantum vibrations in microtubules by **Anirban Bandyopadhyay** from National Institute for Materials Science in Japan<sup>1803</sup>. But that doesn't explain anything. Consciousness is a "macro" phenomenon.

Trying to explain a "macro" phenomenon by a single "nanoscopic" process is meaningless because it completely gets rid of the entire biological hierarchy between the two and the other nanoscopic mechanisms at stake in the nervous system: neurons themselves, neurotransmitters, synapses and

---

<sup>1799</sup> He was awarded the Nobel prize in physics in 2020 for his seminal work on black holes.

<sup>1800</sup> Illustration source: [Is our brain a quantum computer?](#) by Laurent Sacco, April 2018.

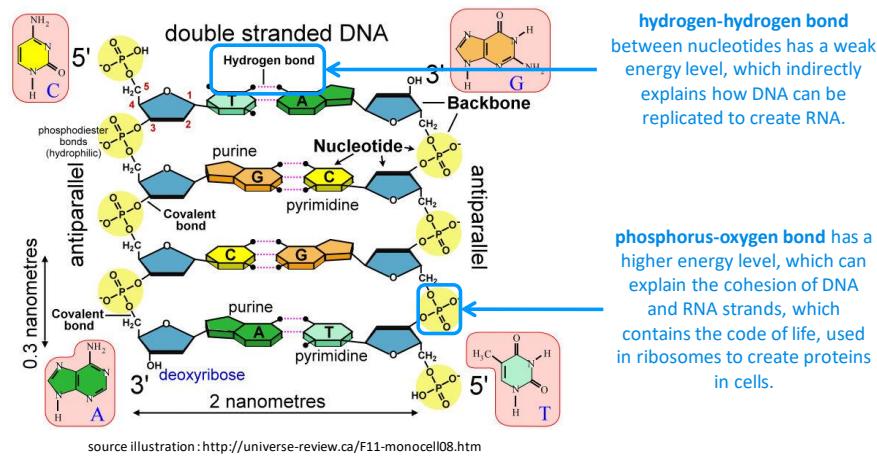
<sup>1801</sup> Other theories think that quantum entanglement also works elsewhere in the brain, at the level of phosphorus atoms associated with calcium. This would allow the creation of quantum bonds between neurons. See [Quantum Cognition: The possibility of processing with nuclear spins in the brain](#) by Matthew Fisher, 2015 (8 pages). As the article indicates, this raises questions but does not provide answers! Therefore, any rather rapid interpretation of the "quantum brain" is to be taken with a grain of salt.

<sup>1802</sup> See [Consciousness in the Universe Neuroscience, Quantum Space-Time Geometry and Orch OR Theory](#) by Roger Penrose, 2011, 50 pages). All this is documented in [Orchestrated Objective Reduction of Quantum Coherence in Brain Microtubules: The "Orch OR" Model for Consciousness](#), 1996 (28 pages) as well as in [Consciousness, Microtubules, & 'Orch OR' A 'Space-time Odyssey'](#) by Stuart Hameroff, 2013 (28 pages), [Are Microtubules the Brain of the Neuron](#) by Jon Lieff, 2015 and popularized in [The strange link between the human mind and quantum](#) by Philipp Ball, 2017. Roger Penrose has collaborated with Stephen Hawking on gravitational singularities and radiation emission from black holes. Hawking had developed a cosmological theory combining the theory of relativity and quantum physics.

<sup>1803</sup> The discovery is disputed by Matti Pitkanen in [New Results about Microtubules as Quantum Systems](#), 2014 (18 pages).

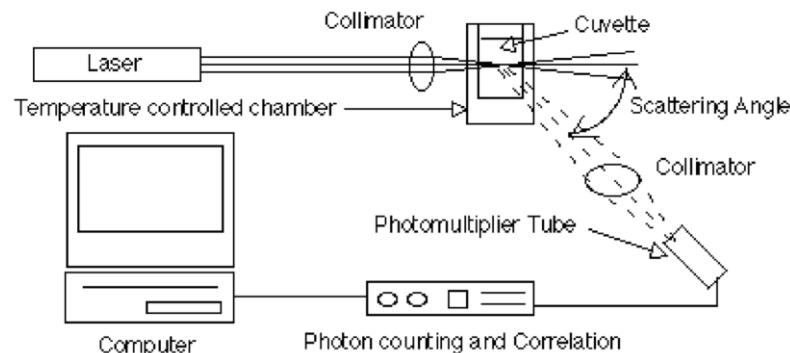
dendrites, neurons nucleus, brain regulatory glial cells, and on a larger scale, senses and brain macro-organization<sup>1804</sup>.

For example, we can explain a good part of living things via the weak hydrogen-hydrogen bonds - (which is quantum, of course) that links the two DNA strands, or with the oxygen and phosphorus bonds, in DNA and RNA, which are strong and can thus explain the cohesion of these fundamental molecules of living things.



However, this is obviously not enough to explain consciousness or how heart and kidneys work. One could also easily build a bozo theory associating consciousness with electrons. Well yes, without electrons, there's no chemistry and no consciousness! It explains the chemical bonds between atoms. Fortunately, nobody has yet ventured into this kind of explanation. In short, explaining consciousness by the possibly quantum nature of a particular structure of neurons is the most simplistic reductionism possible, ignoring all the other knowledge available... or yet unavailable.

DNA would also have a quantum function. A curious paper of Russian, German and English origin describes quantum and non-localized phenomena in DNA, verified in a famous experiment based on laser light diffraction (*opposite*)<sup>1805</sup>. [The bio-digital DNA wave](#) (20 pages) explains that DNA is in fact a hologram, which interacts with its environment with laser radiation.



Through quantum entanglement, the chromosomes of several cells would interact with each other via these radiations. The Russian of history and leader of this work is a certain **Peter Gariaev**, creator of the concept of BioHolograms within his **Wave Genetics Institute** in Moscow<sup>1806</sup>.

Other attempts to explain consciousness by quantum physics have been created. **Matthew Fisher** from UCSB wanted to investigate the brain's potential for quantum computation, based on phosphorus ions spin entanglement<sup>1807</sup>. He launched his **Quantum Brain Project** (QuBrain) with a 1M€ funding in 2018 from the Heising-Simons foundation. Since then, the Project was discontinued.

<sup>1804</sup> See this interesting discussions on Orch-OR in [Why is Orch-OR ignored by the mainstream scientific community?](#), Quora, and also [Falsifications of Hameroff-Penrose Orch OR Model of Consciousness and Novel Avenues for Development of Quantum Mind Theory](#) by Danko Dimchev Georgiev, 2006 (32 pages) which debunks many of Stuart Hammeroff and Roger Penrose assertions in the Orch-OR model with an in-depth neurobiology analysis.

<sup>1805</sup> See [DNA as Basis for Quantum Biocomputer](#), 2011 (22 pages),

<sup>1806</sup> The history of the theme is explored in [Quantum BioHolography A Review of the Field from 1973-2002](#) by Richard Alan Miller, Iona Miller and Burt Webb (23 pages), but these texts do not give any idea of its scientific validity.

<sup>1807</sup> See [Quantum Cognition: The possibility of processing with nuclear spins in the brain](#) by Matthew P. A. Fisher, 2015 (8 pages).

Others like **Johnjoe McFadden** from the University of Surrey in the UK try to explain consciousness with electromagnetic waves circulating in the brain<sup>1808</sup>.

## Biophotons

Another alternative school of thought is related to **biophotons**. These are the low light emissions in the visible generated by living beings. They were discovered in 1922 by the **Alexander Gurwitsch** (Russia). The theory of biophotons was perfected by the **Fritz Albert Popp** (Germany). It complements at a low-level the hologram DNA thesis.

It describes the emission of photons from molecules such as DNA, but also the emission of photons related to the energy metabolism of cells such as the transformation of ADP molecules into ATP in the mitochondria of cells.

The biophotons are ultraviolet and visible light emissions, at levels that are much lower than the mid-infrared emission occurring at around 12 microns wavelength. Up to a few hundred photons per square centimeter of organ analyzed could be detected, often at the skin level.

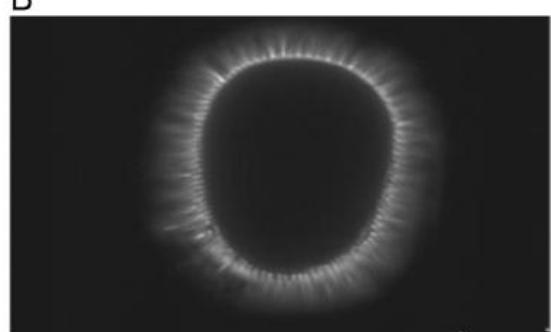
These biophotons are also made of coherent light - photons with the same frequency. They would constitute a form of inter-cellular communication<sup>1809</sup>. I wonder how this communication works: at what range, due to the obvious attenuation of photons scattering, and with what precision targeting (direction, orientation).

According to Fritz Albert Popp, raw foods emit more biophotons than cooked foods, and organic raw plants emit five times more biophotons than traditionally grown plants. Conclusion: eat raw and organic! This is also a reason to have prehistoric men regret having discovered fire!

A



B



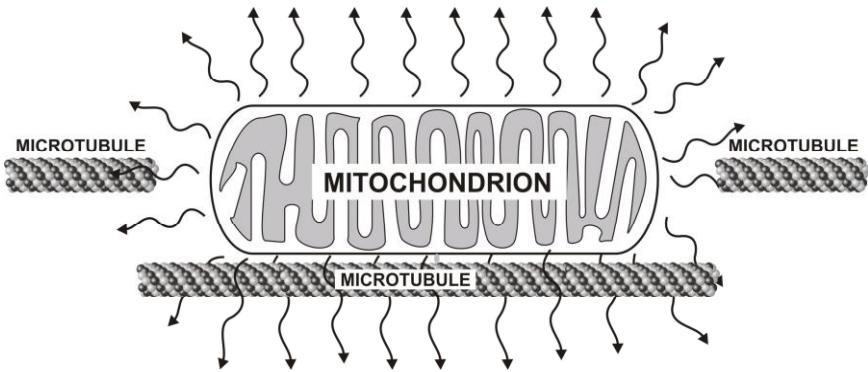
In any case, the detection of biophotons on the 10 fingers of the hand would make it possible to detect cardiac pathologies<sup>1810</sup>. The **ClearView** scanner used exploits a curious process: it sends a high-voltage pulse that creates an electromagnetic field around the finger that amplifies the biophotons that are emitted. This excites molecules in the air, creating a plasma between the sensor and the finger (*above left*) that ionizes the air, generating the emission of UV and visible light. This is the **Kirlian effect**, discovered by the Russian Semyon Kirlian in 1939.

<sup>1808</sup> See [Integrating information in the brain's EM field: the cemi field theory of consciousness](#) by Johnjoe McFadden, September 2020 (13 pages) covered in [New research claims that consciousness itself is an energy field - a professor says this could be the key to building conscious machines](#) by Victor Tangermann, in Futurism, October 2020.

<sup>1809</sup> As described in [Photonic Communications and Information Encoding in Biological Systems](#) by S.N. Mayburov, 2012 (10 pages) and popularized in [Biophoton Communication: Can Cells Talk Using Light?](#), 2012 in the MIT Technology Review.

<sup>1810</sup> According to [Detecting presence of cardiovascular disease through mitochondria respiration as depicted through biophotonic emission](#) by Nancy Rizzo, 2015 (11 pages).

The ionization that is captured by the camera (*above right*). The software analyzes the generated shape and compares it to a pathology database. I have a hard time figuring out the exact link between bioluminescence and this process! And what about the receptors of these biophotons?



Well, it comes from the neurons microtubules, of course, closing the loop<sup>1811</sup>! According to Popp: "matter would only be condensed light"<sup>1812</sup>. By the way, biophotons would be a way to explain chi.

David Muehsam mentions many biological effects of biophotons, which would be involved in the regulation of neurotransmitters secretion (for rats) but without the distinction between correlation and causality being visibly made in the associated publications<sup>1813</sup>.

If all that was just science and research! But hell no. It helps snake oil vendors to sell miracle healings through the control of the body by conscience. Practitioners of quantum medicine are very often psychosomaticians exploiting mysticism and autosuggestion to generate, in the best of cases, a good placebo effect that can work with certain mild pathologies. Even so, they justify their methods on the contested work of researchers such as Roger Penrose and Stuart Hameroff, already mentioned, but also Karl Pribram and Henry Stapp, who want to explain human consciousness by quantum phenomena intervening at a low-level in the brain that would also explain a so-called immortality.

Wikipedia's [Quantum Mind](#) fact sheet reports on the evolution of this branch and the associated criticisms. It underlines the fact that there is no way to apply possible quantum phenomena such as entanglement at the scale of macroscopic brain molecular or cellular structures.

Entanglement is even less justifiable to connect the brain at long distance to the "*holographic global consciousness of the Universe*" promoted by **Karl Pribram** and **Paola Zizzi**<sup>1814</sup>. In the same way, it does not necessarily make sense to link mind and matter as waves and particles and their famous duality. This leads otherwise to absurdities that explain psychic phenomena of synchronicity by the collapse of the wave function of consciousness, an explanation as absurd as Schrödinger's cat thought experiment. Even if the theories of Penrose and Hameroff were verified, the shortcut would be a little hasty, moving quite too fast from a nano-phenomenon to a macro-phenomenon!

The other commonly proposed method involves the use of various electromagnetic waves, including the famous and smokey **scalar waves**. The idea is to exploit them to restore the balance of unbalanced organs, exploiting the wave-particle duality and the ability to restore the basic energy level of... we don't know. Particularly given the proposed waves are not really targeted.

<sup>1811</sup> This is what comes out of [Emission of Mitochondrial Biophotons and their Effect on Electrical Activity of Membrane via Microtubules](#), 2010 (22 pages, diagram on mitochondrion in a previous page).

<sup>1812</sup> See [Introduction of Consciousness in Matter from Quantum Physics to Biology](#) (18 pages) by Jacqueline Bousquet, a former CNRS researcher who died in 2013.

<sup>1813</sup> See [The Energy That Heals Part II: Biophoton Emissions and The Body of Light](#) by David Muehsam, April 2018.

<sup>1814</sup> See [Consciousness and Logic in a Quantum-Computing Universe](#), 2006 (25 pages).

It is notable, however, that few scientific specialists in quantum medicine mention the capabilities of future quantum computers to simulate the operations of organic molecules and create new therapies. Maybe because known applications of quantum computing in health care are part of traditional allopathic medicine, that they usually avoid or at least complement.

However, I found a vague trace of with **Matti Pitkanen** (Finland) who, in the framework of his work on TGD (Topological Geometrodynamics), proposes a unified theory of physics, and puts forward the idea of creating DNA-based quantum computers<sup>1815</sup>. He believes that DNA communicates "with the Universe". It is also based on Luc Montagnier's experiments on DNA. Matti Pitkanen provides the basis for highly speculative theories on the supposed consciousness of the Universe<sup>1816</sup>. His theories of the unification of physics are so complex that they are impossible to understand, and eventually to validate by experience or to refute.

In the field of light-based therapy, one puzzling solution being sold comes from **Bioptron AG** (1988, Switzerland), part of **Zepter Group** (1986, Switzerland), since 1996. Its "Bioptron Quantum Hyperlight" uses "hyperpolarized light" generated with fullerene ( $C_{60}$ ), a molecule also used by Archer for trap its electron spin qubits. Among other benefits, it treats injuries pain, avoiding pain killer drugs. So far, so good. The system generates some vertically linearly polarized light which passes through a filter containing these fullerene molecules which happen to rotate at a  $1.8 \times 10^{10}$  frequency per second. It creates "*perfectly ordered hyperpolarized light*" that is supposed to have some quantum properties similar to those of the biomolecules inside our bodies. Practically, this light is made of both vertically and horizontally polarized photons that "*without exaggeration, [...] reestablish the balance and harmony of energetic processes in biostructures and to harmonize cells, bringing them to back to their initial state of natural equilibrium*". Contrarily to many of the pseudo-quantum scams we'll cover later in this section, this offer is fairly well documented, even scientifically<sup>1817</sup>. You're flooded by tons of scientific information, historical references, links to Nobel prize inventions and scientific publications. But many indices generate serious doubts<sup>1818</sup>. Among others, it mentions these dubious Emoto's research on water structure and the way it can be changed with music and good mood.

## Water memory

The last area on the fine line between science and charlatanism is that of water. It features a model of thought close to Penrose's **Orch-OR** theory, which consists in explaining everything about life based on a few isolated physical phenomena at the microscopic level. The phenomenon of the **memory of water**, its explanation by **electromagnetism**, and parallel theories on the **water structure** are all mixed together.

One of the starting points around the role of water is **Jacques Benveniste**'s work on water memory. This immunology and allergies specialist was a director of an Inserm research laboratory in Clamart, France.

---

<sup>1815</sup> See [Quantum Mind, Magnetic Body, and Biological Body](#) by Matti Pitkanen, August 2018 (186 pages).

<sup>1816</sup> See [TGD Universe as a conscious hologram](#), February 2018 (612 pages).

<sup>1817</sup> See the [Bioptron Quantum Hyperlight](#) brochure (60 pages) and [Hyperpolarized light](#) 2018 (318 pages) by Djuro Koruga.

<sup>1818</sup> Some are well documented in an extensive analysis, although a bit dated, in [Cancer and the magic lamp](#), February 2009. It shows that most scientific surveys were of small scale and non audited and with no control group trials. It was done only on wounds healing. But the vendor web site touts many medical indications that their device is supposed to treat, without any scientific evidence, beyond wounds healing: osteoarthritis, arthroses, lowered motivation and the inability to feel happy. All are good indications, in the best case, of some placebo effect. On top of that, the Zepter also sells blue and red LED light therapy devices, for 500€. The Bioptron is [priced](#) at about 1000€.

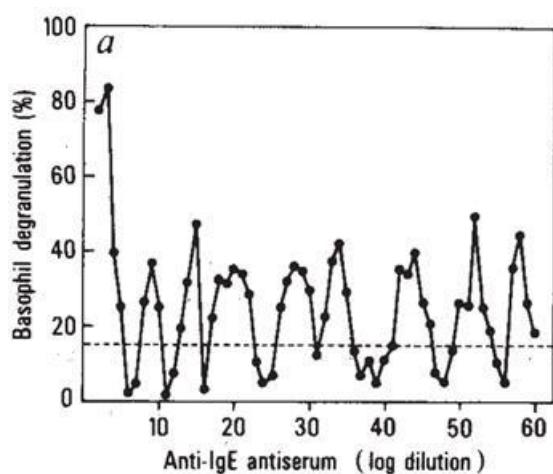
He conducted experiments that led to the conclusion that "water could preserve a memory, a print, of substances that have passed through it". Accompanied by Israeli, Italian and Canadian researchers, he published a landmark article in Nature in 1988, which was soon contested<sup>1819</sup>. He described a series of experiments that showed the effectiveness of anti-IgE (anti-immunoglobulin E) causing the loss of histamine-containing granules by a type of white blood cell, basophilic cells, even when this anti-IgE is repeatedly diluted to the point where no anti-IgE molecule can be found in solution. For this to work, solutions must be shaken vigorously after each dilution. This is the principle of "dynamization"!

In the article, Benveniste hypothesized that the phenomenon could be explained by the creation of structured networks in water or by persistent electric or magnetic fields. They would constitute some sort of "water memory" which would "record" the allergen characteristics and reproduce its effects on basophilic cells.

Therefore we propose that none of the starting molecules is present in the dilutions beyond the Avogadro limit and that specific information must have been transmitted during the dilution/shaking process. Water could act as a 'template' for the molecule, for example by an infinite hydrogen-bonded network<sup>12</sup>, or electric and magnetic fields<sup>13,14</sup>. At present we can only speculate on the nature of the specific activity present in the highly diluted solutions. We can affirm that (1) this activity was established under stringent experimental conditions, such as

This was supposed to explain high dilutions used in homeopathy! The promoters of this empirical medicine devised by **Samuel Hahnemann** around 1810 and explained in the book "The Organon" thought they had finally found their scientific support.

Testing and evaluation protocols were flawed in many ways. Solutions were not analyzed by spectrographic analysis to deduce their molecular composition<sup>1820</sup>. Only electrophoresis was used to detect the presence of ions<sup>1821</sup>. The presence of histamine resulting from the release of granules from the basophiles had not been assessed. It was realized in other experiments that there was none! Moreover, the phenomenon presented a cyclic character of a period of 8 dilutions (*opposite*), according to the successive dilutions, but being out of phase by four dilutions from one experiment to another. No explanation is given for this cyclic phenomenon<sup>1822</sup>.



The electromagnetic theory that would explain the phenomenon is his other Achilles' heel. It is weakly substantiated. These waves are not characterized, measured nor their source explained. The story of Jacques Benveniste is the story of a curious experimenter who lacks, however, the bases in adjacent disciplines around electromagnetism.

<sup>1819</sup> See [Human basophil degranulation triggered by very dilute antiserum against IgE](#), Jacques Benveniste et al, June 1988 (3 pages) and [Ma vérité sur la mémoire de l'eau](#) by Jacques Benveniste, 2005 (122 pages). The book contains a preface by the Nobel Prize winner Brian Josephson. In this book, published after his death in 2004, Jacques Benveniste recounts his experiences, his tumultuous relations with the medical mandarins over several decades, the story of the publication of his famous article in Nature in 1988 and other experiments conducted during the 1990s and early 2000s.

<sup>1820</sup> Raman spectrometry will be used in other experiments, much later from 2007, on various homeopathic strains.

<sup>1821</sup> At high dilutions, electrophoresis showed that there was no anti-IgG molecule left in the active ingredient.

<sup>1822</sup> Ironically, the process used does not prevent allergic reactions as is expected in homeopathy, which wants to treat evil with evil, but in low doses. Here the anti-IgE causes the production of histamine and does not prevent it.

However, he did investigate long-range electromagnetic fields, inspired by the work of Italian physicists specialized in quantum electrodynamics, **Giuliano Preparata** (1942-2000) and **Emilio Del Giudice** (1940-2014). In 1990, he set up an experiment with the CNRS Central Laboratory of Magnetism in Meudon, France, which showed that the activity of the diluted solution is modified by prolonged exposure to a magnetic field. The experiment used animal hearts with an electrical apparatus invented by **Oskar Langendorff** (1853-1908). In another experiment carried out over several years, he also uses an amplifier using a sound card from a microcomputer to transmit the properties of a solution to another neutral liquid. This leads to the concept of "digital biology"<sup>1823</sup>.

After the death of Jacques Benveniste in 2004, his work was taken over by **Luc Montagnier**, the originator of the first AIDS treatment who got the Nobel Prize in medicine in 2008. He described low frequency waves (7 Hz) that would be emitted by DNA strands. He set up an experiment in which the waves of DNA molecules are transmitted through a coil fed at 7 Hz to pure water in another test tube. A PCR is then used to regenerate the DNA in this test tube (DNA multiplication process, "polymerase chain reaction").

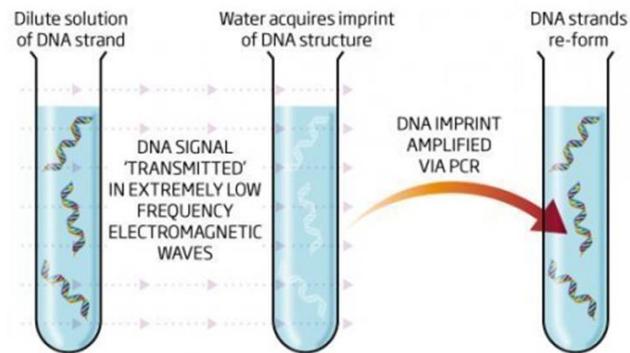
And gel electrophoresis is used to decode the replicated DNA! In the experiment, this DNA corresponds exactly to the original DNA. His code would have been transmitted by electromagnetic wave<sup>1824</sup>. But the documentation does not specify which DNA was used as a primer for PCR! Indeed, a PCR does not start from zero and a bunch of nucleotides, but uses DNA strands to replicate them<sup>1825</sup>.

The work of Luc Montagnier is related to that of the Italian **Emilio Del Giudice**, again, on the structure of liquid water<sup>1826</sup>.

#### What Montagnier claims

A weak electromagnetic field can form an imprint of a DNA strand in pure water, which can then be used to reconstruct the original DNA

©NewScientist



It will not surprise you to learn that this kind of discovery is rather controversial among specialists<sup>1827</sup>. And Luc Montagnier's publication was not made in a peer-reviewed journal. But he continues to publish, with international teams, on interesting research explaining by the quantum field theory how DNA polymerase works<sup>1828</sup>.

<sup>1823</sup> This story is well told in [L'âme des molécules, une histoire de la mémoire de l'eau](#) by Francis Beauvais, 2007 (626 pages). The author was one of Jacques Benveniste's experimenters.

<sup>1824</sup> See explanations in Luc Montagnier's article [DNA waves and water](#), January 2010 (10 pages). [Montagnier and the quantum teleportation of DNA](#) by Vincent Verschoore, January 2011, is the source of the illustration.

<sup>1825</sup> This PCR problem is noted in [The Nobel disease meets DNA teleportation and homeopathy](#), January 2011.

<sup>1826</sup> See Mae-Wan Ho's [Illuminating Water and Life](#), 2014 (18 pages) which describes the theories of Emilio Del Giudice, who died that same year.

<sup>1827</sup> See [Luc Montagnier and the Nobel Disease](#) by David Gorski, June 2012.

<sup>1828</sup> See [Water Bridging Dynamics of Polymerase Chain Reaction in the Gauge Theory Paradigm of Quantum Fields](#) by Luc Montagnier et al, 2018 (18 pages).

The relationship between water and quantum physics is being emulated by others and drove the creation of many scams selling structured water and the likes<sup>1829</sup>.

**Konstantin Korotkov** (Russia) did some experiments supposed to show that projecting negative emotions on water reduced its energy level and vice versa<sup>1830</sup>. This guy created IUMAB (International Union of Medical and Applied Bioelectrography), an organization that promotes the use of bioelectrography devices<sup>1831</sup>. He is promoting DGV Bio Well cameras, aura detection systems around patients that would materialize the chakras, via the analysis of the "gas discharge".



We then have **Mazaru Emoto's MRA** (Magnetic Resonance Analyzer) (1943-2014). He conducted experiments analyzing the impact of emotions on the structure of water. Experiments that were never reproduced independently<sup>1832</sup>. You probably guessed it!

OK, emotions can generate infrared waves and gases that can be exhaled, producing in turn a minute reaction on exposed water<sup>1833</sup>. This makes it possible to sell a concentrated structured water that can be used to prepare distilled water, **Indigo Water** ([opposite](#), [source](#)). Here is the description: "*A geometrically perfect water with the "Message" your body is waiting to receive. Dr. Emoto's Indigo Water contains eight ounces of highly charged hexagonally structured concentrate. By mixing one ounce of concentrate with one gallon of distilled water, you are creating eight gallons of structured water from this 8 ounce Indigo water. This is about a one month supply of structured water*". For \$35. By the way, it doesn't mention if it's drinking water or shower water!



The delirium continues with the structured water of **Rustum Roy** (American). Structured water is said to be an antibiotic: "*One molecule of structured water in 100 million molecules of drinking water can destroy all germs present in a wound. The American army has used this water in Iraq and Afghanistan. Obama uses structured water to wash his hands*". Verification made, the only example

<sup>1829</sup> See [Hypotheses quantum of mechanism of action of high homeopathic dilutions](#), is a doctoral thesis by Mathieu Palluel, 2017 (252 pages). Its first part is a fairly well-supplied history of homeopathy. It also covers the experiences of Jacques Benveniste and Luc Montagnier. The quantum part starts on page 181 and is quite weak. This PhD student was definitely not a physicist. He makes a countersense on Schrödinger's equation on page 189. He uses quantum field theory and quantum electrodynamics in a weird context, water at room temperature. On page 201, the paper states that water molecules have a diameter of approximately 3 nm while it is 0.27 nm. It also talks on page 221 about the Nobel Prize of "Serge Laroche" instead of Serge Haroche. In short, this thesis document was poorly reviewed by the people who validated it, and who were not at all up to date in quantum physics.

<sup>1830</sup> See [The First Korotkov Intention Experiment](#) by Konstantin Korotkov, January 2018 as well as [The Intention Experiment on H2O](#), 2007 (18 pages) which reproduced his experiments in the USA.

<sup>1831</sup> He is also the author of [The Emerging Science of Water: Water Science in the XXIst Century](#) by Vladimir Voeikov and Konstantin Korotkov, 2018 (253 pages), a work or current of thought that certainly influenced Marc Henry's work, unless the opposite is true.

<sup>1832</sup> This is well explained in [The pseudoscience of creating beautiful \(or ugly\) water](#) by William Reville, 2011. See also the site [Structure-altered water nonsense](#) which makes a good inventory of commercial offers of structure water in the USA. The 1995 style layout serves the site but the inventory of solutions is edifying. Mazaru Emoto also certified an effect of exposing zam zam water that is produced at Mecca to Quran. The water is supposed to have similar miraculous effects, a bit like Lourdes' water in France.

<sup>1833</sup> See [The experiments of Masaru Emoto with emotional imprinting of water](#), 2018 (11 pages).

that can be found is the healing of a foot wound and it's water associated with money<sup>1834</sup>. And how can we restructure water, so to speak? Simple: by heating it, with vortexes, magnetic fields, music, the force of thought, "frequencies" or minerals!

The concept of wormholes comes from the astronomer **Nicolaï Kosyrev** (1905-1983) who discovered lunar volcanism and the biologist **Rupert Sheldrake** (1942), who became an expert in telepathy. This led to **Vodaflor**'s Voda vortexors which generate vortexes in water to structure it with models ranging from 936€ to 3300€ depending on the desired water structuring rate.

More recently, the discourse around the benefits of water in homeopathy was renewed with the integration of quantum electrodynamics as an explanatory feature. Why not, since almost nobody can understand anything about it, except the few physicists in this domain<sup>1835</sup>. Not to mention the lack of experimental protocols to verify anything. Again, we are confronting a fake science because it cannot be refuted<sup>1836</sup>!

To conclude this part before moving on to the most beautiful scams of pseudo-quantum medicine, let us recall that there is a fine line between low-level science and its high-level interpretation, especially when it is then exploited by unscrupulous entrepreneurs.

And we're not done finding more of the same such as some weird quantum behavior of water in carbon nanotubes<sup>1837</sup>, superconductivity in the brain<sup>1838</sup> or other elucubrations on quantum cognition<sup>1839</sup>. This will undoubtedly fuel new waves of [quantum mysticism](#)!

## Quantum medicine

As [Wikipedia's quantum healing page](#) on quantum medicine points out, this discipline misuses the jargon of quantum physics to make people believe in magical cures for certain pathologies that traditional medicine, well or badly practiced, cannot treat properly<sup>1840</sup>. The phenomenon is already over a decade old.

### Method for detecting false science

The methods used to promote false quantum science in health (and in general for that matter) are easily detectable to an educated person, or just with some common sense:

- It startups with some **scientific statement** associating very quickly humanities and biology and making approximate shortcuts on quantum physics.
- The solutions are being promoted with some **esoteric jargon** using unprecise terms like wave, matter, vibration, vortex and energy<sup>1841</sup>.

---

<sup>1834</sup> In [Ultradilute Ag-Aquasols with extraordinary bactericidal properties : the role of the system Ag-O-H2O](#), 2006 (13 pages). Rustum Roy is also the author of [The Structure Of Liquid Water; Novel Insights From Materials Research; Potential Relevance To Homeopathy](#) by Rustum Roy, 2009 (33 pages).

<sup>1835</sup> See [Explaining Homeopathy With Quantum Electrodynamics](#) by Antonio Manzalini and Bruno Galeazzi, 2018.

<sup>1836</sup> Fortunately, some scientists address this nonsense, such as [L'homéopathie confrontée à la physique](#) by Alain Bonnier, 2014 (34 pages), which dismantles homeopathy in a very didactic way, relying in particular on Planck's constant.

<sup>1837</sup> See [Evidence of a new quantum state of nano-confined water](#) by G. F. Reiter et al, 2011 (5 pages).

<sup>1838</sup> See [Possible superconductivity in brain](#) by P. Mikheenko, 2018 (10 pages).

<sup>1839</sup> See [What is quantum cognition? Physics theory could predict human behavior](#) by Nicoletta Lanese, January 2020.

<sup>1840</sup> These methods are also well described in Richard Monvoisin's [Quantox - Ideological Misuses of Quantum Mechanics](#), published in 2013 (in French).

<sup>1841</sup> You find a marvelous example with the [Quantum Field Medicine](#) web site that consolidates all these fancy alternative quantum medicines, mostly all based on placebo effect. You have consciousness awareness techniques, acupuncture, homeopathy, electromagnetic resonance, Timewaver (another electrical product scam), color and light therapy and sound/music therapy.

- When they exist, **tests are performed with small samples** that are not statistically representative. The arguments are often based on non-verifiable anecdotes. The miraculous healings observed in Lourdes, France, are even better documented and, moreover, as probable as those occurring in the hospital environment ([source](#)), i.e. between 1/350,000 and 1/100,000 cases.
- Many specialists sell various, rather expensive, **healing materials or devices**, not considered as medical devices, and whose effectiveness is clearly related to the placebo effect.
- These solution's marketing target **vulnerable people** (sick, elderly, etc.). It can be seen in the media used for advertising it.
- The **vague side of the pathologies covered**. Some are related to pain management or to what can be treated by placebo effect, such as psychonomy<sup>1842</sup>. Others target all the major pathologies of the moment: chronic diseases, cancers and in some cases even neurodegenerative diseases.
- **Extended resumes** with impressive diplomas and scientific guarantees to be taken with tweezers for many quantum medicine specialists. There are even "diploma mills" in the USA, where you can buy a doctorate in medicine or another junk discipline at a reasonable price. A bit like in the late Trump University.
- Rare **scientific publications** and when they exist, just as rarely carried out in peer-reviewed journals, knowing that this validation is already not enough to be a guarantee of seriousness. These therefore become "private" publications.
- Some **conspiracy theories** about the pharmaceutical companies lobbying and other healthcare professionals who will do anything to prevent alternative solutions from emerging.

Nonetheless, there are positive comments from readers of these books that show that the market for gogos is a thriving one. It takes place in a context of loss of confidence in politics, media and science and the development of many conspiracy theories, fueled by the fluidity of the Internet and social networks.

## Quantum medicine marketing

Let's review some of the reference books that promote this curious quantum medicine.

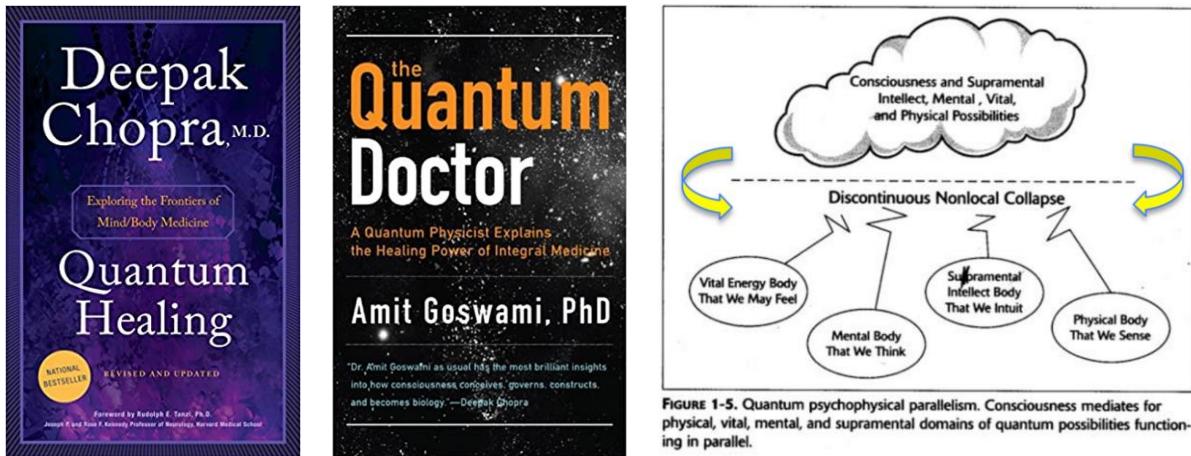
**Quantum Healing** by Deepak Chopra (1988) seems to be foundational. It comes from a former endocrinologist. He became an Ayurvedic practitioner, coming from traditional Indian medicine. According to him, quantum thinking explains some cases of psychosomatic healings that resemble self-healing. The author is a star in the field, especially in India and the USA, with a total prose sales of over 10 million copies and a personal fortune estimated at over \$80M ([source](#)). The content of his works is of course quite weak scientific speaking, especially when he deals with quantum physics, mostly in metaphorical terms<sup>1843</sup>.

---

<sup>1842</sup> Which is yet another false science associating mind and body.

<sup>1843</sup> On this subject, I watched the enlightening debate between [Deepak Chopra and Richard Dawkins](#) (Mexico, 2013, 1h13) which highlights the difficulty of reconciling Chopra's emotional and symbolic approach with Dawkins' rationalist and scientific approach. At one point, the debate focuses on the supposed Universe intelligence that exists according to Chopra and at all levels, from elementary particles to the entire Universe. While this makes no sense to Dawkins beyond biological beings with brains, or computers imitating them. It is a homothetic debate with the link between consciousness and the pathologies that consciousness would or would not necessarily control. The other interesting part of this debate concerns the notion of quantum leap on the appearance of language or certain biological evolutions that are a view of the mind for Richard Dawkins. The latter even denounces Chopra's "deliberate obscurantism". For Richard Dawkins, consciousness is explained or will be explained by neuroscience and certainly not by Deepak Chopra's meta-consciousness galimatias.

Amit Goswami's **The Quantum Doctor** (2004) is along the lines of Deepak Chopra's theories. The author is an Indo-American physics teacher who practiced in Oregon between 1968 and 1997, but in nuclear physics. He defines himself as a quantum activist who even has his own Quantum University which seems to be to healthcare what Trump University was to business schools. According to him, quantum activism through consciousness can save civilization. He also demonstrates scientifically (!) the existence of God by building upon Deepak Chopra's consciousness of the Universe thesis. In his work, he explains the therapeutic effectiveness of "integral medicine" which combines allopathic medicine and more or less soft, alternative and traditional medicines, particularly Indian and Chinese.



The scientific content of the book fits on a tiny postage stamp. It looks even like a giant quantum joke. The idea is the following: your organs are born in good health. A time passes, like a qubit would become after a Hadamard gate, it becomes superposed in good and bad health. Then, with the strength of your consciousness, you could provoke a quantum wave function collapse of your organs into the health version. That simple! It's a scam version of this poor Schrödinger's cat.

The work also seeks to explain the effects and precepts of oriental medicines (chakras, reincarnation, ayurvedic medicine, acupuncture)<sup>1844</sup>. Here are a few selected excepts with the "*morphogenetic fields of the vital body*", "*when the mind creates the disease, sometimes healing is impossible to achieve on the mind level. One must then make a quantum leap to the supralental to heal*" or "*quantum collapse is also fundamentally non-local. Therefore, the non-locality of healing, as in healing through prayer, finds a clear explanation within the framework of quantum thinking*". With quantum entanglement, one can relate everything to everything and explain everything.

Amit Goswami mentions distant healings through prayer by referring to an experiment by physicist **Randolph Byrd** in 1988. The statistical representation was very weak with 6 healings out of 26 patients of not well specified cardiac pathologies. It may not surprise you to find out that it was demonstrated that prayers did not have any large-scale effects<sup>1845</sup>.

He also quotes the telepathy experiment of **Jacobo Grinberg-Zylberbaum** (Mexico)<sup>1846</sup>. It involved measuring EEG waves on a participant to assess the impact on him of a flash of light arriving on one of the participants, both of whom were in Faraday cages. The experiment was repeated later between 2000 and 2004 using MRI<sup>1847</sup>.

<sup>1844</sup> Illustration source: [Messengers and Messages-then, now, and yet to come](#) (15 pages).

<sup>1845</sup> See [Studies on intercessory prayer](#), Wikipedia.

<sup>1846</sup> Documented in [The Einstein-Podolsky-Rosen Paradox in the Brain: The Transferred Potential](#), 1994 (7 pages).

<sup>1847</sup> See [details](#) and [results](#).

A small technical detail: there cannot be any radio waves transmission between the participants who are in Faraday cages, no photon either, nor particles with a common history in the brain of the participants.

Others have a slightly more scientific view of the quantum nature of consciousness, such as **Ervin Laszlo**, even if the latter relies a bit too much on quantum entanglement in his explanations<sup>1848</sup>.

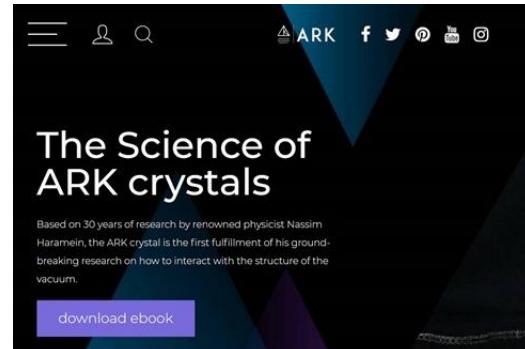
Other pseudo-scientists promote fancy theories related to the so-called quantum medicine.

**James Oschman** (USA) promotes a concept of life energy, based on electric currents and water related quantum phenomenon. He invented the concept of perineuronal brain cells, which are obviously only the glial cells that surround neurons, but with a different name and which generate energy that goes to the hands<sup>1849</sup>.

**Kiran Schmidt** is a German who does "information medicine". He also promotes strange machines that are supposed to cure everything, especially under the brand **Inergetix CoRe**.

**Nassim Haramein** deals with the energy of creation and also water memory. He is selling fancy products through his [Resonance Science Foundation](#). The starting point? Some work on his unified field theory, an old Holy Grail of fundamental physics<sup>1850</sup>. This scientist thinks he has discovered an [infinite source of energy](#). Of course, none of the work of this "scientist" was validated [by his peers](#).

This guru markets [ARK crystals](#), which are magical crystals that heal or improve the performance of athletes. They even publish a [study](#) on how to improve athletes performance. It used a double-blind method with a placebo effect for half of the test subjects. Given the study involved only 10 athletes, 5 men and 5 women, with progress of about 10%, thus within the margin of error of the sample. The study was done by the [Energy Medicine Research Institute](#) laboratory, versed in studies of fancy products such as LifeWave placebos marketed in a Tupperware-style pyramidal model.



These crystals would also help accelerate plant growth! Prices range from 277€ to 1850€. This is part of a trend in the sale of magic crystals that dates from a few years ago and where the offer is plethoric<sup>1851</sup>.

<sup>1848</sup> In [Why Your Brain Is A Quantum Computer](#), 2010. This thesis is partly deconstructed in [The Myth of Quantum Consciousness](#), 2002 (19 pages), although it is an earlier work.

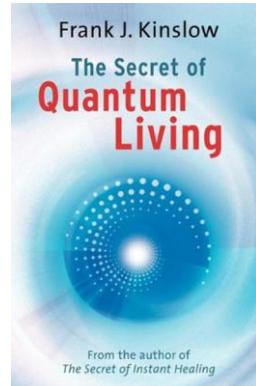
<sup>1849</sup> He is the author of [Energy Medicine](#), James L. Oschman, 2000.

<sup>1850</sup> His list of [scientific publications](#) deals with neutrons and protons. A part of the articles have been published in the journal [Neuro Quantology](#) which is not considered as being serious and whose review committee does not include any scientist in quantum physics or neuroscience. This publication process is known and exists in other fields such as medicine.

<sup>1851</sup> See [Dark crystals: the brutal reality behind a booming wellness craze](#) by Tess McClure dans The Guardian, September 2019, [A Cynic's Search for the Truth About Healing Crystals](#) by Katherine Gillespie in Vice, September 2017 and [The Sickening Business of Wellness](#) by Yvette d'Entremont, December 2016.

Frank J. Kinslow's **The Secret of Quantum Healing** (2011) introduces the notion of "Quantum Training", a "scientific, fast and effective method that reduces pain and promotes healing". In a few words, it is about having your consciousness send vibratory waves to your organs to heal them. By the play of interferences, they will cancel the evil.

Another Schrödinger's cat trick with the application of the quantum mechanics of the pico (elementary particles) to the macro (the organs). It is mainly aimed at physical and emotional pain. It is a variant of meditation. It should be avoided for the treatment of hypothyroidism or about anything else by the way!



This kind of work has the particularity of always being very vague on the notion of pathology treated, especially if a pseudo-medical apparatus is involved, as is the case here. Even if the "Quantum Training" is supposed to work remotely.

**Quantum Intronic Medicine** from Christian Daniel Assoun deals with quantum biology. It is a form of epigenetic treatise describing DNA memory by quantum mechanics. According to him, "*WATER is the first quantum liquid: its current state is liquid whereas its state should be gaseous*". This book describes the presence of a third DNA catenary in the form of physical plasma (hydrogen)<sup>1852</sup>. He states that his "*work is currently focused on the INTRONIC parts which represent 95% of our DNA and which are unfairly classified as silent or even useless*". Intronic is used in the sense of DNA "introns", the part of DNA genes that is transcribed into RNA when the genes are expressed.



These are eliminated during splicing which generates mature RNA that will then be used in the ribosomes to make proteins. In fact, introns represent only 25% of human DNA. The rest, about 73%, corresponds to sequences that are effectively non-coding in the DNA of our chromosomes, but whose role in the regulation of genes is progressively revealed with research. Exons, the coding part of genes, represent 1.5% of human DNA ([source](#)).

Christian Daniel Assoun believes that DNA could be strengthened with "the help of new tetravalent elements such as Germanium or Silicon (reverse optoquantic properties)". Why Germanium and Silicon? Because they are in the same column of Mendeleev's table as carbon with four free electrons. This is a good idea for creating extraterrestrial life. So why didn't life on Earth use silicon, which is as abundant as carbon? One of the reasons is that silicon oxide ( $\text{SiO}_2$ ) is inert and solid while carbon oxides ( $\text{CO}$ ,  $\text{CO}_2$ ) are gaseous and therefore more easily recombinable with other atoms and molecules. Finally, carbon is more abundant than silicon on the surface of the Earth.

Christian Daniel Assoun is also the founder of the **Glycan Group**, in 1996, a company selling organic silicon for various uses and notably as a [food supplement](#). Their subsidiary Glycan Pharma was struck off the commercial register in 2012. The company is in competition with [Silicium España](#), a company linked to Loic Le Ribault, who died in 2007, who was also passionate about organic silicon. The two companies had a legal dispute in 2011 over the use of the G5 trademark.

At last, you also can count on the many books on Transurfing by **Vadim Zeland** who introduces himself as a physicist. This quantum model of personal development is based on the idea that "*When the parameters of mental energy change, the organism moves to another lifeline. When the parameters of mental energy change, the organism moves towards another life line*". So be it!

<sup>1852</sup> Ebook [downloadable here](#). It is also documented in [The 3rd Strand \(or 3rd Catenary\) of DNA](#) by the same author and which dates from 2011/2012.

## Scalar wave generators

The best of the quantum medicine scams are the **scalar wave generators**. These are electromagnetic waves associating a supposedly horizontally polarized electro-magnetic wave and another vertically polarized wave of the same frequency but 90° or a quarter wavelength out of phase.

Scalar waves were initially promoted by a certain **Thomas Bearden** in the USA as well as by the Russian **Sergei Koltsov** with his Functional State Correctors (CEF<sup>1853</sup>). Bearden explains this in a [1991 interview](#). He had also invented a **MEG** (Motionless Electromagnetic Generator) capable of extracting free energy from the vacuum and thus, of generating more energy than it consumed. A product that has of course never been commercialized.

Scalar waves were also promoted by a German scientist, **Konstantin Meyl**, with a paper that had to later be retracted<sup>1854</sup>. The general public propaganda on scalar waves is a big fantasy and always linked to alternative medicine literature. These waves would come from the Sun with neutrinos and have no energy loss over distance. The brain is supposed to produce and sense scalar waves with its own interferometer. It would explain telepathy and other paranormal effects. Well well.

Scalar waves would also make it possible to treat diabetes (I or II? Who cares...), kidney stones, Parkinson's disease, heart attacks, osteoarthritis, cancer and also aging. As for type I diabetes, which is linked to the autoimmune destruction of beta cells of the islets of Langherans in the pancreas, it is not clear how waves of any kind would bring dead cells back to life. The proposed solution?

Scalar wave generators such as the **INDEL** at 8820€. Given its price, it targets professionals in a kind of Ponzi model. This generator produces a scalar wave field with a voltage of 2V. It also includes a music modulation accessory for therapy practices and wellness centers. It is also available at **QuWave**.



You can also (not safely) rely on the **ETHX-SCIO Biofeedback** from William Nelson, which combines global therapies and advanced quantum physics (*above*). The device scans the body on 10,400 different frequencies to detect many pathologies. It then rebalances the body's energy with quantum biofeedback. The toy also runs 200 biofeedback therapies with the world's largest health software that integrates Western and Eastern philosophies<sup>1855</sup>. The EPFX-SCIO includes a wave diffuser box, connected to the patient with sensors attached to his ankles, wrists and skull. One could almost do both an EEG and an ECG with it! All this for getting some placebo!



In the scam devices category, you also find the **Healy** and its bioresonance features using some electrodes and supposed to cure many illnesses<sup>1856</sup>. At best, it can be a temporary pain killer. Another device, the **TimeWaver**, is based on “quantum field theory” from a certain Burkhard Heim (1925

<sup>1853</sup> Watch this video [Functional State Correctors \(FCS\) - Koltsov Plates](#), 2014 (55 minutes) which is a good digest of any scientific theory.

<sup>1854</sup> See [“Way out there” paper claiming to merge physics and biology retracted](#), RetractedWatch 2013 and [Scalar Wave Transponder device](#) by Konstantin Meyl, 2005 (70 pages).

<sup>1855</sup> See [How one man's invention is part of a growing worldwide scam that snares the desperate ill.](#)

<sup>1856</sup> See [A Skeptical Look at the Healy “Bioresonance” Device](#) by Stephen Barrett, July 2020.

-2001, German) on the 12-dimensional composition of the universe where “*the light quantum effect communicates mainly with the Global Information field (GIF) i.e. at a nonenergetic, non-phenomenal and therefore more causative level*”. It looks like a biofeedback device similar to the one above. Burkhard Heim did try to unify all quantum theories but he was neither a Dirac or a Feynman<sup>1857</sup>! The TimeWaver site also mentions of **Kozyrev mirrors** using cylindrical aluminium sheets that were used for extrasensory perception experiments in Russia. But it doesn’t seem to be involved in the TimeWaver device.

Other various Russian ‘quantum’ scientists, dead or alive, are frequently used in support of these scam devices like Nikolai Kozyrev, Vlail Kaznacheev or Alexander Trofimov. When you look at their biographies online, you quickly find that they were not at all mainstream quantum scientists. This is all full of esoterism, not science.

## Quantum medallions

Quantum medallions for smartphones have become commonplace for several years and target another phobia, electromagnetic waves and 5G. This is the case of **Quantum Science**’s Quantum Shield medallions (on [Amazon](#) and [Alibaba](#)). One also finds some in the form of USB keys **5G BioShield** which contain a “*quantum holographic catalyst*”.



It is obviously a huge quantum bullshit of the first kind. It is accompanied by a scientific justification that is not worth a lot of money<sup>1858</sup>. The American FTC has flagged these products as vulgar scams<sup>1859</sup>.

In the field of wacky quantum devices, let’s finish with the **Quantum 5 Ozone Generator** using Neos Technology from the **Longevity Resources** ([sources](#)). It uses a quartz electrode. It’s supposed to help purify indoor air. There is one major drawback: ozone can also be toxic to the human body and cause respiratory problems. It can also affect plants health.



In short, quantum medicine may one day emerge in the wake of scientific discoveries, but the ones proposed today is for the time being full blown charlatanism. They have the advantage of generating at least a placebo effect for users and filling the wallets of their promoters. Except that this can be dangerous if the placebo effect is used instead of a traditional treatment that is essential to stay alive.

I will not, however, trash all the techniques and approaches mentioned here. Some may make sense, even though there is still a lack of both a scientific corpus and more solid evidence to support them. But most are fake sciences and are quite easily detectable.

<sup>1857</sup> See [TimeWaver System](#) website. They hopefully have a: « *Disclaimer: Science and conventional medicine does not acknowledge the existence of information fields their medical and other important TimeWaver systems and their applications due to lack of scientific evidence. The said application is based on, treatment options, experiences and anecdotal reports from the practice*”.

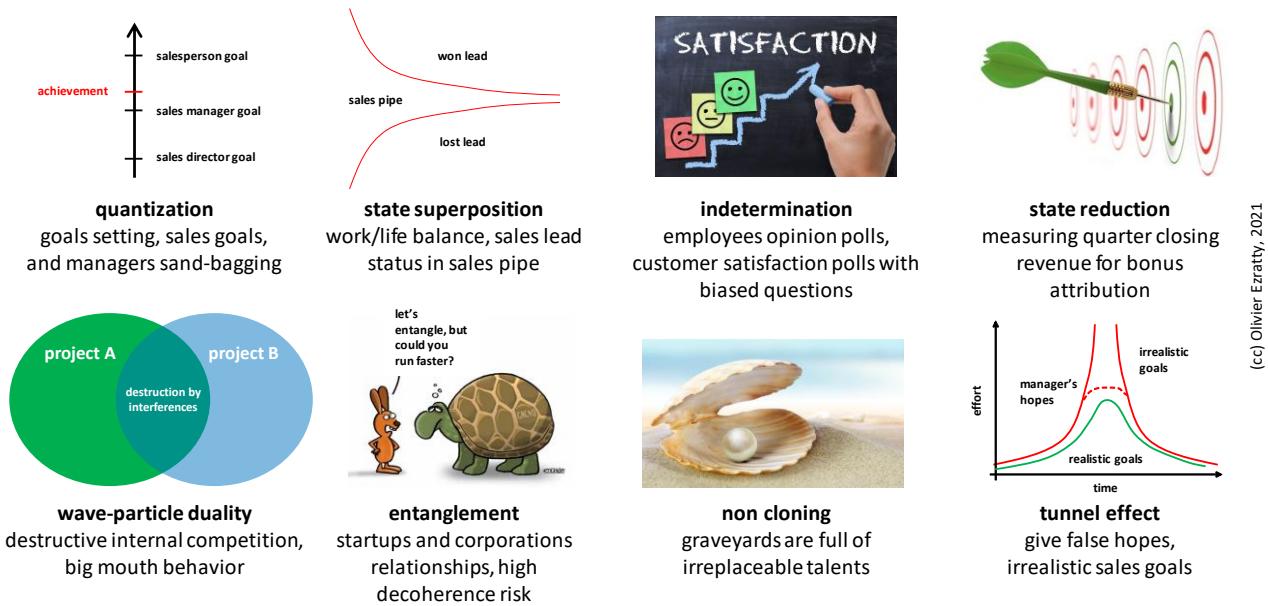
<sup>1858</sup> See ["Aton" True Cell, Atom and Particle Concept](#) by Ilija Lakicevic, 2019 (8 pages).

<sup>1859</sup> See [Cell Phone Radiation Scams](#), 2011.

# Quantum management

Quantum management is a new and fashionable practice that seeks to draw inspiration from the general principles of quantum mechanics. Its practitioners are frequently followers of more or less occult sciences who have converted to target corporate markets that are more financially attractive than consumer markets. The vulnerability of educated executives and managers to the most outlandish proposals is always amazing.

However, we can indeed identify many analogies between quantum physics and management in the broadest sense of the term. For this purpose, I have pushed the enveloped and reused advanced quantum physics fundamentals and applied it to your usual business life. Any resemblance with a real-life situation would be totally fortuitous or entirely intentional, as you will guess.



**Quantization** means that certain physical values can only be very precise, discontinuous and not arbitrary, like the energy levels of a hydrogen atom. After all, an employee is just a cell in a spreadsheet. He's there one day and gone the next. Workforce management is indeed quantum. A company's workforce at a given time is a discrete integer number.

But if we average it over a period of time, taking into account departures during the period, part-time employees, fixed-term contracts, apprenticeships, subcontractors and people whose real activity we are not sure of, it is no longer an integer but a number of FTEs (full time employees) or FTEs (full time equivalents) that is at least a sum of fractions. Fortunately, it is never a complex number and one escapes Hilbert's spaces to represent them.

Quantization also manifests itself with sand bagging, when a sales manager is distributing his own sales goals to his team by adding a quantum margin of safety. The last link in the chain, the unfortunate poor salesperson, will be assigned a goal that is greater than that of all the layers of management above. Only certain layers of sales management have this flexibility. The end result is that salespersons become Rydberg state atoms: they are excited with a very high level of energy and they sometimes burn out. This system is designed so that the base salesperson does not reach his or her objective and is penalized on the bonus side, unlike managers above him or her. Particularly if you want to fire him or her. Judgment about individuals is also subject to quantization. A person is often smart or nice, or a total moron. Personal judgments are rarely nuanced in grey. Yet, in a purist application of quantum physics, this kind of judgment should be a more vague and subtle wave function, until you measure it during a stressful experience.

The top of quantization? Those nasty Internet popups where the given choice is "OK" or "Later". For the quantum measurement guru, it's a real-life example of an exaggerated POVM (see Glossary).

**Superposition** is very common in business. For example, thanks to smartphones and other laptops, employees are kept both at work and in their personal lives all day long. It can also manifest itself in regulatory compliance, which is variable geometry in many companies. And then, of course, in the application of the company values defined in Powerpoint slides and rehashed by managers or the HR department. States superposition also manifests itself in the evaluation of leads that are closed or not in a sales pipeline. They are usually assigned a closing rate which is an amplitude and phase  $|\psi\rangle$  until it is known whether the deal is lost or won, which is like the wave-packet collapse happening with quantum measurement, on a basis state  $|0\rangle$  or  $|1\rangle$ . This collapse also occurs if an external event creates a lead quantum state decoherence. For example, a competitor who wins the deal under the nose of the salesman. This quantum analogy, however, will not help you improve your sales pipe closing rate.

**Indeterminacy** works with the measurement of employee satisfaction, where the measuring tool always influences the quantity to be measured. This is true as well in the questions asked in opinion polls, which are often oriented. More generally, the measurement of any parameter in a company by a consulting firm like McKinsey, particularly during an audit, will probably lead to changes in the measured quantities (e.g., downsizing, management change, reorganization and the likes). You just hope that your enterprise won't become a planar wave afterwards.

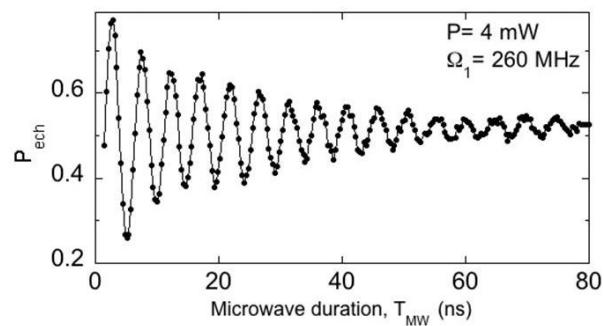
One variation of Heisenberg's principle of indeterminacy is that one cannot accurately measure both the position and velocity of a particle. The analogy in business would be the observation of a growing startup: by the time one understands where it is at a given moment, it has already changed its situation (headquarters, staff, CEO, turnover, M&A, company name, product, done a pivot). This is why it takes an infinite amount of energy to create an up-to-date startup base in one country or worldwide, even with only quantum technologies startups. So, thank you Crunchbase for the effort!

**Measurement** is in line with the history of quantization when measuring revenue at the end of a fiscal quarter. In this case, one is obliged to provide numbers and not to rely on some closing rates fuzzy logic. If only to determine the bonuses of sales representatives. Otherwise, Bill Gates said loud and clear in 1997 that "*bad news should travel fast in efficient companies*". But not too fast my dear, otherwise you'll get fired. That's what is called a non self-destructive measurement.

**Wave-particle duality** manifests itself with real people in companies who work on competing projects and happily annihilate each other. It is the phenomenon of interference linked to the waveform aspect of each and every projects! You also have the loudmouthed managers facing their teams (thus, in the state of a solid particles) who turn into wipes in front of their own management (thus, in the state of very low-energy waves).

This behavioral duality is also often observed with irascible managers who become docile sheep once at home, or who fail to properly educate their children. Can a trendy startup Chief Happiness Officer be quantum? In any case, he has to fight against a universal phenomenon: a good number of passions quickly fade with time, such as the amplitude of a Rabi oscillation, which is commonly observed in quantum physics (*opposite*).

The Doppler effect also allows to indirectly put an end to a messed-up project with light, for example, via a well-managed leak in the media. Remember Theranos?

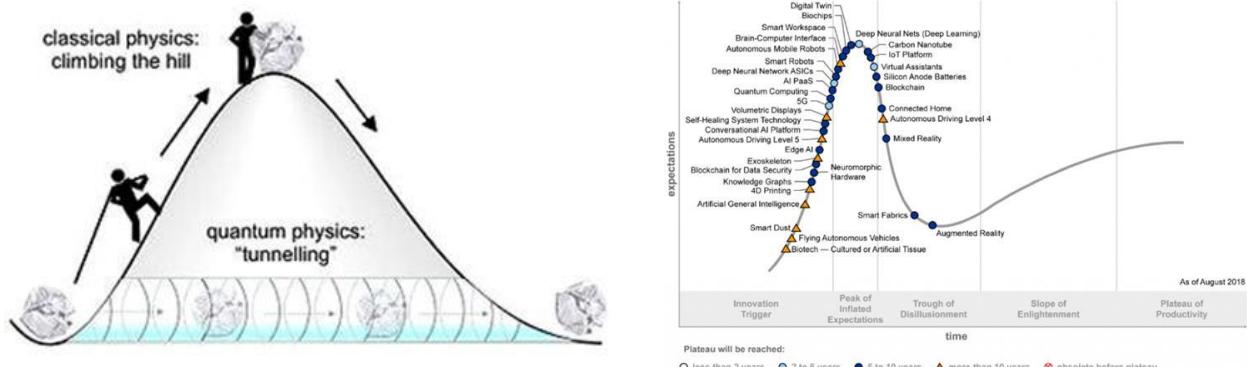


**Entanglement** applies to startups that are integrated into the open innovation programs of large companies. Everything goes well until the appearance of decoherence between the startup and the corporation! I create a product and you want a customized solution, I need speed and you're too slow, etc!

Entanglement also occurs with the teleportation of rumors faster than light. It is also known that the coherence time of qubits is linked to their good physical, magnetic and vacuum insulation, often at very low temperature, in order to avoid any external disturbance. This is the opposite of the open spaces in companies where employees are crammed together! It has long been claimed that open spaces improve teamwork, whereas their main purpose is to compress real estate costs!

**Non-Cloning Theorem** says that it is impossible to identically clone the state of a qubit or quantum, has an application in business life with all those people who are believed to be irreplaceable until the day they leave or die. The theorem applies in particular when the departing manager is not replaced and whose role is then distributed among several existing managers, a bit like a quantum error correction with ancilla qubits and projective measurements. The theorem also works with successful entrepreneurs who find it difficult to replicate a success from one area to another.

**Tunnel effect** makes it possible to implement change management. It consists in presenting a wonderful future situation and making people forget the difficulties to get there. The principle could also be adopted by the Gartner Group with its famous innovation adoption cycle curves ("hype cycle"), as some technologies do not necessarily pass through the valley of death, as was the case for smartphones. It had benefited from the reality distortion field of a certain Steve Jobs, a great adept of quantum management principles. By the way, the trajectory Apple-Next-Apple was a great application of the tunnel effect, Next being a relative failure while both Apple were successes.



**Superconductivity** is linked to meeting rooms. Employees and managers are conditioned to be even-spin bozos, who can be assembled in meeting rooms or covid-zooms. Organizational superconductivity also avoids resistance to change. You freeze employees and their resistance to change disappears. Which is a bit paradoxical because once frozen, you are as solid as a rock, and defrosting is not obvious. If we take the principles of Deepak Chopra's quantum pseudo-medicine, a company is in a superposed state between a healthy leader and a declining star. The strength of leadership should theoretically allow the wave packet function of the company's quantum state to collapse in the healthy leader state. In real life, this collapse is tricky to achieve and companies simply collapse. The processes that lead the company to find itself in a declining situation are most often irreversible and linked to a slow decoherence with the environment, competitors and customers who have not waited to adapt. Corporate life is not a reversible quantum gate nor any sort of linear algebra. It's mostly nonlinear. Try, for example, to turn Nokia into the leader of Android smartphones!

**Universal Gates Quantum Computing** has a beautiful analogy in the life of companies with the management of calls for tenders such as those for communication agencies. The responses of candidate agencies are superposed states of a quantum register.

They undergo a simultaneous evaluation process, as in an oracle-based quantum algorithm. In the end, only one offer emerges: the winner. But during this process, there may be some quantum entanglement affecting the winner final proposal. Translation: the elements of certain answers will magically appear in the winner's answer. Again, perhaps via the enterprise quantum tunnel effect.

Finally, let us mention this other universal principle, the very famous **quantum teleportation** of human stupidity to large sections of the company or in the population. It uses superdense falsehoods encoding. And contrarily to actual teleportation, it travels faster than light. It is so fast that it is the only plausible explanation.

All of these analogies are amusing but not very useful for improving management. Even if its scientific dimension is more than questionable, parody is finally an interesting form of pedagogy!

## Other exaggerations

There are many startups or ventures surfing on the quantum technology wave with various intentions. Some are just quantum startups with fluffy claims and others have only quantum in their name but nothing else.



**Dark Star Quantum Lab** (2020, USA) introduces itself as a contract defense and space research company covering applied quantum physics and quantum information science (QIS). They develop tons of quantum stuff: quantum software and quantum emulation solutions, unspecified hardware, a 'Sentinel' mobile phone including a QRNG.

They also claim to have developed a Qloud high-frequency trading, a Qoin (quantum-secured cryptocurrency), a BloQchain (quantum-secured blockchain working with Qoin), a use-case of Nash embedding to create error-free qubits and, also, some Star Trek Tricorder fancy stuff. This laundry list of things is not credible. And they don't seem to have any real defense customer. Looks like it's not really [serious](#).

Also quite weird is this **Quantum\_AI Group Of Companies** with its 15 branches dealing with aerospace, artificial intelligence, naval, finance, energy, automotive, electronics and... quantum computing. They develop, take it or leave it: Nano-Flux, a range of flux-qubits superconducting computers, Q-optic, the most powerful optical qubits quantum computer, BEC, the fastest Bose-Einstein condensate based trapped ions computer (seems they mixed some things here) and also SSL, a solid-state quantum computer and Infinity-Q a high-performance heavy load quantum computer. Interestingly, these 4 ranges of systems have respectively 40, 200, a 1.6 and 128 billion qubits and they look the same in their 3D rendered pictures.

They are supposed to be based in Stanford, Boston, India, Abu Dhabi, Dublin and Tel Aviv. They still have a CEO, a certain Ranobijoy Bhattacharya. If it's not an April's fool, what is it? Some new form of mythomania?

Quantum physics abuse can be found in various other product categories. In China, for example, a so-called **quantum satellite camera** was used to produce high-resolution panoramas. The view presented is that of Shanghai with 195 billion pixels.

Practically, the pictures were captured from the top of a skyscraper - there is no shortage of them in Shanghai - and not by any satellite. It used conventional high-resolution cameras that have nothing more quantum than the very classic photoelectric effect used in CMOS sensors to transform photons into electric current. The information is totally bogus and was only used to generate buzz.

**SATELLITE  
PHOTO  
CAPTURED BY  
24.9 BILLION  
PIXELS OF  
QUANTUM  
TECHNOLOGY**



Unfortunately, many media outlets around the world have taken the bait without any doubt<sup>1860</sup>.

For its part, a French SME **What-Innove** from the East of France, specialized in renewable energies, claims it is creating an engine that captures energy from vacuum. How does it work? An unlikely mix combining a quantum field generator, the creation of photons from vacuum energy exploiting the Casimir effect, the combination of magnetodynamics and space-time, ambient temperature and pressure superconductors (which would win them a Nobel Prize if it worked), and negative entropy. They just need €2.7M of funding to move ahead!

You are also entitled to a beautiful **quantum cooler** from **Chillout Systems** that has only quantum in its name. It uses a compact classic compressor<sup>1861</sup>.

Other cases extrapolate to the macro scale of quantum phenomena observed at a nano scale. This is the case of **time inversion** with quantum computing, a view of the mind that is linked to the reversible nature of quantum gates but does not mean that one can go back in time scale in macroscopic practice<sup>1862</sup>.



We also have equally wild theories willing to **predict the future** with quantum computing. If it is true that quantum computing allows us to evaluate all the solutions of a complex problem, it is reduced to simple problems in view of the complexity of macroscopic life, even if it could be deterministic<sup>1863</sup>.

The next step is to consider that we are actually living in a **simulation**.

---

<sup>1860</sup> See [60 seconds over sinoland: quantum satellite camera used to do movable, panoramic photos of Shanghai](#), December 2018 ([video](#)) and [Truth Behind Viral 24.9 Billion Pixel Image Taken By Chinese "Quantum Satellite"](#) by Anmol Sachdeva, December 2018 and the [Bigpixel](#) website to view the view.

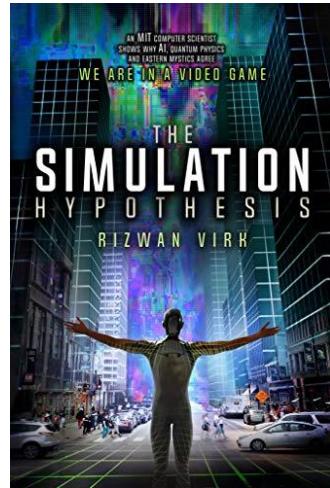
<sup>1861</sup> See [Chillout Systems Quantum Cooler](#). It is sold for \$2199.

<sup>1862</sup> See [Arrow of time and its reversal on the IBM quantum computer](#) by G. B. Lesovik et al, 2018 (14 pages) and [Does the IBM quantum computer violate the second principle of thermodynamics?](#), 2019.

<sup>1863</sup> See [Interfering trajectories in experimental quantum-enhanced stochastic simulation](#) by Farzad Ghafari et al, 2019 (7 pages).

This is the theory presented in Rizwan Virk's The [Simulation Hypothesis](#). The author presents himself as an MIT Computer Scientist, whereas he is more of an entrepreneur in video games, more accustomed to books on entrepreneurship than on science. This kind of simulation scenario is roughly equivalent to believing in a kind of omnipotent God who controls everything or who created the simulation tool. The question can moreover be recursively implemented: if this creator has developed a simulation tool, who created his universe and isn't this one also a simulation?

Another case that should inspire the utmost caution is that of this curious company **Precog Technologies**, which claims to offer solutions for teleportation, time travel and anti-gravity systems. Miracles one stop shopping!



The company was created to valorize the intellectual property of a certain Anisse Zerouta that is covered in a dubious scientific paper<sup>1864</sup>.

Another guy, from **Quanta QB** (South Africa) thinks he has also found a qubit architecture that showcases a miraculous 0% error rate<sup>1865</sup>.

We also saw the first quantum scam appear in 2018 with this fake article in the Guardian reporting a quantum computer project for Elon Musk's finance<sup>1866</sup>. The trained eye quickly detects that it is a montage, like this series of **QuantumAI quantum** computers that are nothing more than D-Waves annealers whose logo has just been photoshopped.

**Support The Guardian**

Available for everyone, funded by readers

Contribute →    Subscribe →

News    Opinion    Sport    Culture    Lifestyle    More ▾

**[INNOVATE]** Elon Musk To Step Back From Tesla And SpaceX, Jumps on Quantum Computing Financial Tech

**CNN EXCLUSIVE**

most viewed

- Venezuela crisis: Maduro claims victory over 'deranged' coup attempt
- Trump Russia: Mueller criticized attorney general's memo on findings
- Live Venezuela crisis: Maduro claims coup has been 'defeated' – as it happened
- Japan welcomes new emperor Naruhito as Reiwa era begins

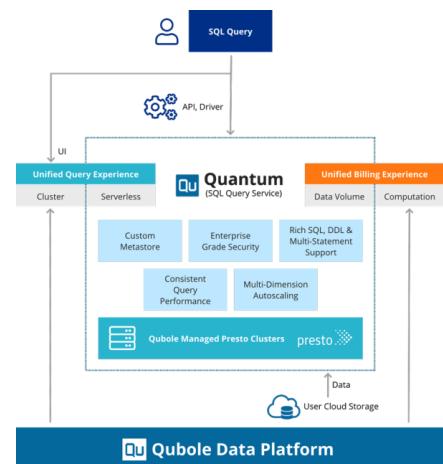
<sup>1864</sup> See [The Seed Theory: Unifying and replacing quantum physics and general relativity with "state physics"](#) by Anisse Zerouta, 2017 (28 pages) which develops a theory of parallel worlds that does not seem to meet the criteria of a scientific publication worthy of the name. Anisse Zerouta is a company manager in Paris born in 1973, first with Elysee Communication (2008-2011) then with Avenir Optique, an optician (2011-\*), companies with only one employee, its founder ([source](#)). Created in September 2018, Precog-tec would have a CTO, a certain François Bissegé, who has a PhD in sociology ([source](#)) and another employee, Julien Darivel, who has a DUT and worked at PSA. It's bizarre!

<sup>1865</sup> See [I made the Quantum Breakthrough](#), June 2019.

<sup>1866</sup> See [Elon Musk to Step Back From Tesla And SpaceX, Jumps on Quantum Computing Financial Tech](#) (not dated).

Second, the article is supposed to come from the Guardian, but not the url! It quotes a number of scientists from research laboratories around the world, all with Russian names. The article points to **QuantumAI**'s online service which would be able to go around robbing the rich and redistributing the money to the poor. And the site indicates that the startup has Jeff Bezos and Bill Gates as advisors and IBM, Microsoft and OpenAI as partners.

There is another, called **Quantum Code**. Obviously, run away! It is in fact a scam designed to rob users of their savings, but in an indirect way. The site offers to create an account by providing its coordinates. These are then resold to unscrupulous companies of shady financial products that exploit leads of prospects easy to fool.



We can also quote **Qubole** which launched its Quantum SQL server, which has nothing quantum<sup>1867</sup>. The **Samsung** Quantum 8K processor launched in 2018 was not particularly quantum either, except via its classical CMOS transistors.

In consumer products goods, we have this washing powder **Quantum Max** of the brand **Finish** from the Reckitt Benckiser group. And also **Quantum American** PQ rolls and Quantum red wine from **Beringer**, a brand from Napa Valley, California.



Otherwise, **Quantum Corp** (USA) does nothing quantum and just manages tape storage. The same goes for **Quantum Entanglement Entertainment** (Canada) which, as its name indicates, is in the content market. **Quantum Surgical** (France) makes surgery robots for liver cancer, which have nothing quantum. **QuansumScape** is a solid-state lithium battery manufacturer in the USA. **Quantic** Executive MBA has only quantum in name. **Quantum Metric** is providing cloud based digital content design software tools. At last, **QuantumLeaf** is a cannabis software company servicing the cannabis industry in the USA.

<sup>1867</sup> See Qubole launches [Quantum, its serverless database engine](#) by Frederic Lardinois, June 2019.



lithium batteries



entertainment



medical device



cannabis software



tape storage



Quantum Metric

digital content design



MBA training

### Quantum fake sciences key takeaways

- Quantum physics has been for a while integrated in highly dubious offerings, particularly in the healthcare and energy domains.
- There is a proliferation of gurus and scams-based miracle cures machines for detecting electromagnetic waves or vague energies, and restoring your body balance. It is at best a subset of the lucrative placebo effect industry targeting the gullible!
- The shift from some low-level physics studies on water and matter led some scientists to explain consciousness with quantum physics. This form of reductionism is unproven. It's the same with scalar-waves detectors or generators, miraculous healing crystals, structured water and other quantum medallions.
- This part proposes a simple methodology to detect these healthcare related scams, with using some common sense.
- We uncover some other scams in the free energy generation category. These systems are supposed to extract some energy from vacuum when their only actual effect is to pump money out of your wallet.
- Quantum physics is sometimes used in management and marketing. This ebook offers you a nice in-depth parody of these methodologies.
- At last, we showcase a few companies using quantum in their branding when they have nothing quantum at all to offer.

# Conclusion

Quantum technologies perfectly symbolize the world of innovation and extreme entrepreneurship: it is full of uncertainties, risks and failures. There is "test & learn", the crossroads of sciences, the need to invest well in advance of economic success, with a critical role for government investments, the only ones able to invest in the long term, more than 10 years ahead. Numerous parallel paths of exploration have been launched by researchers and entrepreneurs. Only a few will succeed. A new industry is emerging from all of this.

To write this book, I downloaded and compiled more than 2500 documents freely available on the Internet, viewed dozens of hours of conferences and courses on YouTube, and met dozens of researchers and entrepreneurs.

I have to thank several talented people here. First of all **Fanny Bouton**, with whom we started this quantum adventure in 2018, starting with the conference [Le quantique, c'est fantastique](#) at the Web2day in Nantes, delivered on June 14, 2018.



This conference in Nantes, the following ones and this ebook benefited from meetings or exchanges with a fine group of specialists in the sector that we must thank: **Alain Aspect** (X, SupOptics), **Daniel Esteve** (CEA-DRF), **Christian Gamrat** (CEA LIST), **Maud Vinet** (CEA-Leti in Grenoble), **Tristan Meunier** (CNRS Grenoble), **Alexei Tchelnokov** (CEA Grenoble), **Laurent Fulbert** (CEA-Leti Grenoble), **Cyrille Allouche** and **Philippe Duluc** (Atos), **Bernard Ourghanlian** and **David Rousset** (Microsoft), **Pat Gummán** (IBM), **Etienne Klein** (CEA), **Christophe Jurczak** and **Zoé Amblard** (Quantonation), **Nicolas Gaude** (Prevision.io) and **Françoise Gruson** (Société Générale).



We have since been able to meet even more quantum researchers such as **Philippe Grangier** (Institut d'Optique), **Elham Kashefi** (LIP6 and VeriQloud), **Marc Kaplan** (VeriQloud), **Pascale Senellart** (C2N and Quandela), **Franck Balestro** and **Alexia Auffèves** (CNRS Institut Néel), **Matthieu Desjardins** (LNA and CNT Technologies now C12), **Jacqueline Bloch** (C2N) and **Iordanis Kerenidis** (CNRS). We were also able to meet with **Cédric Villani** on several occasions to discuss the subject. I also met **Heike Riel** from IBM Zurich as well as **Vern Brownell**, the CEO of D-Wave in 2019.

Then, **Artur Ekert** (CQT Singapore), **Patrice Bertet** (CEA SPEC), **Xavier Waintal** (CEA IRIG), **Yvain Thonnart** (CEA LIST), **Rob Whitney** (LPMMC Grenoble), **Damian Markham** (CNRS LIP6 and JFLI in Tokyo), **Bruno Desruelle** (Muquans), **Georges-Olivier Raymond** and **Antoine Browaeys** (Pasqal), **Théau Perronnin** and **Raphaël Lascanne** (Alice&Bob) as well as **Jeremy O'Brien** (PsiQuantum), **Magdalena Hauser** and **Wolfgang Lechner** (ParityQC), **Roger MKinley** and **Peter Knight** (UK), **Heike Riel** (IBM) and the IBM Zurich research teams. I also had discussions with the teams from **Qblox**, **Qilimanjaro**, **Quantum Motion**, **Strangeworks** and **IQM**.

There were these countless discussions with **Jean-Christophe Gougeon** of Bpifrance, **Neil Abroug**, who is now the coordinator of the quantum strategy in France, as well as **Charles Beigbeder** and **Christophe Jurczak** from Quantonation and Le Lab Quantique, who wrote the [foreword](#) of this ebook, page 9. I should also mention the numerous exchanges related to quantum investments with **Cédric O** and his team, in the French government. He was onboard early on and became its driving force within the government.

This fourth edition benefited from the contributions of the following proof readers for some specified parts or for the whole document: **Alexia Auffèves** (CNRS Institut Néel, measurement, energetics of quantum computing, quantum foundations, photon qubits), **Antoine Browaeys** (IOGS and Pasqal, cold atoms), **Christophe Chareton** (CEA LIST, linear algebra, quantum algorithms and development tools), **Cyril Allouche** (Atos, supercomputing, emulators, European projects), **Daniel Esteve** (CEA DRF, superconducting qubits), **Eleni Diamanti** (CNRS LIP6, quantum telecommunications and cryptography), **Elvira Shishenina** (BMW, proof-read all the document), **Frédéric Nguyen Van Dau** (Thales, quantum sensing), **Georges Uzelger** (IBM, quantum algorithms and software tools), **Jonas Landman** (CNRS IRIF, quantum algorithms), **Léa Bresque** (CNRS Institut Néel, quantum physics 101, postulates, measurement), **Marc Kaplan** (Veriqloud, quantum telecommunications and cryptography), **Michel Kurek** (who patiently proof-read several times all the ebook and checked all hyperlinks), **Peter Eid** (Arm, classical and unconventional computing, telecommunications/cryptography), **Philippe Grangier** (Institut d'Optique, quantum foundations), **Pol Forn-Díaz** (Qilimanjaro, superconducting qubits), **Théau Perronnin** and **Jérémie Guillaud** (Alice&Bob, cat-qubits) and **Valérian Giesz** (Quandela, photon qubits and photonics). Thank you all for your role and your sense of details!

And maybe you, next time :) !

Cheers,

Olivier Ezratty, September 2021

# Bibliography

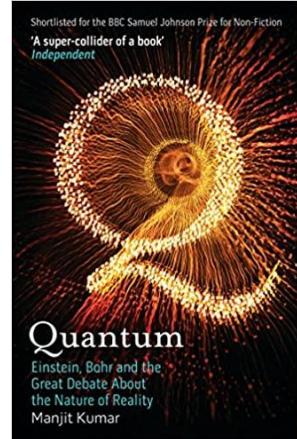
Here are a few books and other sources of information on quantum technologies that I consulted or discovered to prepare and update this ebook.

## Books and ebooks

If you wander in Amazon or your other preferred real-life or virtual scientific bookstore or University library, you'll find an abundant literature on quantum physics and quantum information. Many people willing to learn in these domains have a hard time finding the "right" book that is adapted to their existing knowledge and particularly, to their fluency in mathematics. Here's a not-too long list of books for this purpose. It's mostly adapted to students since, if you work in the industry, you probably won't have much time to read many of these thick books.

### Quantum physics

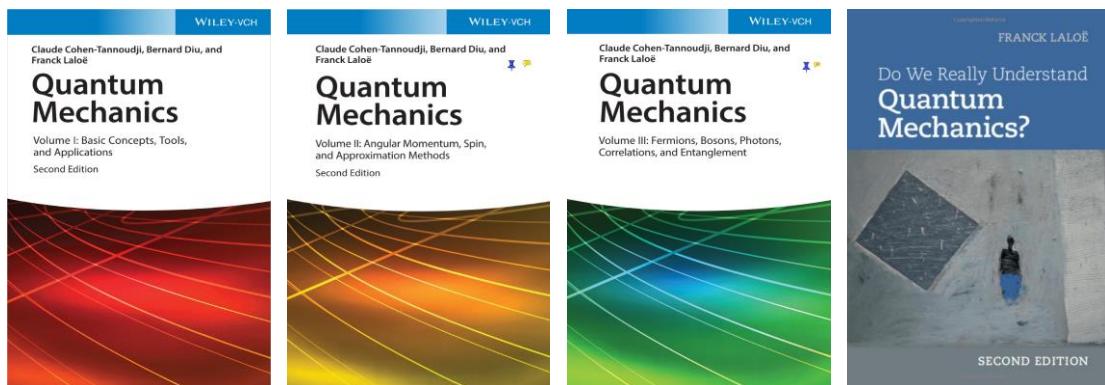
[Quantum: Einstein, Bohr, and the Great Debate about the Nature of Reality](#) by Manjit Kumar, 2009 (480 pages) is an excellent history book about the creation of quantum mechanics. It centers a lot on the works from Max Planck, Niels Bohr, Albert Einstein, Max Born, Werner Heisenberg and Erwin Schrodinger. It's a good account of the history of ideas and how quantum physics saw the day of light. It also showcases a lot of lesser known scientists who played key roles around the most famous ones and the balance between theoreticians and experimentalists. On top of that, the book scientific content is quite good and easy to understand, without any mathematics! Other history books and papers, mostly available in open access, are also mentioned throughout this ebook, particularly in the [History and Scientists](#) section, starting page 32.



[Quantum Mechanics, Volume 1: Basic Concepts, Tools, and Applications](#), Second Edition, 2017, by Claude Cohen-Tannoudji, Bernard Diu and Franck Laloë (879 pages) is an undergraduate reference series of books to learn quantum physics. It is considered to be the reference or the bible by many students and teachers of quantum physics.

[Quantum Mechanics, Volume 2: Angular Momentum, Spin, and Approximation Methods](#), Second Edition, 2017, by Claude Cohen-Tannoudji, Bernard Diu and Franck Laloë (688 pages).

[Quantum Mechanics, Volume 3: Fermions, Bosons, Photons, Correlations, and Entanglement](#), Second Edition, 2017, by Claude Cohen-Tannoudji, Bernard Diu and Franck Laloë (747 pages).



[Do we understand quantum mechanics? Second Edition](#) by Franck Laloë, 2019 (550 pages) is an interesting piece that documents the debates on quantum foundations and how to interpret quantum physics. [Do we really understand quantum mechanics?](#) by Franck Laloë, 2004 (118 pages) is a shorter and older version of this ebook, in public access.

[Lecture notes on Quantum Mechanics](#) by Frédéric Faure, 2015 (397 pages) which provided me with some leads to link quantum mechanics to its mathematical formalism and notably to explain the Born equation.

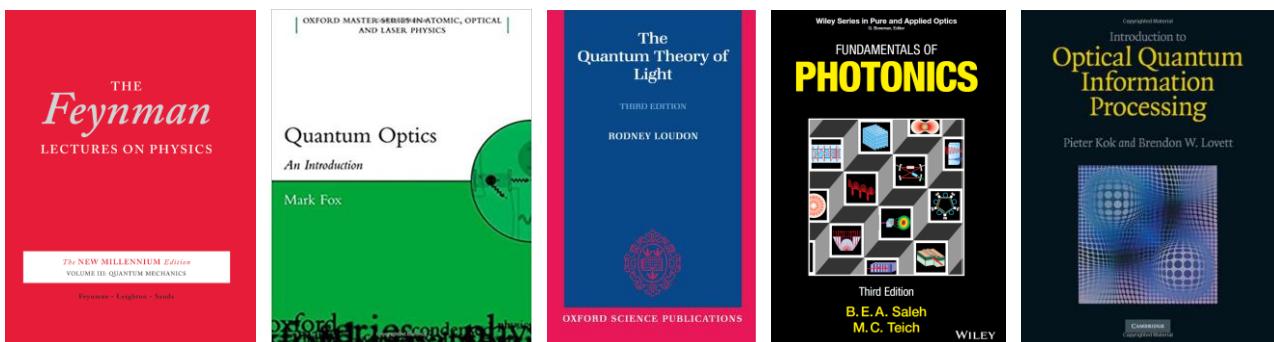
[The Feynman Lectures on Physics - Volume III on Quantum Mechanics](#) by Richard Feynman, Robert Leighton and Matthew Sands, (688 pages). It contains lecture notes of Feynman legendary courses from the early 60s. These are treasures of pedagogy with a content that is still up to date to grasp the fundamental of quantum physics. One advantage is it doesn't make any abuse of mathematics.

[Quantum Optics An Introduction](#) by Mark Fox, 2015 (397 pages) an excellent coverage of the broad field of quantum optics and the second quantization.

[The Quantum Theory of Light](#) by Rodney Loudon, 1973-2001 (450 pages) is a classic book on quantum light, that is useful to later better understand the physics of photon qubits used in quantum computing, telecommunications and cryptography. It classically starts with Planck's radiation law, then covers lasers, light-matter interactions, Mach-Zehnder interferometry, light quantization, single mode, multi-mode and continuous-mode optics and non-linear optics.

[Fundamentals of Photonics](#) by Bahaa Saleh and Malvin Teich, 2019 (1401 pages) is a comprehensive quantum optics books that also covers instrumentation, which means it's good stuff for experimentalists.

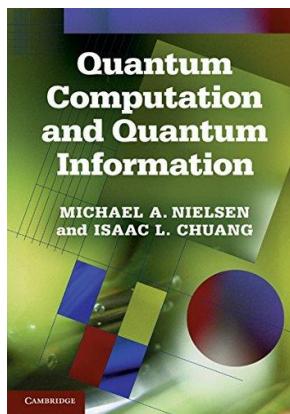
[Introduction to Optical Quantum Information Processing](#) by Pieter Kok and Brendon W. Lovett, 2010 (506 pages) is another classic quantum photonics books covering quantum information systems.



[I Don't Understand Quantum Physics](#) by Douglas Ross, 2018 (104 pages) is a nice primer to conceptualize and visualize many quantum phenomena. It describes the founding experiments of quantum physics (blackbody radiation, photoelectric effect, Compton scattering, etc), the wave-particle duality, matter wave, indeterminacy, Schrödinger's equation, superposition and the EPR paradox.

## Quantum information

[Quantum Computation and Quantum Information](#) by Michael Nielsen and Isaac Chuang, 2010 (10th edition, 704 pages, public access) is the definitive reference on the basics of quantum computing. It answers many key questions, in particular on the mathematical models of linear algebra used in quantum computing. It also covers the basics of quantum physics, quantum postulates, problems complexity classes, quantum measurement, quantum algorithms, how qubits are realized (harmonic oscillators, trapped ions, photons, NMR), the impact of quantum noise and decoherence, how quantum error corrections work, what is fault-tolerant quantum computing, how about Shannon and Von Neumann information entropy and the likes. It also covers quantum key distribution and cryptography.

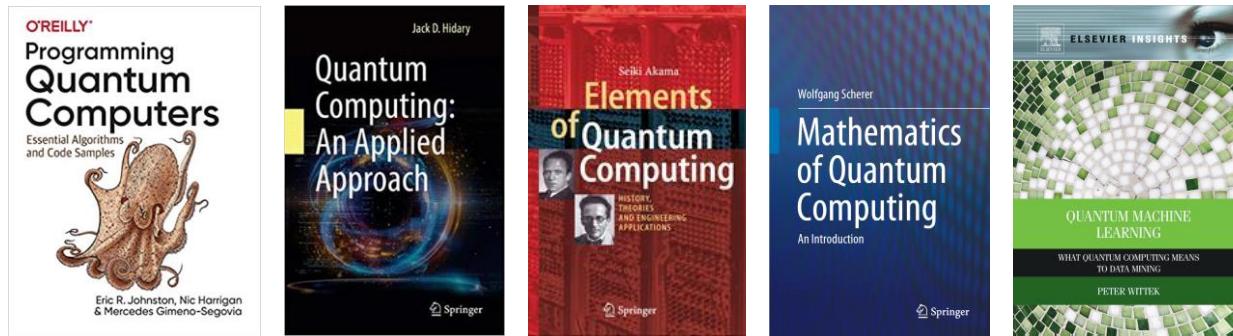


[Programming Quantum Computers - Essential Algorithms and Code Samples](#) by Eric R. Johnston, Mercedes Gimeno-Segovia and Nic Harrigan (2019, 336 pages) is a excellent and detailed description of key quantum algorithms like the QFT, phase estimation and the likes.

[Quantum Computing: An Applied Approach](#) (2021, second edition, 445 pages), a fairly comprehensive book covering quantum algorithms and their mathematical foundations. It briefly describes the different architectures of quantum computers.

[Elements of Quantum Computing](#) by Seiki Akama (133 pages), which is at the same time concise, precise and quite complete on the nooks and crannies of quantum mechanics and quantum computing, with a good historical overview.

[Quantum Machine Learning - What quantum computing means to data mining](#), by Peter Wittek, 2014 (176 pages) is a good introduction to machine learning and quantum machine learning although many progresses were made since this book's publication.

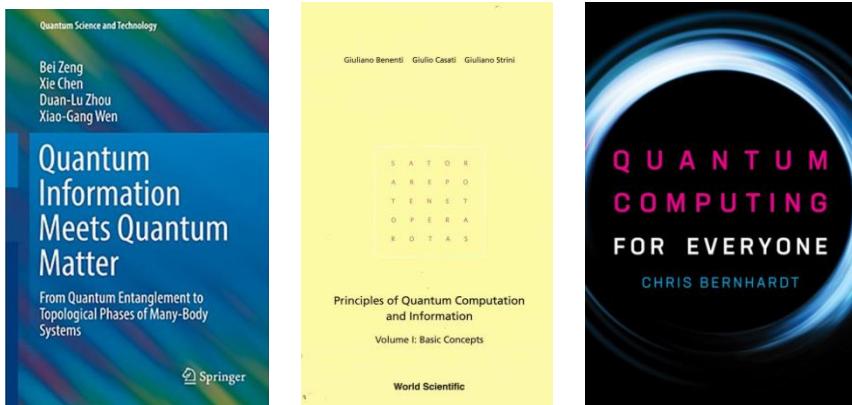


[Quantum Information Meets Quantum Matter](#) by Bei Zeng, Xie Chen, Duan-Lu Zhou and Xiao-Gang Wen. It is available in a February 2018 version [on Arxiv as a free download](#) (373 pages).

[Quantum computing- from quantum physics to quantum programming in Q#](#) by Benoit Prieur, 2019 (244 pages). It starts with the general principles of quantum physics. The section on quantum computers themselves is rather thin and explores only a few technologies (superconductors and NMR, which is little used). The rest is dedicated to learning programming in Q#, Microsoft's quantum programming language.

[Principles of Quantum Computation and Information, A Comprehensive Textbook](#) by Giuliano Benenti, Giulio Casati, Davide Rossini and Giuliano Strini, December 2018 (598 pages).

[Quantum Computing for Everyone](#) by Chris Bernhardt, 2019 (216 pages) which describes the basics of quantum computing starting with the inevitable qubit, quantum gates, accelerations brought by quantum algorithms and the main components of a quantum computer.



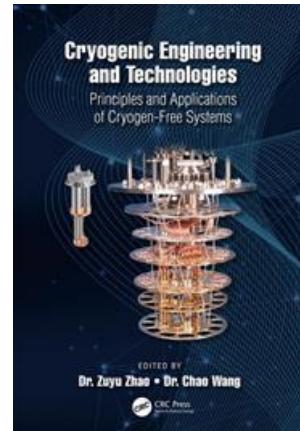
[Quantum computing](#) by Joseph Gruska (1999, 390 pages), another fairly comprehensive base covering all aspects of quantum computing and communication.

[An Introduction to Quantum Computing](#) by Phillip Kaye, Raymond Laflamme and Michele Mosca, 2007 (284 pages) which starts with some mathematical foundations of quantum physics and quantum computing. By reference authors such as Raymond Laflamme (Canada) who is one of the fathers of error correction codes.

[Introduction to quantum computing algorithms](#) by Arthur Pittenberger, 2001 (152 pages) which describes classical quantum algorithms with a good part dedicated to error correction codes.

[Quantum Internet](#), a 60-page magazine presenting the different sides of quantum computing, published by TU Delft (2019).

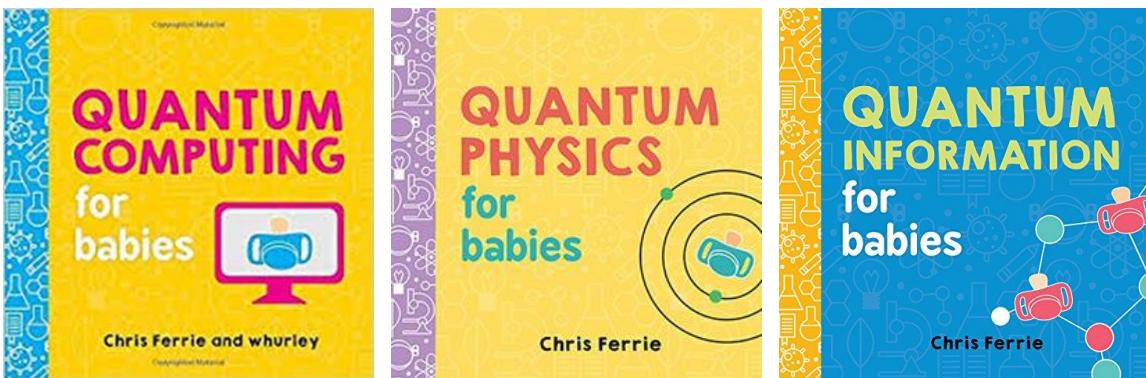
[Cryogenic Engineering and Technologies](#) by Zuyu Zhao and Chao Wang, October 2019 (386 pages) is a reference book on cryogenic issues with a very extensive and well-documented history. There is an excellent chapter on dry dilution cryostats used in quantum computers. This helped me to prepare the part of this ebook on [cryogenics](#) (page 361) in addition to an interview with the team of the French startup CryoConcept and those of the Institut Néel in Grenoble.



[Unconventional Computation](#) by Bruce MacLennan, University of Tennessee, October 2019 (304 pages) which discusses the energy issues of computation (reversible, non-reversible) and various alternative methods of computation including quantum computing and molecular computing.

## Comics

[Quantum Computing for babies](#) by Chris Ferrie and William Hurley, April 2018, is aimed more at children or even older children. The book popularizes the major concepts of physics and quantum computing in a very colorful way. It comes from a professor of quantum computing at Sydney University of Technology and the founder of the American startup Strangeworks. William Hurley is the founder of **Strangeworks**. Two other books in the same vein from Chris Ferrie were also released: [Quantum Physics for babies](#) and [Quantum Information for babies](#), all for less than \$10. I “read” the last one (24 pages) and I’m not sure even an adult would really understand how quantum computing after looking at it. This is the danger of oversimplification and information dilution.



## Presentations

Here are a few conferences and presentation materials rather well done to popularize quantum computing.

[Quantum computing for the determined](#) by Michael Nielsen, a series of 22 videos on quantum computing, 2011, accompanied by a [long text of explanations](#).

CERN's [Quantum Computing for High Energy Physics workshop](#) in November 2018, with presentation materials and videos and interesting talks by various players in quantum computing, including Intel, who are not often seen. The specific content may be overtaken by the basic principles remain valid.

[Quantum computing Overview](#) by Sunil Dixit, September 2018 (94 slides) is a presentation by Northrop Grumman that takes a fairly broad look at quantum computing and the underlying mathematical models.

[A Practical Introduction to Quantum Computing From Qubits to Quantum Machine Learning and Beyond](#), by Elias Combaro, CERN course, 2020 (251 slides) is a good course on quantum algorithms, debugging, validation, verification and benchmarking.

[Quantum computing](#), a four-part course by Hélène Perrin at Université Paris 13, February 2020 ([lecture 1](#) of 77 slides on trapped ions, [lecture 2](#) of 36 slides on superconducting qubits, [lecture 3](#) of 39 slides on silicon, molecular and NV Centers qubits, [lecture 4](#) of 75 slides on cold atoms). This requires a good background in physics to be understood from start to finish. The references provided allow to deepen the topics covered.

## Events

There are numerous conferences on the different scientific branches of quantum technologies.

More generalist conferences include the **QCB** organized by Bpifrance in Paris (June 2019 and November 2020), the **Q2B** of QC Ware organized in California in December each year, the English **QT Digital Week** in June (which was held as a webinar in 2020) and the **European Quantum Technologies Conference** in Dublin in November-December 2021. It goes without saying that all conferences of this kind have the ambition to be international, if only because the expertise is spread around the world, and many research teams work in partnership with teams from other countries.

Various international conferences on quantum computing take place in France, either permanently or temporarily.

This is the case of the **ICoQC** (International Conference on Quantum Computing) held at the ENS in Paris in November 2018<sup>1868</sup>.

---

<sup>1868</sup> See <https://icoqc.sciencesconf.org/>.

To mobilize the ecosystem, **Bpifrance** organized the **QCB** (Quantum Computing Business) **Conference** on 20 June 2019 in Paris with a fine line-up of speakers including Alain Aspect, Cédric Villani, the CEO of D-Wave, representatives from IBM, Rigetti, etc., as well as leading French quantum researchers and entrepreneurs such as Maud Vinet (CEA-Leti) and Pascale Senellart (Quan-dela), all with the participation of Cédric O, Antoine Petit (President of the CNRS) and Thierry Breton (Atos). The next edition was scheduled for November 4, 2020.

On June 28, 2019, **CEA-Leti** organized a quantum workshop on the occasion of the Leti Innovation Days ([program](#)). It brought together an excellent panel of researchers in the field, from a number of French research laboratories<sup>1869</sup>. The next edition ran in June 2021 in virtual format.

**Quantum Technology International Conference** or QTech conference is organized by European researchers, mostly from Spain, Germany, France, UK, Sweden and Italy. The last edition was online and organized in November 2021.

Otherwise, scientific symposia are organized by different groups such as the **PWYP** and the **GDR IFQA**, for example the 10th symposium of the latter which took place in Paris in November 2019 ([link](#)). The next edition is planned for early December 2020 in Grenoble.

Europe is also quite active in the organization of scientific conferences on quantum computing. With a few examples: the [QIP](#) conference in January 2018 at the University of Delft in the Netherlands, followed by the [Quantum Europe](#) 2018 conference on May 17-18, also in the Netherlands. Other [2018 conferences on quantum](#) computing have been or will be held in Switzerland, Portugal, Spain, France, Germany, Austria and even Greece. Sometimes the presence of French speakers is negligible, as at [Quantum Simulation & Computation](#) in Bilbao in February 2018.



**Laser World of Photonics and World of Photonics Congress** (June). 2019 edition had 34K visitors and 6717 congress and panels participants.

Last edition was June 20-24, 2021 (online). Next edition is planned on April 26-29, 2022 in Munich, Germany. A Shanghai (March 23-25, 2022) and India edition (Bengaluru, September 22-24, 2021) are also planned.



**MLQ Conference**, or Machine Learning for Quantum, was held online in March 2021. It was sponsored by Nvidia and Quantum Machines.



**Inside Quantum Technologies** New York is organized by QuTech and 3DR Holdings. May 17-20, 2021 (online). A European edition in September 2019 was held in The Hague, Netherlands. It gathers industry and academics.

**Quantum.Tech** is another conference focusing on industry use cases of quantum technologies. The fourth edition, organized out of the UK, was held online in September 2021 and covered all quantum technologies (hardware/software, computing, sensing, telecoms/cryptography). An US edition is planned in Boston in June 2022.



**QuApps** is an International Conference on Applications of Quantum Technologies happening in Düsseldorf. The next/last edition was in September 2021.

<sup>1869</sup> I reported on it in [Towards an Industrial Strategy for Quantum Computing?](#) June 2019.

## Training

Berkeley courses for 2013: [Quantum Mechanics and Quantum Computation](#) on YouTube.

[Videos](#) from the Stanford Quantum Computing course.

The [Quantum Computing Fundamentals](#) course offered by MIT.

An [online training course on quantum programming](#) offered by Brilliant in partnership with Microsoft.

The [QSIT](#) course ([FS 2016](#)) at ETH Zurich with its slides and lecture notes.

[Quantum Computing as a High School Module](#), a curriculum with exercises on the basics of quantum physics for students at the BAC level.

## Websites

[Fact Based Insight](#) is an analyst shop run by David Shaw in the UK. It publishes very interesting charts and analysis on the quantum ecosystem, including some insights on quantum hardware.

[The Quantum Daily](#), a quantum news site created by Ethan Hansen, which also broadcasts a [monthly podcast](#). Many of the news are cut and pastes of press releases from vendors, government and research labs.

[Quantum Zeitgeist](#) is another quantum news media.

[Quantaneo](#) is yet another quantum news web site, created by Philippe Nieuwbourg in 2019 with an English and a French edition.

[AzoQuantum](#), an information site on quantum science news.

[Quantum - the open journal for quantum science](#), a site of scientific news on quantum mechanics.

[Quantiki](#), an information site on quantum computing.

[Quantum Info](#), which lists, among other things, the agenda of world quantum events.

[Qosf](#), a site that inventories guides and training for developers of quantum applications.

[Nathan Shammah's newsletters](#) from RIKEN (Japan).

[Quantum Journal](#), the open journal for quantum science, which references scientific publications on quantum, generally available on Arxiv.

[Quantum-show](#) from the company Anabole, is a popularization site that offers graphic, sound and interactive representations of the states of each of the qubits mobilized in quantum algorithms. They allow to think from a philosophical point of view about the interpretation of what is a superposition of "true" and "false". It is a revisiting of the origins of computer science in the light of quantum computing.

## Podcasts

[Chris Bishop's podcasts](#) on quantum technology news, published on Inside Quantum Technology's web site. These are mostly half-and-hour interviews of quantum startup founders, the first and lasts episodes as of September 2021 being with Qblox, ColdQuanta, IonQ, Strangeworks and SeeQC founders. It started mid-2021.

Consulting firm [Protivity](#) also launched its own series of podcasts, in May 2021. Like Chris Bishop's podcasts, it's about interviewing quantum startup founders. They also last half an hour.

[Quantum Computing Now](#) by Ethan Hansen covers quantum computing news, basic concepts, and what people in the field are doing. The first episode was aired in July 2019. They are biweekly and cover news as well as science and learning tutorials.

The [Quantum podcasts](#) that I have been recording regularly (in French) since September 2019 with Fanny Bouton (OVHcloud). They are available on all audio platforms (Spotify, iTunes, Deezer, ...) as well as on YouTube in video version. It covers quantum news including what's happening in the ecosystem, with startups and in research. We decipher many lead scientific announcements. Our first episode was on Google's supremacy!

They are complemented by the Decode Quantum interviews that we have been publishing since March 2020 with a great variety of personalities (lead researchers, startup founders, investors, user companies, public servants, etc.) in partnership with Frenchweb. The first episodes featured [Pascale Senellart](#), [Alexia Auffèves](#), [Maud Vinet](#), [Eleni Diamanti](#), [Elham Kashefi](#), [Théau Peronnin](#) and [Raphaël Lescanne](#) from Alice&Bob, Christophe Jurczak from Quantonation and Jean-Christophe Gougeon from Bpifrance, Georges-Olivier Reymond and Antoine Browaeys from Pasqal and Alain Aspect. We had over 30 episodes in-store as of September 2021! They last about one hour.

## Reports

[Inside Quantum Technology](#), an analyst company dedicated to quantum technologies, which sells industry reports.

You can also find analysts reports on quantum technologies with McKinsey, BCG, Yole Development and other analysts companies.

## Miscellaneous

[Designing and Presenting a Science Poster](#), Jonathan Carter, Berkeley (20 slides) which is intended to help researchers design a good research project presentation poster.

# Glossary

*What is the purpose of a glossary? It allows you to find your way around in a new terminology and to step back to understand new concepts. For the author, it was also a good checkpoint of his own understanding and ability to popularize scientific and technological concepts. Some of these descriptions are simplified versions derived from Wikipedia definitions. Welcome to the lingua franca of quantum technologies!*

**137:** constant used to compare different equivalent quantities in quantum physics. It turns out that 1/137 is a value that corresponds approximately to the fine-structure constant, a ratio that is found in several places in quantum physics and compares data of the same dimension. It is for example the ratio between the speed of an electron in the lower layer of a hydrogen atom and the speed of light or the probability of emission on the absorption of a photon for an electron. 137 is a bit like 42 in quantum physics. Wolfgang Pauli died after an operation for pancreatic cancer, while his hospital room was number 137.

**ADC:** analog-digital converter. Converts an analog signal into a digitized signal. In quantum technologies, it is used to convert the reflected microwave signals used in superconducting and electron spin qubits readout.

**Adiabatic:** quantum computation method used in particular with D-Wave quantum annealing computers. A complex Hamiltonian describing a complex system is first determined whose fundamental state describes a solution to the problem under study. A system with a simpler Hamiltonian is then prepared and initialized in its fundamental state. This Hamiltonian then adiabatically (meaning, with no energy or mass exchange with the outside environment) evolves into the complex Hamiltonian. According to the adiabatic theorem, the system remains in its fundamental state, and its final state describes a solution to the problem under consideration.

**Adiabatic theorem:** quantum mechanics concept created by Max Born and Vladimir Fock in 1928. It states that a quantum mechanical system subjected to gradually changing external conditions adapts its form, but when subjected to rapidly varying conditions there is insufficient time for the functional form to adapt, so the spatial probability density remains unchanged. This can be used to find Hamiltonian energy minimums with quantum algorithms running on various architectures: gate-based, annealing and quantum simulation.

**Advantage:** see quantum advantage.

**Algorithm:** a method of problem solving that is made up of a finite sequence of operations or instructions. The word comes from the name of the 9th century Persian mathematician, Al-Khwârizmî.

**Algorithmic qubit:** benchmark metric proposed by IonQ which corresponds to the number of qubits usable with an equivalent computing depth with a randomized benchmark producing a good result in 2/3<sup>rd</sup> of the runs. It's actually  $\log_2$  of IBM's quantum volume.

**Amplitude:** this term has various meanings depending on the context. It can be the classical amplitude of a wave,

i.e. half of its maximal variation, as opposed to its phase. For a quantum object, it can be the complex amplitudes of its basis states or eigenvectors. With a qubit in its Bloch sphere representation, the amplitude is related to the projection of the qubit vector on the z axis. But the  $\alpha$  and  $\beta$  describing the qubit vector are also amplitudes, although, precisely, complex amplitudes. These complex amplitudes define the qubit amplitude ( $1-\cos(\theta/2)$ ) and its relative phase (angle  $\varphi$ ).

**Anharmonic oscillator:** contrarily to harmonic quantum oscillator that have the same energy difference between each consecutive energy levels, an anharmonic quantum oscillator has different energy differences between consecutive energy levels. This is the case of superconducting qubits, in order to create two manageable energy levels that are controlled with microwaves with the highest energy transition level of the oscillator.

**Angular momentum:** generally speaking, speed of rotation of a rotating object. In quantum physics, angular momentum is quantized and can have only discrete values.

**Anyons:** type of elementary particle found in two-dimensional systems. It is a generalization of the concept of bosons and fermions. Anyons have intermediate statistical behaviors between the two types of elementary particles. They are in fact virtual particles that live in two spatial dimensions and are generally based on electrons or electron gaps moving in superconducting metallic 2D structures. Anyons are a particular type of quasi-particles. They are used in topological quantum computers and would be used in particular in computers based on the hypothetical Majorana fermions studied at Microsoft.

**Arxiv:** Cornell University's site that allows researchers to publish scientific papers prior to publication in peer-reviewed journals such as Nature, Science or Physical Review. It can take up to 9 months between publication of an article on Arxiv and publication in a peer-reviewed journal. In the latter case, the article will have eventually evolved. The interest of Arxiv in literature search is that publications are open and free of charge whereas most of the peer-reviewed journals are not free. The disadvantage is that the articles are not necessarily validated and that one has to make his own evaluation. It should be noted that in a researcher's publication, there are often several authors, up to several dozen. The first author is generally the PhD student who has carried out a large part of the work, particularly its experimental part. Others are contributors who helped him/her. The last author is the thesis director or principal investigator (PI), the group leader or the laboratory director who has closely or remotely su-

pervised the project. He/she probably contributed significantly to the article writing and cleanup.

**Atoms:** the smallest constituent element of matter that manifests chemical properties. It consists of a nucleus, with one or more positively charged protons and zero or more neutrally charged neutrons, around which negatively charged electrons gravitate. In a neutral atom, the number of electrons is equal to the number of protons. Otherwise, the atom is negatively or positively charged and forms an ion. The number of protons determines the nature of the atom in Mendeleev's Elements Periodic Table. An atom with one proton is hydrogen, with two protons it is helium, etc. Uranium has 92 protons. The nucleus represents the bulk of the atom mass. The isotopes of an element correspond to variations in the number of neutrons. In general, the number of neutrons of an element is equivalent to that of protons. Electrons are distributed in layers whose number depends on the atomic number. They are numbered from 1 to 7. Each layer can contain a maximum of  $2n^2$  electrons, n being the number of the layer (thus 2, 8, 18, 32, 50, 72 and 98). This model was developed by Niels Bohr between 1909 and 1913. The chemical properties of the element depend on the number of electrons of the last layer which is called the valence layer. If this number is  $2n^2$ , the atom will be inert and will not combine chemically with other atoms. Carbon has three layers of electrons, the last one having 4 which allows it to combine with other atoms such as hydrogen (1 layer, 1 electron) or oxygen (6 electrons in the last layer).

**Autonomous quantum error correction (AQEC):** quantum error correction codes and architectures that doesn't require error syndrome measurement. It replaces real-time feedback by analog feedback circuits using engineered dissipation with the reservoir engineering technique. It couples the system with a dissipative reservoir to transfer the entropy created by errors to an ancillary system, the reservoir. This entropy is then evacuated via the strong dissipation of the ancilla. This technique is used in cat-qubits.

**Back action:** in quantum measurement, this is the physical impact of the measurement device on measured quantum objects. Quantum measurement usually modifies the state of the measured quantum object unless it is already in a basis state (mathematically, one of the eigenvectors of the measurement observable operator...). After measuring a quantum object state, performing the same measurement on the already measured system will not provide any additional information. In order to increase our knowledge on the final state of some quantum computation, the only solution is to start again the computation from the beginning and measure again the final state. The subtlety being that this new final state has not yet been measured and thus corresponds exactly to the one we are trying to infer. Then, we compute an average of the obtained results across several experiments. Some measurement techniques like gentle measurement or weak measurement are designed to minimize this back action and are sometimes used in quantum error correction codes.

**Balmer series:** set of four spectral emission or absorption lines with the hydrogen atom, generated by electron transitions between the second and higher energy levels of the atom.

**Beam splitter:** optical device that splits a beam of light in two. It's usually made with two glued triangular glass prisms. Polarizing beam splitters are a particular class of beam splitters that use birefringent materials to split light into two beams of orthogonal polarization states.

**Balanced beam splitter:** beam splitter where the light is equally divided in two streams.

**Baryon:** class of elementary particles of the first level of the nuclei of atoms. It contains protons and neutrons.

**Bell inequalities:** Bell's 1964 theorem proves that no hidden variable theory - imagined by Einstein in 1935 - can reproduce the phenomena of quantum mechanics. Bell's inequalities are the relations that measurements on quantum entangled states must respect under the hypothesis of a local deterministic hidden variable theory. Experiments shows that Bell's inequalities and related statistics are systematically violated, forcing scientists to give up one of the three following hypotheses on which Bell's inequalities are based. The first is the locality principle according to which two distant objects cannot have an instantaneous influence on each other, which means that a signal cannot propagate at a speed greater than the speed of light in a vacuum. The second is causality, according to which the state of quantum particles is determined solely by their experience, i.e. their initial state and all influences received in the past. The third is realism, which means that individual particles are entities that have properties of their own, carried with them ([source](#)).

**Bell test statistic:** it is a test of correlation of quantum state detection with two entangled quantum objects which can have values A and A', and B and B'. Quantum entanglement showing a correlation of the values of these two objects will yield and average value of:  $|S| = \langle AB \rangle_{lim} + \langle AB' \rangle_{lim} + \langle A'B \rangle_{lim} - \langle A'B' \rangle_{lim} = 2\sqrt{2}$  (about 2.828). In this formula,  $\langle A'B \rangle_{lim}$  is the probability to have outcome A with the first quantum object and outcome B' for the second. It's usually a photon polarization. This test is also a way to evaluate the entanglement of two qubits in quantum computers.

**Black body:** a body that is in thermal equilibrium with the radiation it emits. It can be the inside of a furnace or a star. It is by studying the radiation of the black body and its frequency distribution as a function of the body temperature that Max Planck uncovered the existence of energy quanta in 1900. Also written blackbody or black-body depending on the source.

**Blind Quantum Computing:** technique for distributing quantum processing in remote quantum processors and securing the confidentiality of the processing.

**Bloch sphere:** geometric representation of a qubit state with a vector in a sphere of radius 1. The qubit ground state is an upwardly directed vector  $|0\rangle$  and the excited state is a downwardly directed vector  $|1\rangle$ . An intermediate state vector is defined by its amplitude and phase, in

line with the wave-particle duality of the qubits. It models of the state of a qubit using polar coordinates with two angles, one indicating the amplitude of the quantum and the other its relative phase.

**Born rule:** postulate of quantum mechanics created by Max Born in 1926 giving the probability that a measurement of a quantum system will yield a given result. It states that the probability density of finding a particle at a given point, when measured, is proportional to the square of the magnitude of the particle's wavefunction at that point.

**Bose-Einstein Condensate**, or BEC, state of very low density boson gas cooled to a temperature close to absolute zero (-273.15°C) where a large part of the bosons are in the lowest possible quantum energy state and exhibit particular properties such as interferences. A special case of BEC is superfluid helium, discovered in 1938, which, at very low temperatures, has no viscosity, i.e. it can move without dissipating energy. These condensates were imagined and theorized by Satyendra Nath Bose and then Albert Einstein in 1924. Their existence was demonstrated experimentally in 1995 by Wolfgang Ketterle, Eric Cornell and Carl Wieman who were awarded the Nobel Prize in Physics in 2001. In quantum computing, this field is related to the field cold atom-based qubits.

**Boson sampling:** typical experiment with photons qubits that mixes photons in an interferometer. It's hard to emulate on a classical computer and is used to show a specific quantum advantage. The only caveat is these experiments are not programmable and are therefore entirely useless and irrelevant to compare any calculation capacity between systems.

**Boson:** particles with gregarious behavior, which can accumulate in arbitrarily large numbers and in the same state. Bosons comprise photons and composite objects with whole integer spin such as hydrogen, lithium-7, rubidium-87, carbon and silicon atoms in crystalline structures. These particles escape Pauli's exclusion principle. They have a symmetrical wave function.

**Bosonic codes:** hardware system that implement quantum error corrections with bosonic modes, using a quantum harmonic oscillator with a continuous energy levels. It includes cat-qubits, GKP codes (Gottesman-Kitaev-Preskill) and binomial codes.

**BQP** (problem class): complexity class of problems that can be handled by quantum algorithms. Means a bounded-error quantum polynomial time. It is the class of problems that can be solved in polynomial time relative to the size of the problem with a probability of obtaining an error not exceeding one third of the results. This class is positioned between the class P (problems that can be solved in polynomial time on a classical machine) and NP (problems for which a solution can be verified in polynomial time on a classical machine).

**Bra-ket** (notation): A notation model describing the state of a quantum and a qubit in the form  $|\psi\rangle$  and  $\langle\psi|$ . It was created by Paul Dirac in 1939. A bra psi vector is a quantum state described as a column vector. A ket is its transpose, a row vector. It facilitates the writing of operations

with quantum states, like inner products  $\langle\phi|\psi\rangle$ , outer product  $|\phi\rangle\langle\psi|$  and projection  $\langle\psi|A|\psi\rangle$ .

**Chandelier:** nickname of the quantum computing system located inside the cryostat of a superconducting or electron spins quantum computer. It contains several stages made of copper disks covered with gold. These disks are crossed by numerous coaxial cables that are used to drive the qubits and read their state with microwaves. It is completed by filters, attenuators and amplifiers for the microwaves that circulate in these wires, various sensors, and heat exchangers that cool the copper disks, which in turn cool the elements that are placed on them.

**Clifford group:** group of unitary quantum gates that can be easily simulated in polynomial time on classical computers according to Gottesman-Knill's theorem. A Clifford gate is a quantum gate that can be decomposed into gates of the Clifford group. It is sufficient to have one unitary gate rotating on the X axis and another on the Z axis to create a complete set of Clifford gates. They must be completed with at least one two-qubit gate as a CNOT. These gates make quarter turns or half turns in the Bloch sphere. They are not sufficient to create a universal gates set. You need non-Clifford gates like the T gate.

**Cluster state:** the starting point for an MBQC (Measurement Based Quantum Computing) calculation with a grid of embedded qubits that are usually initialized in an entangled state. Used mostly with photon qubits.

**CMOS:** a common semiconductor fabrication technique used to produce processors and memory, and which is reused to create qubits that manipulate electron spins.

**Coherence:** quantum coherence is the ability of a quantum system to demonstrate interference. The coherence between different parts of a wave function allows for the famous double-slit interference and the formation of short quantum wavepackets propagating in space. Two wave sources are coherent when their frequency and waveform (or phase for an electromagnetic signal) are identical. There are temporal coherence (same waveforms with some time delay), spatial coherence (in 2D or 3D such as with plane waves) or spectral coherence (waves of different wavelengths but with a fixed relative phase form a wave packet). In quantum physics, coherence comes with linear superposition of various states of a quantum system containing one or several quantum objects (represented by a wave due to the wave-particle duality). Quantum coherence progressively degrades naturally due to the interactions with the environment and ends after a certain time for qubits (the coherence time) and also when measuring the state of a qubit.

**Cold atoms:** atoms cooled at very low temperatures, generally with techniques using lasers and the Doppler effect. They are used in certain types of quantum computers called cold atom quantum computers. The atoms used are neutral atoms (not ionized) and quite often rubidium, an alkali metal.

**Compatible properties:** physical properties of a quantum system that can be measured in any order or simultaneously.

**Commutativity:** mathematically, two variables A and B commute when  $A \times B = B \times A$ . They do with integers but not with non square matrices. Even square matrices don't necessarily commute. They are then "noncommutative".

**Commutator or commutation operator:** Characterize the level of non-commutativity between two variables, usually matrices. For two matrices A and B, their commutator is  $[A,B] = AB - BA$ .

**Complementarity:** principle of quantum physics introduced by Niels Bohr in 1927 according to which quantum objects have certain pairs of complementary properties which cannot all be observed or measured simultaneously. These are incompatible properties. Another version of this principle is that it's not possible to simultaneously observe a quantum object as a particle and as a wave, like in the Young slit experiments.

**Complementary variables:** pairs or complementary variables or properties according to the Bohr complementary principle.

**Complex number:** set of complex numbers created as an extension of the set of real numbers, containing in particular an imaginary number noted  $i$  such that  $i^2 = -1$ . Any complex number can be written in the form  $a + ib$  where  $a$  and  $b$  are real numbers. These numbers are used in particular to describe the state of a qubit and to represent the phase of a quantum object with its complex component.

**Complexity (theory):** branch of theoretical computer science and mathematics that plays an important role in quantum computing to evaluate its performance compared to traditional Turing/Neumann machine computing. It defines classes of problems by levels of complexity, in terms of computing time or even the memory space required, with, in particular, problems that are solved in polynomial time in relation to their complexity (class P) and whose results are verifiable in polynomial time (class NP). The methods used to solve these problems are most often based on the brute force of navigating through an increasingly large space of combinations to be evaluated according to the size of the problem to be solved.

**Compton effect:** effect which demonstrates that photons can have some momentum and behave as particles, that was demonstrated by Arthur Holly Compton in 1922 with scattering of X rays and gamma rays photons by atomic electrons.

**Computational basis:** naming of the basic states of a qubits register. For a single qubit, this corresponds to the  $|0\rangle$  and  $|1\rangle$  states. For a register of N qubits, the computational basis is made of the  $2^N$  combinations of series of N 0s and 1s, named in Dirac's notation  $|000\dots000\rangle$  to  $|111\dots111\rangle$ . All these states are mathematically orthogonal with each other. A N qubits register in a pure state mode is a linear superposition of all these states using complex amplitudes.

**Concatenated codes:** describes the recursive application of error correction codes where in an error correction code, a physical qubit is replaced by a logical qubit, and so on.

**Condensed matter physics:** branch of physics that studies the macroscopic properties of matter (solids, liquids, glasses, polymers) and in systems where the number of constituents is large and the interactions between them are strong. Condensed matter physicists seek to understand the behavior of these phases using the laws of physics (quantum mechanics, electromagnetism and statistical physics). In practice, it mainly covers low temperature superconducting, ferromagnetic, antiferromagnetic and ferrimagnetic phases of spins in crystalline lattices of atoms, spin glasses, spin liquid, and Bose-Einstein condensates. Physicists working on superconducting qubits are part of this discipline.

**Conjugate variables:** pairs of dynamic variables describing the state of a quantum object, like position and momentum, that are related to the other with the Heisenberg indeterminacy principle which prevents a precise measurement of both variables.

**Continuous variables quantum computing (CV):** a type of quantum computer that uses qubits whose values are continuous and not binary. Used in two types of quantum computers: analog quantum simulators (particularly based on cold atoms) and CV photon-based systems.

**Cooper pair:** pairs of tightly coupled electrons creating electric current flow in superconducting materials, usually at very low temperatures and without resistance. Cooper pairs have an integer spin because they accumulate two electrons with a spin of  $\frac{1}{2}$ . They become bosons and can accumulate and form macro quantum objects.

**Copenhagen interpretation:** interpretation of quantum physics elaborated by Niels Bohr in Copenhagen and by Werner Heisenberg, although it was never clearly formalized. Applied to individual quantum objects, it is mostly based on Bohr's correspondence and complementarity principles, Heisenberg's indeterminacy principle, Born's probability interpretation of the Schrodinger wave function and on the wave function collapse and its fundamental indeterminism. It avoids describing any reality beyond what can be measured like an exact position of an electron. The completeness of this theory was challenged by Albert Einstein. Physicists are still debating about this interpretation, as part of the quantum foundation field.

**Correspondence principle:** principle formulated by Niels Bohr in 1920 which states that the behavior of systems described by quantum physics matches classical physics in the limit of large quantum numbers (large orbits and large energies or electron quantum numbers).

**Coulomb force:** electrostatic force between electrically charged particles like electrons and protons. Its strength is inversely proportional to the square of their distance and proportional to the product of their respective charge.

**CPTP map:** completely positive and trace preserving map or operator also referenced as a quantum channel or superoperator. It is a linear operator that turns a density matrix describing a mixed state system into another density matrix. Its size is then the square of the density matrix size, so  $2^{4N}$  for a system of N qubits. It can describe any operation on a mixed state system: some quantum

gates, any sort of measurement, quantum filters, as well as feedback networks in quantum control theory.

**Circuit quantum electrodynamics** (cQED): architecture used in solid state qubits systems using superconducting qubits and microwave photons. Science behind the interactions between microwaves and electromagnetic circuits.

**Cavity quantum electrodynamics** (CQED): field of quantum physics coupling trapped atoms in physical cavities and microwaves. It is about the interactions between photons and electrons and atoms.

**Cryogenics**: cooling technology. Very low temperature cryogeny is used with superconducting and electron spin qubits computers. The temperatures required to stabilize qubits and reduce their error rate are very close to absolute zero: around 15 mK. The most commonly used systems are dilution refrigerators that use helium-3 and helium-4. Cryogenics is also used for photon generators and photon detection systems, but at a higher temperature situated between 2K and 10K.

**CSCO**: complete set of commuting observables, the most complete measurement of a quantum system comprised of compatible properties that can be measured in any order.

**DAC**: digital-analog converter. Classical electronic device converting a digital signal into an analog signal. Is used in the microwave generation systems implemented to control superconducting and electron spin qubits.

**Dark count**: photons detected by photon detectors that come from the environment and thermal or tunneling effect. This explains why most single photon detectors must be cooled at a temperature usually below 10K.

**De Broglie wavelength**: wavelength of a particle calculated with its momentum  $p$  with  $h/p$ , with  $h$  being Planck's constant.

**Decoherence**: marks the end of the coherence of a quantum object or a qubit. It is notably caused by the interactions between the quantum objects and their environment. One often uses indifferently the expression coherence time (time during which the qubits are in a state of superposition and entanglement with other qubits) or decoherence (time at the end of which this superposition and entanglement end), which is the same.

**Degenerate**: a quantum system energy level is degenerate if it corresponds to two or more different measurable states. Mathematically, a quantum state is degenerate when several linearly independent eigenvectors may have the same eigenvalue. A normalized linear combination of these eigenvectors is also an eigenvector with the same eigenvalue. The number of linearly independent eigenvectors having the same eigenvalue corresponds to the degree of degeneracy of the quantum system. The number of different eigenstates corresponding to a particular energy level is the degree of degeneracy of the level. This happens for example when the energy level alone is not sufficient to characterize the state of a quantum system. That's where we need other quantum numbers to characterize the state. This is the case with the hydrogen atom

electron. Its energy level depends only on its principal quantum number  $n$  (the electron layer), and not the three other electron quantum numbers (orbital angular momentum, magnetic moment and spin, although this degeneracy can be broken with using relativistic quantum mechanics and hyperfine structure splitting of electron energy levels). But you also have degenerate quantum error correction codes, which are supposed to correct more errors than they actually detect, particularly with noisy quantum channels (meaning practically qubits gates).

**Density matrix**: matrix of complex numbers used to describe the statistical state of a physical system that is more precise than the computational state vector used in quantum computing. Density matrices are useful to describe so-called mixed states versus pure states that are sufficiently described with state vectors. They are used to describe what happen to subsystems of entangled systems, when decoherence happens and also, during measurement.

**Dequantization**: said about some quantum algorithm where an efficient classical equivalent is found. Term initiated with Ewin Tang's work on recommendation systems in 2018, when she found a dequantized classical equivalent to a quantum recommendation algorithm devised in 2016 by Iordanis Kerenidis and Anupam Prakash. Interestingly, quantization is a term used in artificial intelligence and deep learning when the numbers used in these models are integers (or even binary numbers) instead of floating point numbers.

**Determinism**: situation when events are determined completely by previously existing causes and parameters. Applied to classical mechanics to predict objects position and momentum based on initial conditions. Contrarily, in quantum physics, it is not possible to determine simultaneously the position and momentum of any particle at any instant. This indeterminism is observed with quantum measurement when the quantum object is in a superposed state.

**Deutsch-Jozsa (algorithm)**: quantum algorithm created in 1992 by David Deutsch and Richard Jozsa. It can check whether a given function is balanced or not, i.e. whether it always returns 0 or 1, or 0 and 1 in equal proportions. The alternative between equilibrium (as many 0's as 1's) or not (as many 0's or 1's in output) is a starting postulate. The gain in performance compared to classical algorithms is exponential. In the case of  $N$  qubits, the function should be classically evaluated on at least half of the possible input values, i.e.  $2^{N-1}+1$ . Unfortunately, this algorithm is not very useful.

**DFT (Density Functional Theory)**: mathematical model used to describe the structure of molecules at rest as a function of inter-atomic interactions. Used in high-performance computing as well as in quantum computing for chemical simulation.

**Diffraction**: phenomenon created when a wave encounters an obstacle or opening, like a small hole or slit. It is generated by the bending of photon waves around the corners of the obstacle. It creates interferences between the passing waves as they are detected in a plane further

down the waves path. The phenomenon can be described classically with the Huygens–Fresnel principle that considers points in the hole or slit as a collection of individual spherical wavelets. The interference pattern shows up with laser light and can also be explained by the photon wave functions and their probability distribution. All-in-all, you can consider that a Young single-slit experiment also create quantum interferences!

**Dilution refrigerator:** name given to the very low temperature cryostats used to cool quantum computers below 1K. They cool superconducting or electron spin chipsets to respectively 15 mK and 100 mK. Dilution is related to the use a mixture of two helium isotopes (3 and 4), which are diluted in a mixing chamber, the two isotopes having slightly different physical properties. A helium 4 cryostat only goes down to about 2.8K, a helium 3 cryostat goes down to 300mK while a cryostat using both goes down to 10mK. The most common variant is the "dry" as opposed to "wet" dilution refrigerator. This version uses less helium and leaves more space in the chandelier to house electronic and quantum devices.

**Dirac's notation:** see bra-ket.

**Dirac constant:** Planck constant divided by  $2\pi$ , also called reduced Planck constant and denoted  $\hbar$  (h-bar). Some physicists called sometimes, abusively, this constant "Planck constant".

**Discrete log problem:** mathematical problem consisting in finding a log of a number that happens to be an integer. It is used in finding the solution of cryptographic problems with quantum algorithms. Shor's dlog algorithm is a quantum algorithm solving discrete log problems.

**Distillation:** technique used in quantum error correction codes based on magic states. It consists in combining several magic state qubits to feed others with a lower error rate. Distillation has the effect of purifying the state of qubits, meaning turning mixed states into pure states.

**Doppler effect:** shift in the electromagnetic spectrum due to the speed at which the source moves away from or closer to the observer. If the source moves away from the observer, the light wavelength is shifted towards the red (redshift), otherwise towards the blue. This effect is used in particular in the technique of atoms laser cooling. It consists in illuminating atoms that are in thermal motion with a wavelength that is just below the absorption level of the atoms. Those atoms moving towards the laser beam will absorb the photon, which will reduce their kinetic energy and movement. Those atoms moving in the other direction will not absorb it because the apparent frequency of the photon will be too low to change the energy state of the atoms. As atoms get cooled, the cooling laser wavelength has to be adjusted. This technique allows atoms to be cooled to below mK (milli-Kelvin).

**D-Wave:** Canadian company designing quantum annealing computers. They do not have the same power as universal gate quantum computers with equal numbers of qubits. The current generation of D-Wave "Advantage" using Pegasus chipsets includes 5000 qubits.

**Eigenstate:** for a quantum object, these are the elementary wave functions in which it is possible to decompose it. They are represented by eigenvectors.

**Eigenvalue:** see eigenvector.

**Eigenvector:** for a square matrix A, an eigenvector x of A is a vector that verifies the equation  $Ax = \lambda x$ ,  $\lambda$  being a real number called eigenvalue. Their direction do not change once multiplied with matrix A.

**Electromagnetic spectrum:** all electromagnetic radiation from the largest radio waves to X-rays and gamma rays. Visible light is only a very small part in the middle of this spectrum. An EM wave is decomposable in a number of photons, the smallest elementary unit of an EM wave.

**Electron:** elementary particle found in atoms, orbiting the nucleus, but also in freeform traveling between atoms and creating something we know as being electric current. According to Bohr's model developed in 1913, there is a finite number of electron orbits around the nucleus of atoms. The movement of electrons from one orbit to another corresponds to the absorption or emission of a photon. Electrons are elementary particles in the standard model because it is not composed of sub-particles, unlike neutrons and protons which are composed of quarks. According to quantum physics, the electron as many other particles behaves as a particle and as a wave. Electrons are often used in qubits, in the form of electrons circulating in semiconductors loops or who are trapped in quantum dots or electromagnetic cavities and whose spin is controlled.

**Elliptic Curves Cryptography (ECC):** a type of public key cryptography that is potentially broken by Shor's quantum algorithm. One of its advantages is that it requires small keys, about three times smaller in number of bits than RSA public keys.

**Energetics of quantum technology:** cross-disciplinary research field and sector studying the energetics of quantum computing but also quantum telecommunications, cryptography and sensing. It's about making sure quantum technologies are not power hungry and also dealing with the energetic constraints related to quantum computing scalability. It's about balancing the act between cooling requirements, cabling, control electronics to ensure quantum computers can scale in number of physical and logical qubits.

**Entanglement:** quantum phenomenon where two quantum objects are related with each other in a way that a measurement done on these two objects generates a correlated (but random) value. Mathematically speaking, two quantum objects are entangled when their quantum state (psi, vector state) cannot be expressed as the tensor product of individual quantum states. This process is used to link qubits together through two or three qubit quantum gates in quantum computers. It is also used in quantum cryptography and telecommunication systems based on entangled photons in QKDs.

**Entropy:** measures the degree of disorder and randomness of a physical system. Key concept related to the second law of thermodynamics that states that the entropy

of an isolated system cannot decrease spontaneously. In quantum mechanics, the (Von Neumann) entropy of a system is  $-tr(\rho \log \rho)$  where  $\rho$  is the density matrix describing the system state.

**ERC Grants** : European Research Council grants. Funding of European research projects with several levels, the top of which is the Synergy Grant which funds "moonshots" in European research associating at least two principal investigators (PIs) from public or private research laboratories. 14M€ is the maximum funding for such a project with 10M€ of core funding and 4M€ which can notably finance heavy investments or access to large infrastructures. Other levels include the Starting grants with up to 1.5M€ for 5 years and the Consolidator grants with 2M€ also for 5 years.

**Ergodicity**: capacity of a moving system to explore all parts of the space in which it can move in, in a uniform and random manner. Happens with many physical systems like with electron. Quantum ergodicity states that in the high-energy limit, quantum objects tend to a uniformly distribute in the classical phase space.

**Ergotropy**: maximum amount of work that can be obtained from a quantum system.

**Error Correction Codes**: describes both logical methods and physical architectures to correct physical errors happening in both classical and quantum computing and telecommunication technologies.

**Errors**: a major concern in the operation of quantum computers. Operations on qubits: one and two qubit gates and qubit readouts generate errors that must be minimized. Error rates are in 2021 between 0.1% and 2% for quantum gates. When several quantum gates are chained together, the rates of correct results (1 - error rate) multiplies quickly to the point of distorting everything. This is avoided either by reducing the physical level error rate like with cat-qubits, using shallow algorithms (low number of gates) or with error correction code systems.

**Exclusion principle**: see Pauli exclusion principle.

**Expectation value**: average or mean value of a measured quantum object property. With an observable operator A on a quantum state  $\psi$ , the expectation value is  $\langle a \rangle = \langle \psi | A | \psi \rangle$ . In other words, it's a scalar product of the  $\psi$  vector and the vector resulting from the projective measurement of  $\psi$  using the observable A.

**Euclidean networks**: class of encryption algorithms used in post-quantum cryptography (PQC).

**Fabry-Pérot cavities**: equipment used in lasers that combines two parallel mirrors, one of which is semi-reflective. This contributes to the creation of the laser effect in the cavity. The length of the cavity is generally a multiple of the laser light wavelength, at least if we want to emit coherent light with photons having all the same phase. The name of the cavity comes from the French scientists Charles Fabry (1867-1945) and Alfred Pérot (1963-1925).

**FBQC**: fusion-based quantum computation, a variant of MBQC crafted by PsiQuantum that is based on micro-

clusters states with groups of 4 qubits connected together and using Resource State Generators (RSGs). It's replacing measurement of entangled states in MBQC with double measurement of non connected adjacent qubits to create entanglements between them.

**Fermions**: particles with individualistic behavior. Two particles of this type cannot be in the same state at the same place. This includes electrons, quarks, half-integer spin composite objects. For example deuterium, lithium-6, potassium-40 atoms (source: Jean Dalibard). In contrast, integer spin bosons such as photons and some atoms can accumulate in the same state. In a word, bosons are communists and fermions are ultra-liberal.

**Fine structure**: splitting of an energy level or spectral line into several distinct components that take into account electron spins and relativistic corrections to Schrödinger's wave equation.

**Fluxonium**: variation of flux superconducting qubit. It has a better coherence time than transmon, above 100 μs but two-qubit gates are more difficult to implement and this architecture seemingly has not yet been tested beyond 10 functional qubits.

**Flying qubits**: qubits that can move, as opposed to stationary qubits that do not move. They are usually photons but there's a small branch of flying qubits studying flying electrons.

**Fock space**: mathematical object of algebra used to describe the quantum state of a set of identical particles whose number is variable or unknown. It is a Hilbert space made up of the sum of the tensor products of Hilbert spaces for the particles that make up the set.

**Fock state**: defines a group of quantum objects, like photons, who have the same quantum numbers and are indistinguishable. They are defined by their number, a photon number in the case of photons, and their common quantum numbers describing the quantum objects state.

**Fourier Transform**: mathematical decomposition of a time domain signal into elementary single frequency signals with their frequency, amplitude and phase. It is a complex value function of time with, for each frequency, a magnitude (real part) and a phase offset (complex part) of the sinusoid of this elementary frequency. The inverse Fourier transforms that frequency decomposition function back into its original compound signal.

**FPGA**: Field Programmable Gate Arrays. Integrated circuit where some or all functions can be dynamically defined and programmed on-demand. It can have analog and digital features. Modern FPGAs also embed full-fledged processing units (Arm cores, GPUs, neural processing units, networking units). FPGAs are used in qubit control electronics for reading out the signals coming from the resonators attached to superconducting and electron spin qubits. It measures the phase and amplitude of the reflected microwaves after they are converted from analog to digital with an ADC (analog-digital converter) that can be embedded in the FPGA.

**Fredkin gate**: quantum gate operating on three qubits that inverts the state of the second and third qubit if the

first qubit is 1. Also called CSWAP gate (conditional SWAP).

**FTQC**: Fault-Tolerant Quantum Computer. Error-resistant quantum computer that is based on logical qubits made of many physical qubits and implementing quantum error correction. Fault-tolerance is based on the error correction making sure errors don't propagate to many qubits.

**Gate-based quantum computing**: the broader category of quantum computing system based on qubits and quantum circuits implementing quantum gates on 1, 2 and 3 qubits at a time.

**Gaussian state**: describe particular photon states that are classical. The gaussian curve is the form in three dimensions of Wigner's function which describe the phase and amplitude distribution of the photon. It is opposed to non-gaussian states which are non-classical, with some negative Wigner function values and a non-Gaussian form for the 3D function.

**GHZ**: means something other than giga Hertz in quantum computing! It is a three-qubit Greenberger-Horne-Zeilinger superposed state that allows to demonstrate the inexistence of hidden variables in the quantum entanglement of at least three particles and with a finite number of measurements. The concept dates back to 1989 and has been experimentally validated in 1999.

**GKP qubits**: error corrected qubits according to a method proposed by Gottesman, Kitaev and Preskill. Can be produced by Gaussian boson sampling (GBS) devices.

**Gleason's theorem**: according to Andrew M. Gleason's theorem proved in 1957, the functions assigning probabilities to measurement outcomes are projection operators that must be expressible as density operator and follow the Born rule. This determines the way to calculate probabilities and the set of possible quantum states.

**GPGPU**: General Purpose Graphical Processing Unit, used for simulation and machine learning bound GPUs like the Nvidia V100 and A100. These are coprocessors which are mostly not anymore used for graphics software but more for machine and deep learning and scientific computing, thus the "general purpose" nickname addition.

**Grotian diagram**: diagram used to show the various electronic energy transitions for a given atom, introduced in 1928 by the German physicist Walter Grotian. The indicated frequencies of transitions to higher energy levels provide an indication of their source like lasers (in the hundreds of nm wavelengths) or microwaves (in the 4-20 GHz frequency regimes).

**Ground state**: lowest energy state of an atom, other states being excited states. The hydrogen atom ground state happens when its electron occupies the lowest energy level (with main quantum number = 1). More generally, is said of a qubit that is in its ground basis state  $|0\rangle$ .

**Grover** (algorithm): quantum algorithm for finding an element in a non-indexed array or a unique element for which an oracle function returns 1.

**H-bar**: see Dirac constant.

**Hadamard** (gate) : quantum gate creating a superposed state between  $|0\rangle$  and  $|1\rangle$  in a qubit when starting with  $|0\rangle$  or  $|1\rangle$ .

**Hamiltonian**: equation describing the total and potential energy of a system of quantum objects. It is the global operator of the right part of Schrödinger's equation. This notion is used in D-Wave quantum annealing computers and with quantum simulators. "Preparing a Hamiltonian" in this kind of computer is equivalent to setting up a matrix of qubits linked together by potentials and which will seek a minimum energy resulting in a balanced Hamiltonian corresponding to the solution of the problem to be solved. The solution is about finding the right combination of qubits states (up/down for quantum annealing) that minimizes the energy of the whole system.

**Hamming distance**: metric used to compare two binary data strings of equal lengths. It is the number of bit positions in which the two bits are different. For two strings  $a$  and  $b$ , it is denoted as  $d(a,b)$ .

**Harmonic oscillator**: in classical mechanics, system that, when displaced from its equilibrium position, experiences a restoring force proportional to its displacement  $x$  with a frequency that does not depend on the amplitude. Quantum physics formalize the whereabouts of many harmonic oscillators including photons in cavities, superconducting qubits, phonons, diatomic molecules, etc.

**Hartree-Fock**: method to compute atomic structures using the time dependent Schrödinger's wave equation.

**Heisenberg** (principle of indeterminacy): fundamental principle of quantum mechanics which postulates that there is a lower limit to the precision with which one can measure two independent parameters relating to the same object such as its speed and position or the energy emitted and the duration of emission.

**Heisenberg limit**: in quantum metrology, like with interferometry, the optimal rate at which the accuracy of a measurement can scale with the energy used in the measurement. More precisely, not every quantity is a quantum observable that can be measured directly. The estimation of such quantity, however, can be performed by measuring a state whose probability distribution depends on it. To evaluate the accuracy of this estimation, one often considers the variance of the estimated quantity. When using, for instance, an ensemble of photons as the meter probing our parameter of interest, if these photons are allowed to be initially entangled, then this variance is lower bounded by the fundamental Heisenberg limit. As for the standard quantum limit, it implies that the more resources, the more accurate the measurement. However, only quantum probing resources can reach the Heisenberg limit which states that our estimation's standard deviation is at best inversely proportional to the size of the meter, hence here the number of photons.

**Helium 3**: a rare isotope of helium that is used in cryogenic quantum computer systems to generate temperatures below 1K as part of dilution refrigeration systems. It is usually produced from tritium in specialized nuclear

power plants, including the US Department of Energy's Savannah River nuclear power plant.

**Helium 4:** a common helium isotope that is also used in cryogenic systems.

**Heralded single-photons:** pairs of single photons can be generated in highly correlated states from using a single high-energy photon to create two lower-energy ones. One photon from the resulting pair is detected to "herald" (or "signal") the other so its state is pretty well known prior to its own detection or whereabouts. The two photons need not be of the same wavelength, but the total energy and resulting polarization are defined by the generation process. Two commonly types of heralded single-photon sources are SPDC (spontaneous parametric down-conversion with line width in the THz range) and SFWM (spontaneous four-wave mixing with line width in the MHz range or even narrower). It's used with QKD.

**Hilbert** (space): vector space of real or complex numbers with an Euclidean or Hermitian scalar product, which is used to measure distances and angles and to define orthogonality. It is an n-dimensional extension of the concept of three-dimensional Euclidean space. In quantum mechanics, the state of a quantum is represented by a vector in a Hilbert space with as many dimensions as the number of basic (or observable) states of this quantum. These are geometrical spaces which are used in particular to measure lengths and angles, to make projections on dimensions and to define the orthogonality between vectors.

**Hidden variables:** interpretation proposals of quantum physics based on the use of (yet) unobservable hypothetical entities what would explain phenomena like entanglement and describe reality. Bell's theorem implies that local hidden variables of certain types cannot exist. Based on the assumption, promoted by Albert Einstein in the famous 1935 EPR paper, that quantum physics is an incomplete theory.

**Homodyne detection:** method used for extracting information encoded as modulation of the phase and/or frequency of an oscillating signal. It compares that signal with a standard oscillation carrying no information. Homodyne amplifies using a single frequency while heterodyne detection uses dual frequencies. In quantum technologies, homodyne detection is used with photonics as well as with superconducting qubits.

**HPQC:** High Performance Quantum Computing, a quantum analogue of HPC (High Performance Computing). These are currently theoretical models of quantum mainframes comprising giant matrices of qubits that can be partitioned for shared use by several users. See [High Performance Quantum Computing](#), 2011 (7 pages).

**Hubbard model:** physics simulation model of mixed conducting and isolated systems based on a simple Hamiltonian. Mentioned in the sizing benchmark used by Amazon for its cat-qubits fault-tolerant quantum computing system being currently designed.

**Hybrid quantum algorithm:** an algorithm that combines classical processing running on classical computers and some processing performed on quantum computers, where needed.

**Hyperfine structure:** small splitting of atomic energy levels or spectral lines with electrons with the same quantum numbers into several distinct components that are explained by the interactions between the nucleus and electron clouds.

**Indistinguishability:** relates to bosons quantum objects that have the same quantum state in a given location and are impossible to separate with any measurement tool.

**Integrated Quantum Photonics** (IQP): technologies exploiting photons as quantum information carriers and implemented on chipsets using wafer-scale fabrication, mostly in silicon-based CMOS or with III/V materials like gallium arsenide (GaAs) and indium phosphide (InP). IQP is used in quantum telecommunications and computing. It is using optical waveguides to guide and route single-photons, provides miniaturized split and phase control circuitry, entangled state generation, overall manipulation and sometimes even photons generation and photons detection.

**Interference:** fundamental phenomenon of quantum physics used with the wave aspect of quantum objects, when several waves can add or annihilate with constructive and destructive interferences. Is the basis of gate-based quantum algorithms!

**Invertible computation:** involves computations that run both forwards and backwards so that the forward/backward semantics form a bijection. In classical computing, it can correspond to some symmetric logical circuits that can process data forward and backwards with both ends used as inputs and outputs. It's used for example in MemComputing classical processors. The principle was created by Supriyo Datta from Purdue University in Indiana, USA.

**Irreversible:** said in computing of a calculation that makes it impossible to compute the initial values with using the result of the calculation. This is the case with all two-classical bits gates (NOR, OR, AND). Contrarily, quantum computing gates are mathematically reversible since relying on unitary transforms that, multiplied with their transconjugate, generate an identity operator. In plain language, if you apply an unitary (set of quantum gates) to a set of qubits, you can reverse this computing with the transconjugate of this unitary. Practically, it means playing in reverse order the gates initially applied. This technique is used in the uncompute trick that we describe elsewhere.

**Ion:** non-neutral atom, which has a positive or negative electric charge. It is negative if its number of electrons exceeds the number of protons (anions) and positive in the opposite case (cations).

**IonQ:** an American startup from the University of Maryland that pioneered the first commercial quantum computers using ion traps. Their operational record as of 2021 was 11 qubits with 32 qubits to be made readily available.

**Ising** (model): a statistical physics problem that can be simulated and solved using quantum algorithms, especially on quantum annealers like those from D-Wave. It models the interactions between two-level particles (spin, ferromagnetism). All algorithms for D-Wave annealers are reduced to solving an Ising model.

**Isotopes**: variations of atoms where the number of protons and electron is the same, sharing the same atomic number, but when the number of neutrons is different. For example, helium can exist in the for He<sup>3</sup> and He<sup>4</sup> with one and two neutrons. Many materials involved in quantum technologies are used with particular isotopes, like Si<sup>28</sup> in silicon wafer used with electron spin qubits, the reason being the number of neutrons has an influence on atom nucleus spins, that can interfere with their electron spins.

**Josephson** (effect): physical phenomenon happening in a superconducting current loop traversing a thin insulating barrier known as a Josephson junction (JJ) like some non-superconducting metal thanks to the tunneling effect. It enables the creation of a multiple level energy or phase state for the superconducting current. This technique is used in superconducting qubits from quantum systems such as those of IBM and Google. It is also used in quantum sensing with SQUIDs (superconducting quantum interference devices) that are used as very sensitive magnetometers.

**Kerr effect**: when some materials refractive index is modified in a non-linear (quadratic) manner as a function of the electric field applied to them. Is a variant of Pockels effect.

**Ket**: vertical vector describing in Dirac's notation the state of a quantum object. It contains complex number amplitudes defining the relative weights in the computational basis. For a qubit, it's a 2 complex numbers vector. For a register of N qubits, it's a 2<sup>N</sup> size vector of complex numbers defining the amplitudes of each combination of N 0s and 1s, which are orthogonal states in the 2<sup>N</sup> state vector Hilbert space.

**Kochen-Specker theorem**: no-go theorem that states that it is impossible to assign simultaneously values with certainty to all observables in all possible contexts. This simple observation contradicts classical physics, where such an assignment is quite possible. It is the formal proof of quantum contextuality.

**Larmor frequency**: frequency of the Larmor precession (magnetic moment rotation). It is frequently mentioned in papers related to electron spins qubits.

**Larmor precession**: rotation of the magnetic moment of an object like an electron when it is exposed to an external magnetic field. This rotation happens along the axis of the magnetic field.

**Laser**: coherent light source invented in 1960 and used in many fields such as CD and DVD players, fiber optic communications, surgery, ophthalmology and dentistry, LiDARs. They are also often found in quantum computing to control cold atoms or manage photon-based qubits as well as in quantum cryptography and telecommunications (QKD & co). Laser means Light Amplification by

Stimulated Emission of Radiation. It is a source of coherent light, i.e. it consists of photons of the same polarization, phase and wavelength, and emitted in the same direction in a narrow beam. Light amplification uses a process of stimulated emission in an amplifying active medium made of solid, fiber, liquid, gas or semiconductor which is placed in the center of a resonant optical cavity with a reflecting mirror on one side and a semi-reflecting mirror on the other side, which allows the light beam to exit. The wavelength and power of the light radiation depends on many parameters. The energy comes from an excitation or pumping system: primary laser, laser diode, flash lamp or electric discharge.

**Linblad equation**: equation describing the time evolution of the density matrix  $\rho$  of a quantum system that preserves the laws of quantum mechanics, meaning it preserves the trace and positiveness of the matrix. But the transformation is usually not a unitary due to decoherence. Also named a Lindbladian, a quantum Liouvillian, and in the long form, a Gorini–Kossakowski–Sudarshan–Lindblad equation (GKSL equation, for Vittorio Gorini, Andrzej Kossakowski, George Sudarshan and Göran Lindblad).

**Linear algebra**: branch of mathematics that is used in quantum physics and quantum computing. It is based on the manipulation of vectors and matrices within Hilbert spaces. In particular, the state of a sets of qubits is represented by vectors in a Hilbert space of size 2<sup>N</sup> when N is the number of qubits. Computing with qubits consists in applying linear transformations.

**Linear optics**: field of quantum mechanics that manipulates photons based on their classical properties: polarization, phase or frequency.

**Locality** (principle): in classical physics, principle according to which distant objects cannot have a direct influence on each other. An object can only be influenced by its immediate environment. This principle derived from Albert Einstein's restricted relativity is questioned by quantum mechanics, non-locality and quantum entanglement observed experimentally since at least 1982 with photons, in Alain Aspect's famous experiment (with Philippe Grangier and Jean Dalibard). But there are various interpretations of quantum physics which explain entanglement without resorting to non-locality.

**Logical Qubit**: an assembly of physical qubits implementing hardware and software quantum error correction. Seen from the software developer's point of view, it creates a virtual logical qubit with a very low error rate. The fidelity of logical qubits depends in particular on the number of physical qubits they contain, the quality of the error correction codes and the qubits fidelity stability with the increase in the number of physical qubits.

**LSQC**: Large Scale Quantum Computing also frequently called FTQC for fault tolerant quantum computing. Category of future fault tolerant quantum computers. These will be based on the use of numerous physical qubits assembled into logical qubits with a very low error rate as seen from the software. Precisely, an LSQC implementing fault-tolerance has error corrections codes with at

least two characteristics: it must not propagate errors broadly in the physical qubits and it must be able to implement non-Clifford group qubit gates like the single qubit gate T or the three qubits gate Toffoli.

**Magic states distillation:** process that converts a set of noisy qubits into a smaller number of qubits with a lower noise. It is particularly useful for non-Clifford group quantum gates that bring universal computing power and exponential speedup. It is one of the ways to create fault-tolerant quantum computers but it has a high overhead cost with physical qubits. It was proposed in 2004 by Emanuel Knill, Sergey Bravyi and Alexei Kitaev.

**Majorana fermion:** an electron-based quasiparticle in superconducting materials that could be used to manage reliable qubits in so-called topological computing. This virtual particle was imagined by Ettore Majorana in 1937. Microsoft intends to build a quantum computer based on these quasiparticles. But their very existence has not yet been really demonstrated.

**Matrix:** mathematical object made of rows and columns of values.

**Matter wave:** principle of quantum physics enacted by Louis De Broglie in 1924 according to which massive objects can also behave as waves. The De Broglie wavelength of a massive particle is the Planck constant divided by its momentum.

**MBQC:** Measurement Based Quantum Computing, a quantum computing method invented in 2001 by Robert Raussendorf and Hans Briegel that uses a high number of groups of pre-entangled qubits, called cluster states, embedded in two-dimensional grids in which qubit state readouts modify the grid structure and help create quantum gates. The last measured qubit gives the result of the algorithm. This technique is particularly useful with flying qubits like photons because it can be implemented in a highly parallel way and support the finite depth of quantum gates that these qubits enable.

**Mode-locked laser:** pulse laser generating streams of very short pulses of light formed of wave-packets in the picosecond to femtosecond range. These pulses are generated thanks to the emitted photons being synchronized in phase. A synonym of mode-locked is phase-locked!

**MVP:** Minimum Viable Product. Concept used mostly in startups consisting in creating the most simple form of a product before starting to sell it. Opposite to full-fledged product with tons of R&D and an ever-lasting perfectionist approach.

**MINLP:** Mixed Integer Non Linear programming, a class of complex problems that can potentially be solved with quantum algorithms. It is about finding the minimum(s) of non-linear functions and under constraints that aim to respect non-linear functions. The variables in the equation are a combination of integers and floating-point numbers. The applications are numerous in all cases where one seeks to optimize a constrained function (energy distribution, optimum take-off of an aircraft, optimization of financial portfolio, minimizing risk in insurance or credit, etc.).

**Mixed state:** quantum objects state that is a classical statistical combination of several pure states. They can be prepared with physically associating several sources of pure states, like with merging two laser beams in one beam. A subsystem of an entangled quantum objects system is also a mixed state. A mixed state is mathematically represented by a density matrix operator, providing all the information that can be obtained about the related quantum system.

**Momentum:** physical property of an object or particle that for a massive particle is equivalent to its mass multiplied by its velocity. Usually denoted p. A (massless) photon has a momentum equal to their wavelength multiplied by Planck's constant.

**Multimode:** said of an optical fiber with a larger core (about 50 to 62  $\mu\text{m}$ ) where several light beams can be transported, usually with different wavelengths. Light propagation use bouncing inside the fiber walls. These fibers are used for short distances communications of less than a kilometer and with bit rates reaching 200 GBit/s. The contrary of multimode fibers are monomode fibers. Also said of multimode photons, with an entirely different meaning and a way more complicated one, never explained in plain language by quantum photonicians. Its contrary is single mode photons. A single mode photon has one complex amplitude while a multimode photon is a mixed state of single mode photons with several independent complex amplitudes. If you want to know more, you get to use a complicated mathematical formalism.

**NISQ:** Noisy Intermediate-Scale Quantum, a name for current and near future gate-based quantum computers, which are intermediate in terms of number of qubits (a few tens to hundreds) and subject to quantum noise that limits their capabilities. This acronym was created by John Preskill.

**Non-Clifford gates:** said of quantum gates that are outside the Clifford group itself based on combining Pauli gates (half-turns in Bloch's sphere), Hadamard gates (quarter turns) and CNOTs for entanglement. To make things simple, non-Clifford gates enable the creation of arbitrary rotations in Bloch's sphere and their multi-qubits gates derivatives. The single qubit T gate (one eighth turn in Bloch's sphere) is the minimum additional gate, that, combined with the others, enable by approximation the creation of any arbitrary gate and unitary transformation.

**Non cloning theorem:** prohibits the identical copy of the state of a quantum. As a consequence, it is impossible to copy the state of a qubit to exploit it independently of its original. Any copy destroys the original !

**Non-linear optics:** field of optics where the optical properties of materials depend on the light amplitude and lead to the creation of new frequencies. Non-linearity qualifies the response of a medium to an excitation that is generally quite energetic from intense fields, mainly from lasers, especially femtosecond pulsed lasers. In this case, the response of a material to the sum of two electromagnetic fields is not equal to the sum of the response to each individual field. Non-linear optics can be used to create

two-photon quantum gates with continuous variables photons.

**Non-locality:** principle allowing a (quantum) object to influence the state of another (quantum) object at a distance, which can be very large. Contradicts the principle of locality, which means that an object can only influence another object at close range. Photons quantum entanglement at great distances verifies the non-locality. However, the initial quantum state of both objects is always random. So it doesn't transmit a predetermined information per se from one place to the other.

**NMR:** Nuclear Magnetic Resonance, a type of qubit that was investigated in the 1990s and early 2000s and was then nearly abandoned. The reason is it didn't scale well at all and these were very noisy qubits and difficult to entangle. It was based on exploiting quantized states of atoms nuclei spins. However, the Chinese startup SpinQ is offering a desktop NMR-based quantum computer with 2 to 5 qubits. It's useful only for educational tasks.

**Non-classical light:** forms of light and electromagnetic fields treated as quantum systems. It contains single photon wave packets, pairs of entangled photons and squeezed states of light.

**NP** (problem class): class of problems whose solution is verifiable in a polynomial term relative to the size of the problem. Includes in particular the so-called exponential or intractable problems, whose solution time is exponential with respect to their size. A quantum computer is supposed to solve some NP problems in a tractable way, meaning, not exponential time.

**NP-complete** (problem class): decision problem for which it is possible to verify a solution in polynomial time and for which all problems of the NP class are reduced to it via a polynomial reduction. This means that the problem is at least as difficult as all other problems of the NP class. The problems of the traveling salesperson and the knapsack problem are Complete NP problems. The concept dates from 1971 and comes from Stephen Cook.

**NP-difficult** (problem class): problem to which any problem of the NP class can be reduced by a polynomial reduction. If it is also in the NP class, it is said to be an NP-complete problem. If  $P \neq NP$ , then NP-difficult problems cannot be solved in polynomial time.

**Observable:** equivalent in quantum mechanics of a physical quantity in classical mechanics, such as position, momentum, spin or energy. In quantum physics, an observable is a mathematical operator used for the measurement of one property.

**Optical molasses:** gas of cold neutral atoms whose cohesive strength is of the viscous type.

**Optical pumping:** technique used to modify the states of atoms by increasing their energy level using polarized photons. Alfred Kastler, invented it in 1950 and was awarded the Nobel Prize in Physics in 1966. The technique is used in lasers and quantum sensing. Optical pumping passes through three to four energy levels of atoms ( $E_0, E_1, E_2, E_3$ ). Pumping moves an atom from its

fundamental level  $E_0$  to  $E_3$ . A (mechanical) relaxation brings the atom back from the  $E_3$  state to  $E_2$ . In lasers, this generates a population inversion between the  $E_1$  and  $E_2$  states, so that there are more atoms in the  $E_2$  state than in the  $E_1$  state. The spontaneous and stimulated emission of photons of  $E_2-E_1$  energy can then take place. The atom in the  $E_1$  state then returns to the  $E_0$  state by relaxation.

**Orbital angular momentum** (OAM): is one of the two angular momentum of photons with spin angular momentum. Discovered in 1992 by Les Allen et al from Leiden University, this phenomenon is more difficult to visualize than spin angular momentum. With OAM, the photon itself is rotating along its propagation axis or vector. One analogy with the Earth is its own rotation (spin angular momentum, defining days) and its rotation around the Sun (orbital angular momentum, defining years). This orbital angular moment is quantified with integers times the reduced Planck constant. It can be any integer! One record OAM number of 10.100. Being quantified, it can lead to superposition and entanglement. It can also be used to encode information on fibers.

**P** (problem class): problem that can be solved in polynomial time with respect to its size, on a deterministic Turing machine.

**Pauli** (exclusion principle): postulates that two fermion particles cannot be in the same quantum state. Two electrons or two neutrons cannot be in the same place with the same energy level. If an external force such as gravitation forces them to be in the same place, they cannot have the same energy, i.e. the same speed. If a set of fermions has to be in the same place, they will have to have different velocities. Fermions have half-integer spins.

**Permanent:** real number resulting from  $n!$  additions of multiplications of  $n$  values of a square matrix  $n \times n$ . They are used to evaluate the complexity of matrices representing graphs.

**Phase Estimation Algorithm:** algorithm created by Alexei Kitaev in 1995 and used to find the phase of an eigenvector of a unitary operator  $U$ . This algorithm is based on an inverse QFT. It is used as part of period finding in Shor's factoring algorithm and in quantum chemistry algorithms.

**Phase:** an important physical properties of quantum objects given they all can behave as waves. It explains interferences between all sorts of quantum objects, like electrons on top of photons.

**Phasor diagram:** two dimensional diagram describing electromagnetic field quadratures positioning the statistic characteristics of a photon source, with  $X_1$  and  $X_2$  orthogonal axis corresponding to two oscillating electric fields that are out of phase by  $90^\circ$ .

**Phonon:** collective excitation in a periodic, elastic arrangement of atoms or molecules in condensed matter, specifically in solids and some liquids. In quantum information technologies, it is mostly used with trapped ions to provide a n-to-n connectivity between qubits.

**Photoelectric effect:** emission of electrons from a material like a metal when electromagnetic radiation above a certain minimum frequency strikes it, independently of its intensity. Formalized by Albert Einstein in 1905.

**Photon:** quantum of energy associated with electromagnetic waves ranging from radio waves (long waves, low frequencies) to gamma rays (very short waves, very high frequencies) through visible light. Its mass is zero. Its spin is 1 and it is therefore part of the bosons. Photons are absorbed or emitted by atoms during energetic levels changes.

**PKI:** Public Key Infrastructure, set of roles, policies, hardware, software and procedures used to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

**Planck constant:** fundamental constant of quantum physics ( $h=6.626 \times 10^{-34}$  Js). Created in 1900 with Max Planck's explanation of black body radiation spectrum and then used in most other quantum physics equations, including Schrodinger's wave equation.

**Pockels effect:** effect used in optical modulators where a medium refraction index changes in a linear manner as a function of the electric field applied to it.

**Polarized Beam Splitter (PBS):** class of beam splitters that use birefringent materials to split light into two beams of orthogonal polarization states.

**Polaritons:** quantum quasi-particles with strong interactions between light and matter in semiconductors. It results from the coupling between photons and an electrical polarization wave which occurs in particular in plasmons (oscillations of free electrons in metals), phonons (oscillations of atoms, especially in crystalline structures) and excitons (pairs of electron holes generated by photons in semiconductors).

**POVM:** Positive Operator-Valued Measure, quantum measure generalizing Projection-Valued Measures (PVMs) which is useful when the measurement basis is not made of orthogonal states in their Hilbert space. POVMs that are not PVMs are called non-projective measurements. They have many use cases like enhancing quantum states tomography, help detect entanglement and allow unambiguous state discrimination of non-orthogonal states, with applications in quantum cryptography and randomness generation

**PQC:** Post Quantum Cryptography, cryptography resistant to quantum computers-based codebreaking algorithms. It is based on the use of public keys that are not decomposable with conventional or quantum computers.

**PQS:** Programmable Quantum Simulator, or analog quantum computers.

**Private Key:** key used in private key encryption systems. Keys are exchanged beforehand by the parties using an encryption algorithm, often hash or Diffie-Hellmann algorithms.

**Property:** physical characteristic of a physical object. In quantum physics, observables are the mathematical operator used to compute properties values using the quantum

object state vector. For a photon, it can be for example its phase, polarization and wavelength. In quantum physics, it's not possible to evaluate the values of all properties of quantum systems to describe it, due to Bohr's complementarity principle.

**Public key:** an encryption system that involves sending a public key to an interlocutor who will use it to encrypt a message sent in the other direction. The elements used to create this public key are used to decrypt the message sent. It is normally impossible or very difficult to decompose the public key to find the elements that were used to create it. PQCs are based on public keys.

**Pure state:** quantum state of an isolated quantum system of one or several objects constructed as a linear superposition of the states from its computational basis.

**PVM:** Projective Value Measurement, used in quantum computing, consists in doing a geometrical vector projection of your qubit pure state on any axis in the Bloch sphere.

**Q factor:** dimensionless value defined as the ratio of energy stored in a qubit resonator electromagnetic field to the loss per period of oscillation T, multiplied by  $2\pi$ . It is linked to cavity losses. The higher the better, this factor can exceed  $10^7$ . It depends on the materials and structure of the electromagnetic cavity. It can help compare the quality of superconducting qubits and cat-qubits. High Q factor qubits are labelled "high-Q". Another definition for Q factor for an oscillator is the ratio between the main resonance frequency and its bandwidth.

**QCaaS:** quantum computing as a service, a fancy acronym for quantum computing running in the cloud.

**QFHE:** Quantum Fully Homomorphic Encryption. A method of quantum information encryption allowing to perform processing on encrypted data.

**QFT:** Quantum Fourier Transform. Quantum variation of the Fourier transform. The classical Fourier transform allows to decompose a signal (as in audio) into frequencies (or frequency spectrum). The QFT does this on a sequence of integers and determines its largest observable frequency.

**QIP:** Quantum Information Processing, a name sometimes used to information tools based on second-generation quantum technologies. It contains quantum computing, quantum simulation, quantum cryptography and quantum telecommunications.

**QKD:** Quantum Key Distribution, a secure protocol for sending symmetrical keys via an optical link based on quantum entanglement (fiber or satellite). These keys are tamper-proof, or at least an interception of the key is detectable.

**QLM:** Quantum Learning Machine, name of the Atos quantum emulator appliances using classical hardware (Intel and/or Nvidia).

**QMA:** Quentin Merlin Arthur, a class of problems that is verifiable in polynomial time on a quantum computer with a probability greater than 2/3. It is the quantum analogue of the "traditional" NP complexity class. QML: Quantum Machine Learning. Branch of quantum algorithms used in machine learning.

**QML:** Quantum Machine Learning. Class of quantum algorithms implementing machine learning or deep learning techniques.

**QRNG:** Quantum Random Number Generator, the optical random number generators used in quantum cryptography, like those of the Swiss IDQ.

**Quantization:** in quantum physics, happens with quantum objects having some physical properties that are discontinuous and not continuous, like electron energy levels and electron spins.

**Quantum accelerator:** quantum computer used as a complement to a supercomputer or HPC, usually to run hybrid algorithms like VQE (Variational Quantum Eigensolvers) combining a classical part that prepares the data structure that feeds a quantum accelerator.

**Quantum advantage:** occurs when a quantum computer executes some processing faster than its optimum equivalent adapted to a supercomputer, with a useful algorithm. This advantage can be declined on another aspect than the duration of the calculation. For example, a quantum energy advantage relates to energy consumption instead of computing time.

**Quantum annealing:** technique used to find the global minimum of a given objective function over a given set of candidate solutions, based on using quantum fluctuations. It is used to solve combinatorial optimization problems with a discrete search space. This computational process is in D-Wave quantum computers.

**Quantum channel:** transformation of a quantum state resulting from any kind of interaction with a quantum environment. It is modelized with a density matrix superoperator. It is useful to modelized subsystems, decoherence, quantum error correction and qubits noise .

**Quantum Chaos:** branch of physics studying how chaotic classical dynamical systems can be described with quantum theory. It deals with the relationship between quantum mechanics and classical chaos and with the boundaries between classical and quantum physics in modelling chaos.

**Quantum chromodynamics:** describes the strong interaction, one of the four fundamental forces, that governs the interactions between quarks and gluons and the cohesion of atomic nuclei. Why "chromo"? Because we describe the states of elementary particles with color codes: blue, green and red for particles, then anti-blue, anti-green and anti-red for anti-particles. This theory is based on the quantum field theory. This part of quantum physics is not used in the creation of qubits. It is used for the physics of elementary particles and is verified in large particle accelerators such as the CERN LHC in Geneva.

**Quantum cognition:** descriptive model of the functioning of human knowledge (language, decision-making, memory, conceptualization, judgment, perception) based on the mathematical formalism of quantum mechanics, proceeding mainly by analogy, without going through physical explanations or quantification of the neurosciences, which themselves fall within the "quantum mind" field resulting from the work of Roger Penrose.

**Quantum dots:** we can mention at least three different types of quantum dots: the powders used in LCD screens that convert the blue backlighting LED light into green or red light based on their grain size. Then we have the quantum dots used to generate single photons. At last, we have quantum dots used to trap electron spins in spins qubits.

**Quantum Electro-Dynamic (QED):** branch of quantum physics, or QED, which is "*a physical theory that aims to reconcile electromagnetism with quantum mechanics using a relativistic Lagrangian formalism. According to this theory, electric charges interact by photon exchange*" (Wikipedia). This is the basis of the quantum field theory which applies to all elementary particles.

**Quantum emulator:** a software and/or hardware system using a conventional computer to run and test some software programmed for a quantum computer. This makes it possible to test quantum programs without a quantum computer. The execution speed is not as good as on a quantum computer as soon as you exceed a few tens of qubits. And beyond about fifty qubits, the capacity of classical machines is insufficient to perform it properly. Emulation should not be confused with quantum simulation, which simulates quantum physics phenomena with an analog quantum processor like those using cold atoms.

**Quantum engineering:** is about developing quantum technologies in computing, telecommunications, cryptography and/or sensing with a pluridisciplinary approach merging quantum physics and other related sciences and technologies like thermodynamics, cryogeny, electronics, semiconductors, cabling, mathematics, information theory, programming and the likes.

**Quantum foundations:** branch of science philosophy that aims to build some understanding and description of the real world in quantum physics and, as such, associate it to some ontology.

**Quantum gates:** operations modifying the state of one or several qubits. Multi-qubit gates (Toffoli, Friedkin, ...) exploit the principle of quantum entanglement. The operations of quantum gates are generated by physical actions on the qubits which depend on their nature. For superconducting qubits, this involves sending microwaves between 5 and 10 GHz via electrical conductors. For trapped ions, these are laser-controlled operations. For electron spins qubits, these are a mix of electrical voltages and microwave pulses. For qubits based on mass particles (electrons, ions, cold atoms), quantum gates act on the qubits but these do not move in space. For flying qubits based on photons or electrons, these circulate and cross quantum gates which modify their state (phase, frequency, or other).

**Quantum hydrodynamics:** studies the hydrodynamic effects of quantum systems such as superfluid elements (helium at very low temperature) or polaritons and associated light fluids.

**Quantum Internet:** marketing term describing a quantum network enabling the quantum telecommunications based on entanglement, particularly to connect quantum systems like quantum computers and quantum sensors. By extension, it also includes quantum key distribution infrastructures that are used to secure information exchange with encryption keys that are shared quantumly between senders and receivers.

**Quantum medicine:** in general, false science and charlatanism based on a totally fanciful interpretations of quantum mechanics.

**Quantum Non Demolition measurement** (QND): type of measurement in which the uncertainty of the measured observable does not increase from its measured value during the subsequent normal evolution of the system. QND measurements are the least disturbing type of measurement in quantum mechanics. In other words, for a qubit, it would mean that after a  $|0\rangle$  or  $|1\rangle$  is measured, subsequent measurements will always yield the same  $|0\rangle$  or  $|1\rangle$  that was obtained in the first place.

**Quantum number:** variables describing quantum objects physical quantities or variables that are discrete. Electrons have four quantum numbers: principal quantum number (energy level or electron shell), angular momentum also named azimuthal or orbital quantum number describing electron subshell, magnetic quantum number describing the electron energy level within its subshell and spin projection quantum number, being either +1/2 or -1/2, in a given spatial direction.

**Quantum postulates:** basis of quantum physics formalism. These are postulates and not laws because it describes a mathematical formalism that cannot be proved per se. There are many different presentations of quantum postulates in reference sources (Nielsen & Chuang, Preskill, Cohen-Tannoudji, Wikipedia, ...). Depending on the sources, you'll find 3, 4, 5, 6 or even 7 of them.

**Quantum Physical Unclonable Functions** (qPUF): quantum based physical identifiers that can be used to create unique and unclonable security keys.

**Quantum reservoir computing:** specific category of recurrent neural networks used to process time series. It uses a set of neuron weights and links between neurons randomly fixed in the reservoirs, all with non-linear activation functions. The hundreds of neurons in a reservoir are fed by input data stored in the reservoirs. The activation functions non-linearity makes this memory evanescent. The training parameters of these networks are located in the weights of the neurons that connect the reservoirs to the output data

**Quantum reservoir engineering:** set of techniques for managing qubits through their interaction with a "quantum thermal bath" (quantum bath) to reduce energy consumption, reduce the duration of the measurement of the state of the qubit and allow a non-destructive and reversible measurement of this state ("Quantum non-demolition" or QND). Reservoir engineering is used in cat-qubits.

**Quantum simulator:** name given to analog quantum computers that are capable of simulating quantum objects and solving related problems, particularly in materials physics. By abuse of language, the name is used for supercomputers capable of executing quantum algorithms by numerical simulation. In this case, it is preferable to use quantum emulator.

**Quantum state:** mathematical object used to compute at a given time the probabilities of a quantum object or set of object property values that would be obtained when measuring it and to predict their evolution over time. It is usually represented by a vector in a Hilbert space (linear, metric and complete). This is however only the case for a pure state. A mixed state is represented by a density matrix. The notion of quantum state is usually the first quantum postulate.

**Quantum state tomography:** technique used to characterize the quality of qubits and qubits gates or any quantum channel. It is used to experimentally reconstruct a density matrix of a set of qubits. It also requires a lot of classical computing to process the experimental data obtained with repeated state preparation and measurements.

**Quantum supremacy:** describes a situation where a quantum computer can perform some computation that is inaccessible to the best current supercomputers with the best classical algorithm and in a humanly reasonable time. The computing time differential between quantum computing and classical computing must be several orders of magnitude. It can deal with a useful calculation or not. Thus, the quantum supremacy claimed by Google in October 2019 dealt with a random algorithm that had no practical interest. The term was coined by John Preskill in 2011. Nowadays, the trend is to use the quantum advantage denomination.

**Quantum teleportation:** technique used to transfer the state of one qubit to another location. It is usually performed with three communication links: a pair of previously entangled photons and two classical bit links. It has many uses such as in quantum cryptography (QKD). The non-cloning theorem also says that the state of a teleported quantum disappears from the source after teleportation. It can be used to transmit a rich quantum state of several qubits and can enable distributed quantum computing.

**Quantum variational circuits:** type of quantum algorithm used to implement machine learning.

**Quasi-particles:** physical concept which treats elementary excitations in solids like spin waves, as particles. As the particles do not consist of actual matter, they are called quasi particles. Majorana fermions and polaritons are examples of quasi-particles.

**Qubit** or physical qubit: the elementary unit of information in quantum computing in quantum computers and quantum telecommunication. It stores a quantum state associating two distinct states of a particle or of a quantum system (electron spin, energy level of a superconducting loop, energy level of a trapped atom or ion, polarization or other property of a photon). Its mathematical representation is a vector comprising two complex numbers in a Bloch sphere.

**Qudit**: generic form of qubit that has d possible quantum states instead of two. The approach is rarely used, at least in quantum computers outside research laboratories.

**Qunat**: another name for qubits based on continuous variables.

**Qutrit**: it is a form of qubit which instead of having two possible quantum states, has three. It is a special case of qudits.

**Rabi** (oscillation): oscillations between states of a two-level system excited at a frequency close to its resonance. This phenomenon is observed between two spin states in nuclear magnetic resonance as well as when an electric field acts on the transitions from one electronic state of a system to another for an atom or molecule. The curve describing the oscillation resembles a sinusoidal curve that attenuates over time. Isidor Isaac Rabi is an American physicist of Hungarian origin (1898-1988) who was awarded the Nobel Prize in Physics in 1944. Rabi's oscillations can be found almost everywhere, especially in the operation of superconducting qubits with microwave pulses.

**Raman cooling**: variant of the Doppler effect using the Raman effect used to cool atoms below the limit of Doppler-based cooling, under  $1\mu\text{K}$ . It uses two counter-propagating laser beams. This effect is sometimes used in cold-atom based interferometry.

**Raman effect or Raman scattering**: shift in wavelength of an inelastically scattered radiation where an incident monochromatic photon energy and momentum are both changed. Discovered by Chandrasekhara Venkata Raman (1888-1970, India), Nobel Prize in physics in 1930. This is a small effect that accompanies the predominant Rayleigh scattering of light (unchanged wavelength). The incident polarized light is scattered at its original frequency (Rayleigh elastic scattering) and with higher and lower frequencies (Raman stokes and anti-stokes anti-elastic scattering).

**Raman spectroscopy**: determines vibrational and rotational level spacings from the energy (wavenumber) shifts of inelastic scattered light (*aka* Raman scattering). It is used to analyze multi-atoms molecules through their vibrational modes, particularly in organic chemistry.

**Raman transition**: couples two atomic levels by the absorption of a photon in one Raman beam (pump beam) and by stimulated emission of another one in the other beam (Stokes beam).

**Rayleigh scattering**: predominantly elastic scattering of electromagnetic radiation by particles that are much smaller than the radiation wavelength. Elastic scattering

happens with incident photons whose direction is changed but not their energy (color or wavelength). It explains why the sky is blue, linked to blue light being more scattered than green and red light, and also polarized.

**Realism**: in science, philosophical view according to which there exists a reality independently of an observer. The Copenhagen interpretation of quantum physics is non-realist since it believes reality is only what can be observed and measured.

**Reduced Planck constant**: see Dirac constant.

**Reflectometry**: technology used with superconducting and electron spin qubits readout. It consists in sending a microwave to the qubit and to analyze the reflected microwave, which can have different phase and amplitude depending on the measured qubit state.

**Register**: set of bits or qubits. In the case of qubits, it provides an exponentially growing computational base space with the number of qubits.

**RSA**: a public key encryption system based on the difficulty of factoring a public key formed by multiplying two very large prime numbers. This factorization is theoretically possible with Peter Shor's quantum algorithm. However, it requires a very large number of qubits to break the most common RSA keys at 1024 or 2048 bits. For 2048-bit keys, 20 physical million qubits with a 99,9%+ fidelity are required, which is very long-term in quantum computer roadmaps.

**Rydberg** (atoms): excited state of an atom having one or more electrons and whose principal quantum number  $n$  (index of the electron layer in the atom which is an integer between 1 and the number of electron layers in the atom) is very high. These atoms are generally of large size, proportional to  $n^2$ , and with very strong inter-atomic interactions. These interactions are used to build entanglement between atoms. These atoms have been used by Serge Haroche's team to detect non-destructively the presence of a photon in a cavity, and thus study quantum decoherence. Hydrogen can also be a Rydberg atom if it is excited with high energy levels.

**SAT**: class of logic problem or Boolean satisfiability problem, of 0-order logic. It is a decision problem, which, given a propositional logic formula, determines whether there is an assignment of propositional variables that makes the formula true. As when looking for Boolean variables  $x$ ,  $y$  and  $z$  that satisfy the equation  $(x \vee y \vee z) \wedge (\bar{x} \vee \bar{y}) \wedge (\bar{x} \vee y \vee z)$ ,  $\wedge$  meaning "and", and  $\vee$  "or" or "and".  $\bar{x}$  being the negation of  $x$ . The problem becomes very complex if the number  $N$  of variables becomes very high because to test their combinatorics with brute force, we will have to test  $2^N$  combinations. This problem has been highlighted by Cook's theorem according to which the SAT problem is NP-complete. The SAT problem also has many applications, notably in constraint satisfaction, classical planning, model verification, diagnostics, up to the configurator of a PC or its operating system: we go back to propositional formulas and use a SAT solver.

**Scale-out:** generic information technology term describing the capacity to expand computing power with several processors connected to the other. This is done in classical server clusters and data-centers, using both hardware (multiple processors on same board, high-speed connectivity between boards and servers, high-speed data storage, ...). Such techniques are envisioned with quantum computing, consisting in connecting different processing units, usually with using photons and entanglement resources.

**Scattering:** deflection of moving particles by some physical medium or radiations.

**Schrödinger** (equation, wave function): describes the evolution in time and space of the wave state of a quantum object with a mass like an electron, i.e. the probabilities of finding the object at a given place and time in time.

**Schrödinger wave function collapse:** in the case of a qubit, happens at the end of the coherence (superposed state) which is generated by its state readout, bringing it back to one of its basis states ( $|0\rangle$  or  $|1\rangle$ ). This collapse is also caused by the interaction between the qubit and its environment and after qubit measurement.

**Second quantization:** field of quantum physics that deals with many-body quantum systems. It was introduced by Paul Dirac in 1927 and developed afterwards by Vladimir Fock and Pascual Jordan.

**Second quantum revolution:** covers advances in quantum physics since the 1980s, when we began to control the properties of individual quanta, at the level of photons (polarization, ...), electrons (spin) and atoms and also use superposition and entanglement. It covers in particular the uses of these properties in cryptography and telecommunications, quantum computing and quantum sensing. The term was created simultaneously in 2003 by Alain Aspect, Jonathan Dowling and Gerard Milburn.

**Semi-classical light:** describes interactions between quantized matter (atoms, electrons) and classical light fields. Laser light belongs to this category.

**Shor** (algorithm): integer quantum factorization algorithm invented by Peter Shor in 1994. It would theoretically allow to break RSA public keys by decomposing them into prime numbers.

**Silicon 28:** Silicon isotope allowing the creation of silicon wafers suitable for the creation of silicon qubits. Silicon 28 has a zero spin that does not affect the spin of the trapped electrons used to manage the qubits. It is purified in Russia and can then be deposited in a thin layer in the gas phase on conventional silicon.

**Single mode:** said of a optical fiber using a small core (around 9  $\mu\text{m}$ ) and transporting a single light beam that doesn't bounce off the inside walls of the fiber. It has low loss and is adapted to long distance transport, usually in the 1310 nm or 1550 nm wavelengths. These cables still use multiple wavelengths, with WDM (wave-division multiplexing). Also said of a single mode photon, see Multimode.

**SPAC:** special purpose acquisition company. A funding mechanism used by IonQ and HQS (Honeywell Quantum Systems) consisting in getting acquired by an investment fund creating a dedicated fund for the company and raising money on both limited partners (individual corporate ventures and the likes) and on the stock market like the NASDAQ.

**SPAM:** State Preparation And Measurement, a sequence of operations after which the fidelity of qubits is measured. This fidelity reflects that of an initialization sequence, the application of single qubit gates and the measurement of the qubit state.

**Spectral lines:** lines obtained graphically after decomposing an electromagnetic radiation into frequency components, usually with some spectrography apparatus. You have absorption and emission spectral lines depending on the source of light (indirect, direct). Each line corresponds to the emission or absorption of photons in atoms at particular energy levels, then wavelength and frequency.

**Spectral decomposition:** mathematically, spectral decomposition of a pure state vector in a Hilbert space is its eigenstates  $|i\rangle$  and eigenvalues  $\lambda_i$ . It can be related to the wave-duality aspect of all quantum objects. A quantum object pure state is indeed decomposable in a coherent superposition of elementary waves, the eigenstates.

**Spin:** quantized angular momentum of elementary (like electrons or photons) or composite particles (like atoms) that cannot be described or explained in classical physical terms. The spin of composite particles is the addition of its components spin. A proton and a neutron have a spin of 1/2. An electron has a spin of +1/2 or -1/2. A photon also has a spin, which relates to its circular polarization. Spin help distinguish fermions who have half integer spins from bosons who have integer spins.

**Spintronics:** a set of technologies based on the manipulation of electron spin. It is found in memristors as well as in hard disks using giant magnetoresistance (GMR). The latter was discovered by Albert Fert (France) and Peter Grünberg (Germany) independently and the same year, in 1988. This got them the Nobel Prize in Physics in 2007.

**Spontaneous emission:** when an atom emits a photon resulting from the transition of an electron from an excited to a lower energy state.

**Spontaneous Four-Wave Mixing (SFWM):** photons pairs source category based on pumping nonlinear optical waveguides or cavities.

**Spontaneous Parametric Down-Conversion (SPDC):** system converting high-energy photons into pairs of photons of lower energy, based on pumping nonlinear optical waveguides (crystals) or cavities. It can be used to create pairs of entangled photons as well as single photons sources.

**Squeezed states of light:** correspond, in a quadrature or phasor diagram representation, to wave functions which have an uncertainty in one of the quadrature amplitudes (phase or photon number) smaller than for the ground-state corresponding to the vacuum state. It can be gener-

ated by different means like a parametric down conversion. In other words, it's a way to increase the measurement precision of one of the photons characteristics at the expense of another characteristic.

**SQUID:** Superconducting Quantum Interference Device, a magnetometer that measures the direction of current in a superconducting qubit. It is notably used by D-Wave and in some quantum sensors.

**Stabilizer gates:** quantum gates that are used in error correction systems: CNOT, H (Hadamard) and P (phase).

**Standard quantum limit:** to estimate a system's parameter, one usually uses light as the meter by making it interact with the system and thereby extracts some information. The standard quantum limit, also known as shot noise, states that the variance of this estimation is larger than the inverse of the square root of the number of times the measurement is made.

**State reduction:** consequence of the measurement of the state of a quantum or a qubit, which modifies its (superposed) state into a stable state (not superposed). For a qubit, it is one of the two basic states: excited or non-excited, horizontal or vertical polarization for a photon, spin orientation for an electron, excited state for an ion or a cold atom, etc.

**State vector:** Hilbert space vector representing a pure state of a quantum object.

**Stationary qubits: stationary** (or static) qubits, which do not move in a circuit. This is the case of superconducting qubits, trapped ions and cold atoms qubits as well as electron spin qubits. They are opposed to flying qubits that move, like photons.

**Stimulated emission:** when an incident photon is not absorbed by an excited atom, but stimulates the atom to emit a second photon with the same wavelength. This principle is used in lasers to amplify light in their cavity.

**Sturm-Liouville problem:** mathematical problem consisting in solving some second-order differential equations where the unknown is a density function and finding eigenvalues and eigenvectors and satisfying bound limits. Solving Schrodinger's wave equation is a particular case of such a problem.

**Superconductivity:** the ability of some materials to conduct electricity without resistance. It generally occurs at low temperatures. It is linked to the behavior of electrons in some crystalline structures who happen to gather in pairs, Cooper pairs, who become bosons, and have a collective behavior enabling them to move around within the structure. Superconducting and electron spins qubits use this effect. The first with superconducting loops traversing a Josephson barrier and all of them with cabling and some surrounding electronics.

**Superdense coding:** technique used to send two bits on a single (optically transmitted) qubit between two points when they are already connected by a pair of entangled photons. It is a communication protocol imagined by Charles Bennett and Stephen Weisner in 1992 and experimented in 1996 by Klaus Mattle, Harald Weinfurter, Paul

Kwiat and Anton Zeilinger. The initial entanglement preceding the transmission of the two bits in the qubits avoids violating Holevo's theorem that a set of qubits cannot carry more information than the equivalent number of classical bits.

**Superoperator:** linear operator that transforms a linear operator like a density matrix. It must be a CPTP map, completely positive and trace preserving map (see CPTP definition).

**Superposition:** property of quantum objects and qubits to be able to be in several states at the same time. This can be explained by the wave-like nature of quantum objects. A superposition is a linear combination of quantum eigenstates (the  $|0\rangle$  and  $|1\rangle$  in the case of qubits).

**SWAP:** quantum gate that inverts the state of two qubits. It is very useful since most qubit geometries don't allow an any-to-any qubit connection. The SWAP gate enables this kind of connection that is mandatory for many quantum algorithms.

**Symmetry:** of Schrödinger's wave function, with bosons. Fermions have an antisymmetric wave function. It is the mathematical consequence of Pauli's exclusion principle which states that two fermions with the same quantum numbers cannot cohabit while two similar bosons can.

**T<sub>1</sub>:** qubit amplitude coherence time, which indicates the end of coherence of the qubits linked to a loss of amplitude ("energy relaxation"). Aka qubit lifetime.

**T<sub>2</sub> :** phase related coherence or time when some phase shift occurs, i.e. a rotation around the z axis in the Bloch sphere of the qubit state.

**Tensor:** in multilinear algebra and differential geometry, a tensor designates a very general object whose value is expressed in a vector space. In quantum physics and computing, tensors are used to describe the state of a compound quantum object with several quanta or qubits. A qubit is represented by a vector of 2 complex numbers. A register of N qubits is represented by a vector with  $2^N$  complex numbers resulting from the tensor product of N vectors of 2 complex numbers. In a way, the tensor product represents the combinatorial space of the values that a combination of qubits can take. Before entanglement comes into play to mix things up and create non separable vector states, i.e., which cannot be expressed as tensor products of individual quantum states.

**Thermodynamics first law:** the internal energy of an isolated system is a constant, applying the principle of the conservation of energy. Inside the system, the form of energy can however be transformed.

**Thermodynamics second law:** the entropy of a closed system cannot decrease. In other words, heat does not flow spontaneously from cold to hot objects. Was formalized by Rudolph Clausius in 1854.

**Time domain:** deals with the evolution of some value and signal over time. It's frequently opposed to frequency domain where a signal is analyzed with decomposing it into frequencies (mathematically, with a Fourier transform).

**Toffoli** (gate) : also called CCNOT is quantum gate operating on three qubits which modifies the value of the third qubit if the value of the first two is 1.

**Topological**: topological quantum computing is based on the notion of anyons which are "quasi-particles" integrated in two-dimensional systems. The anyons are asymmetric and two-dimensional physical structures whose symmetry can be modified. This allows the application of topology principles with sets of successive permutations applied to pairs of anyons that are in close proximity in circuits. The associated algorithms are based on the concepts of topological organizations of braids or nodes ("braids"). There is an algorithmic equivalence between computation with universal gated qubits and topological qubits.

**Transmon**: transmission-line shunted plasma oscillation qubit, variation of superconducting qubit with superconducting current oscillating at two different frequencies across a Josephson junction. The difference between these two frequencies corresponds to the energy of the microwave pulses sent to the qubit to drive single qubit gates.

**Transpilation**: generically, compilers are source-to-source compilers. It is used in classical computing and quantum computing. It is used to optimize the source code based on some hardware constraints. It can help reduce the number of gates to execute and as a result, reduce errors (particularly with NISQs) and reduce the algorithm execution time.

**Transversal gates**: relates to quantum error correction and fault tolerance. These are gates implemented with QEC where there is a 1-1 correspondence and link between all qubits from a given corrected qubit with a similar corrected qubit, when they are assembled through concatenation. This mechanism limits the propagation of errors between logical and physical qubits.

**Trapped ions**: these are ions used in certain types of quantum computers. They are usually trapped magnetically or electrically and their state is controlled with lasers. Their readout use a laser excitation and an imager readout of the resulting ions fluorescence.

**Tunnel effect**: property of a quantum object to cross a potential (or energy) barrier even if its energy is less than the minimum energy required to cross this barrier. This effect is used in D-Wave's quantum annealers to quickly determine the minimum energy of a complex system ("Hamiltonian" implemented as an Ising model).

**Two-Level Systems** (TLS): other descriptor of quantum systems used to implement qubits. A qutrit is a three-level system.

**UHV**: Ultra High Vacuum, the ultra-high vacuum required to operate certain types of qubits. It is mainly used for cold atoms and trapped ions. Superconducting qubits are integrated in a vacuum cryostat that does not require ultra-high vacuum.

**Ultraviolet catastrophe**: expression of Paul Ehrenfest, linked to the Rayleigh-Jeans law proposed in 1900 to explain the black body radiation spectrum, which was

diverging to infinite values as the temperature was growing, when reaching ultraviolet wavelengths. Planck's law based on quanta solved the problem and got rid of the ultraviolet catastrophe.

**Unary gates**: single qubit gates. Not to be confused with unitary operations that are the result of the combination of all qubit gates on a given set of qubits. A unitary transformation of the computational state vector is a matrix operator that is equal to its transconjugate. It is a mathematically reversible operation.

**Unconventional Computing**: computing methods that do not fall under the classical computing principles of Turing and Von Neuman machines. Covers non-traditional tools and methods that include, but are not limited to, quantum computers. It also includes molecular computers and neuromorphic processors.

**Unitary operation**: linear operation on a vector that preserves its length. In the case of qubits whose vector always has a length of 1, the unitary quantum gates apply on it a transformation that preserves this length and is also reversible. In the representation of qubits in the Bloch sphere, the operation rotates the vector representing the state of the qubit in this sphere.

**Universal quantum computer**: most generic form of a quantum computer exploiting a universal quantum logic gate set, and which can both simulate quantum physics and implement any operations of a classical computer.

**Universal quantum gates**: sets of quantum gates from which all other quantum gates can be reproduced to create any unitary transformation on any number of qubits. It requires a non-Clifford group gate, namely a T gate or a Toffoli gate.

**VQA** (Variable Quantum Algorithm) more generic quantum hybrid algorithm than VQE. It combines a classical optimizer that is used to train a parametrized quantum circuit. It could lead to obtain some quantum advantage with NISQ quantum computers. VQA has a broad set of applications: finding ground and excited states, quantum simulations, machine learning and optimizations.

**VQE** (Variational Quantum Eigensolver): hybrid quantum algorithm used in chemical simulation created in 2013. Its main contributor is Alan Aspuru-Guzik, a researcher at the Zapata Computing startup. It is also used in machine learning tasks. VQE was the first proposed VQA.

**Wavepackets**: is a burst of electromagnetic wave that travels as a unit. It is formed by the addition of an infinite number of sinusoidal waves of different frequencies, phases and amplitudes creating constructive and destructive interferences on a small region in space, and destructively elsewhere. Wavepackets are used in many quantum technologies such as with microwaves sent to superconducting and electron spin qubits or by femto- and picoseconds lasers. In these cases, their decompositions in frequencies lead to so-called frequency combs.

**Wave-particle duality**: the property of elementary particles such as electrons, neutrons, atoms and photons to behave as both particles with momentum and waves that

can generate interference. It is verified with the famous Young's slits experiment which shows these interferences with both photons and electrons.

**Wien's displacement law:** describes the relationship between peak wavelength and temperature in black body energy spectrum. Discovered by Wilhelm Wien in 1893.

**Wigner function:** representation of a quantum state used to measure the level of quantumness of a light pulse. It has the particularity of having negative values for entangled and non-gaussian states. It is usually visualized in a 3D chart with peaks and lows. Also called Wigner quasiprobability distribution or Wigner-Ville distribution. It was created by Eugene Wigner in 1932.

**X:** quantum gate at a qubit that inverts its amplitude, goes from  $|0\rangle$  to  $|1\rangle$  or from  $|1\rangle$  to  $|0\rangle$  for the basis states.

**XY gates:** are single qubit gates which operate a rotation around an axis in Bloch's sphere equator. It can be viewed as amplitude change gates.

**Y:** single-qubit quantum gate that performs a  $180^\circ$  rotation around the Y axis in the Bloch sphere.

**Z:** quantum gate to a qubit that applies a sign change to the  $\beta$  component of the qubit vector, i.e. a phase inversion and a  $180^\circ$  rotation with respect to the Z axis. More generally, Z gates is also a denomination for phase change gates.

**Zeeman effect:** splitting of spectral lines when atoms are placed in a static magnetic field. Explained by the different electrons magnetic moment.

**ZX calculus:** graphical language and formalism used to visualize in quantum programming the notions of entanglement, complementarity, causality and their interactions. It can be used for Measurement Based Quantum Computing (MBQC), the creation of error correction codes and compiler optimization techniques.

# Index

- 137, 48, 51, 123, 802  
1QBit, 249, 422, 424, 515, 524, 525, 547, 550, 551, 561, 567, 569, 686, 687  
2D-SIPC, 718  
A\*Quantum, 568, 728  
Aalto University, 274, 304  
ABCMintFoundation, 633  
Absolut System, 376  
Accelink, 400  
Accenture, 249, 315, 321, 483, 538, 547, 555, 567, 696  
Accubeat, 721  
Active Fiber Systems, 400  
Adamas Nano, 406  
Adaptive Finance Technologies, 567  
Adiabatic computing, 28, 228, 417, 429, 430, 431  
AegiQ, 633  
Aeponyx, 405  
AgilePQ, 633  
Agnostiq, 633  
AIQTECH, 567  
Air Liquide, 111, 365, 373, 374, 375, 376, 410, 413, 710  
Akira Furusawa, 727  
Alain Aspect, 11, 12, 19, 43, 57, 58, 59, 60, 65, 79, 96, 103, 233, 401, 606, 670, 696, 701, 747, 792, 799, 801, 811, 818  
Alain Couvreur, 622  
Alan Aspuru-Guzik, 75, 477, 480, 483, 522, 820  
Albert Einstein, 31, 32, 38, 40, 42, 43, 45, 50, 55, 88, 94, 109, 395, 692, 745, 747, 804, 811  
Alberto Amo, 118  
Alberto Boretti, 654  
Alberto Bramati, 116, 118  
Aleks Kissinger, 355, 501  
Alexander Holevo, 72  
Alexander Rostovtsev, 623  
Alexandre Blais, 256, 274, 685  
Alexei Grinbaum, 71, 750  
Alexei Kitaev, 55, 73, 74, 214, 217, 255, 303, 305, 459, 812, 813  
Alexei Orlov, 429, 430  
Alexia Auffèves, 11, 36, 60, 67, 177, 228, 230, 292, 429, 703, 704, 731, 749, 793, 801  
Algorithmiq, 567  
Alibaba, 76, 239, 277, 421, 504, 505, 506, 523, 602, 669, 725, 783  
Alice&Bob, 76, 177, 189, 207, 240, 252, 255, 278, 280, 384, 405, 675, 698, 704, 709, 793, 801  
Alireza Shahsaf, 666  
Aliro Quantum, 568  
Alonzo Church, 55, 487, 510  
Alpes Lasers, 400  
Alpine Quantum Technologies, 63, 182, 188, 239, 308, 314, 321, 713  
Alter Technology, 405  
Alternatio, 633  
Altitun, 400  
Aluminum, 64, 109, 110, 189, 197, 269, 273, 370, 371, 396, 405, 415, 416, 432, 631, 653, 724  
Amazon, 65, 76, 177, 189, 212, 231, 232, 233, 235, 240, 248, 252, 255, 272, 274, 278, 279, 280, 315, 317, 508, 519, 522, 524, 525, 570, 578, 580, 581, 582, 583, 669, 685, 739, 783, 810  
AMD, 183, 281, 419, 421, 426, 598, 628  
Amdahl's law, 23  
Ampliconyx, 400  
Amplitude encoding, 452  
Amplitude Laser, 400  
Anametric, 633  
Andrea Morello, 68, 286, 363  
Andreas Wallraff, 66, 252, 256, 260, 274, 394  
Andrew Adamatzky, 417  
Andrew Childs, 450, 471, 623  
Andrew Jordan, 177  
Andrew S. Dzurak, 68, 286  
Andrew Steane, 74, 154, 209, 687  
Andrew Wiles, 593  
Angle encoding, 452  
Angstrom Engineering, 405  
Angular momentum, 46, 89, 94, 333, 349, 802, 806, 816, 818  
Ankh.1, 568  
Anna Grassellino, 682, 714  
Anne Broadbent, 71, 75, 76, 355, 525, 526, 625, 626  
Anne Canteaut, 698  
Anne Matsuura, 71, 289  
Ansatz, 484  
Anthony Leggett, 58, 79, 189  
Anthony Leverrier, 203, 216, 521, 595  
Antiparallel, 150  
Antoine Béret, 427, 429  
Antoine Browaeys, 60, 67, 222, 323, 324, 325, 326, 328, 330, 701, 793, 801  
Anton Stolbunov, 623  
Anton Zeilinger, 47, 58, 61, 100, 612, 819  
Anupam Prakash, 78, 219, 466, 473, 806  
Anyon Systems, 276  
ApexQubit, 546, 561, 568  
AppliedQubit, 568  
Apply Science, 568  
Aqemia, 568  
AQT, 63, 188, 310, 321, 516, 570  
AQTION, 314, 507, 717  
Aquubits, 322  
aQuantum, 547, 568  
Aram Harrow, 74, 450, 474, 585  
Archer, 287, 288, 733  
Arieh Warshel, 544  
Arline, 569  
Arnold Sommerfeld, 48  
ArQit, 633  
Arthur Holly Compton, 45, 745  
Arthur Leonard Schawlow, 56, 396  
Artist-eqb.net, 569  
Artur Ekert, 11, 65, 79, 573, 606, 725, 730, 793  
Asher Peres, 462, 612  
Ashley Montanaro, 450, 462, 471  
ASML, 25, 26, 292, 399  
ASTERIQS, 655, 699, 701  
Astrid Lambrecht, 121, 124  
Atlantic Microwave, 393  
Atom Computing, 184, 233, 326, 330  
Atos, 11, 16, 59, 60, 65, 78, 183, 224, 274, 275, 279, 295, 314, 328, 329, 408, 419, 422, 423, 503, 506, 507, 508, 513, 519, 522, 523, 532, 551, 560, 586, 606, 618, 621, 632, 669, 702, 709, 710, 717, 718, 719, 731, 735, 739, 792, 799  
Audrey Bienfait, 69, 626, 704  
Audrey Cottet, 296, 698  
Aurea Technology, 400, 710  
AuroraQ, 405  
Australia, 10, 16, 66, 68, 69, 85, 190, 191, 274, 281, 282, 285, 287, 299, 300, 301, 308, 332, 347, 406, 411, 414, 415, 575, 578, 581, 583, 641, 649, 654, 673, 675, 682, 686, 715, 732, 733, 734, 753, 757, 763  
Austria, 11, 16, 47, 48, 62, 70, 100, 114, 177, 182, 188, 308, 312, 314, 321, 326, 328, 330, 344, 347, 402, 507, 516, 533, 562, 574, 575, 610, 612, 614, 635, 665, 695, 708, 712, 713, 717, 718, 719, 799  
Automatski, 569  
Avanetix, 569, 696  
AVaQus, 242  
Axel Becke, 544  
Azur Light Systems, 400, 706  
Balmer series, 94  
Basis encoding, 221, 452, 457  
BCS theory, 56, 109  
Beit.tech, 569  
Belgium, 56, 71, 293, 295, 358, 386, 407, 617, 708, 712, 718, 832  
Bell inequalities, 58, 803

- Ben-Gurion University, 721  
 Benoît Valiron, 77, 509, 510, 526, 701  
 Bert de Jong, 201, 204, 242, 503  
 Beryllium, 307, 381, 399, 409, 416, 479, 550  
 Bettina Heim, 78  
 Bikanta, 406  
 Black body, 39, 40, 41, 92, 93, 121, 325, 745, 746, 803  
 Black Brane Systems, 569  
 Bleximo, 276  
 Bluefors, 283, 370, 372, 373, 374, 376, 378, 381  
 Blueqat, 569  
 Bolometry, 375, 376  
 Boltz.ai, 570  
 Boris Podolsky, 42, 43, 55  
 Bose-Einstein condensate, 35, 41, 113, 330, 648, 787, 804, 805  
 Boson, 29, 70, 75, 113, 125, 126, 144, 193, 233, 241, 267, 268, 290, 334, 335, 347, 348, 349, 350, 352, 358, 402, 403, 492, 527, 534, 566, 714, 724, 804, 809  
 BosonQ Psi, 570  
 Boxcat, 570  
 Bpifrance, 4, 205, 670, 709, 793, 798, 799, 801  
 BQP, 464, 485, 493, 494, 495, 804  
 Bra-ket, 37, 51, 804, 807  
 BraneCell, 331  
 Brian Josephson, 62, 79, 687, 774  
 Bronze, 370, 381, 705  
 Brookhaven National Laboratory, 682  
 Bruce Kane, 285  
 Bruce MacLennan, 417, 797  
 Bryce DeWitt, 58, 748, 768  
 C12 Quantum Electronics, 295, 409, 416  
 C2N, 11, 66, 67, 70, 117, 118, 251, 292, 304, 347, 350, 401, 402, 700, 793  
 Cadmium, 307, 416  
 CAILabs, 400  
 Calcium, 59, 148, 188, 307, 308, 309, 310, 314, 414, 415, 416, 769  
 Calmar Laser, 400  
 Caltech, 65, 68, 70, 74, 217, 251, 267, 279, 280, 326, 524, 533, 566, 627, 666, 680, 684  
 Cambridge Quantum Computing, 275, 321, 329, 555, 563, 570, 692  
 Canada, 11, 16, 74, 77, 210, 221, 235, 276, 281, 308, 322, 358, 377, 399, 404, 405, 413, 414, 415, 416, 424, 426, 427, 462, 508, 524, 533, 534, 567, 569, 570, 571, 573, 574, 575, 576, 577, 579, 580, 582, 583, 584, 585, 604, 605, 610, 626, 633, 634, 635, 637, 638, 640, 642, 643, 656, 657, 665, 670, 673, 675, 676, 682, 685, 686, 687, 691, 715, 720, 722, 730, 753, 755, 757, 790, 797  
 Carlo Rovelli, 126, 748, 750  
 Carlton Caves, 746  
 Carnegie Mellon University, 30, 63  
 Casimir effect, 14, 121, 122, 123, 124, 788  
 CEA LIST, 244, 389, 526, 792, 793  
 CEA-Leti, 11, 67, 190, 193, 240, 281, 283, 285, 290, 291, 292, 293, 294, 295, 346, 374, 375, 376, 385, 387, 389, 390, 412, 429, 440, 507, 691, 695, 703, 704, 708, 712, 718, 734, 758, 792, 799  
 Cerebras, 27, 421  
 CERN, 52, 57, 64, 111, 120, 125, 251, 410, 411, 565, 566, 761, 798, 815  
 Cesium, 65, 103, 148, 221, 319, 323, 325, 330, 409, 413, 416, 645, 646, 650, 653, 654, 657  
 Chandrasekhara Venkata Raman, 817  
 Chao-Yang Lu, 351, 612  
 Chapman University, 67  
 Charler Herder, 626  
 Charles Beigbeder, 670, 793  
 Charles Bennett, 36, 74, 164, 210, 228, 428, 605, 609, 612, 685, 819  
 Charles Hard Townes, 56, 396, 397  
 Charles Hermite, 33  
 ChemAlive, 571  
 Cheng-Zhi Peng, 612  
 Chien-Shiung Wu, 57, 762  
 China, 10, 15, 16, 20, 221, 233, 277, 290, 298, 299, 304, 308, 347, 351, 359, 384, 399, 400, 411, 413, 414, 415, 416, 419, 435, 444, 471, 473, 505, 523, 525, 567, 575, 602, 606, 608, 609, 611, 612, 613, 614, 616, 628, 635, 639, 643, 647, 657, 661, 665, 675, 676, 678, 679, 680, 681, 713, 717, 722, 723, 724, 725, 728, 731, 744, 761, 787  
 Chinese Academy of Sciences, 222, 277, 526, 614, 639, 723  
 Chirp pulse, 133  
 Chloe Martindale, 623  
 Chris Hoofnagle, 755  
 Christine Silberhorn, 69  
 Christophe Jurczak, 9, 11, 329, 472, 670, 792, 793, 801  
 Christophe Salomon, 65, 68, 698  
 Christopher Fuchs, 746  
 Christopher Monroe, 64, 213, 309, 313, 315, 318, 321, 683  
 Chromacity, 399  
 Ciena, 634  
 CIQTEK, 384, 657  
 Cirq, 266, 271, 329, 504, 520, 524, 549, 573, 580, 585, 586  
 Cisco, 632, 640  
 CiViQ, 718  
 ClassiQ, 571  
 Claude Cohen-Tannoudji, 59, 68, 101, 327, 684, 696, 794  
 Claude Crépeau, 462, 612  
 Claus Jönsson, 47  
 Clifford group, 74, 163, 217, 237, 341, 804, 812, 820  
 CLOPS, 532  
 Cloudflare, 623  
 CMOS, 23, 26, 27, 67, 181, 190, 197, 198, 199, 213, 225, 232, 270, 276, 281, 282, 283, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 322, 332, 345, 355, 356, 382, 385, 386, 387, 388, 389, 390, 392, 393, 404, 417, 423, 424, 426, 427, 428, 429, 430, 431, 433, 438, 439, 600, 601, 603, 653, 655, 662, 703, 704, 712, 727, 729, 732, 734, 788, 790, 804, 810  
 Coax Co, 380, 414  
 CogniFrame, 571  
 ColdQuanta, 184, 233, 237, 317, 318, 326, 330  
 Color codes, 74, 197, 207, 217, 283, 815  
 Complementarity, 90, 95, 104, 417, 814, 821  
 Compton effect, 41, 45, 120, 333  
 Concatenated codes, 805  
 Conjugate variables, 90  
 Continuous variables, 75, 185, 193, 332, 338, 345, 357, 358, 477, 805, 813  
 Copper, 109, 110, 111, 197, 254, 363, 370, 371, 372, 379, 381, 387, 392, 413, 415, 416, 804  
 Cornell University, 79, 802  
 CPTP, 143, 168, 175, 176, 805  
 CQC2T, 68, 285, 286, 287, 733, 734  
 CQT, 251, 381, 408, 573, 722, 730, 731, 757, 793  
 Craig Costello, 623  
 Craig Gidney, 500, 591  
 Craig Lent, 429, 430  
 CreativeQuantum, 571  
 Crédit Agricole CIB, 329  
 Cristian Calude, 78, 234, 603  
 CryoConcept, 371, 373, 375, 376, 797  
 CryoFab, 377  
 Cryogenic Limited, 377  
 Cryomech, 232, 365, 367, 376  
 Crypto Labs, 604, 634  
 Crypto Quantique, 635  
 Crypto4A Technologies, 634  
 CryptoExperts, 618, 634, 709  
 CryptoMathic, 604  
 CryptoNext Security, 634, 670  
 CRYSTALS - Kyber, 623  
 Culgi, 571  
 Cymaris Labs, 406  
 Cyph, 635  
 Cyril Allouche, 11, 78, 793  
 Cyril Elouard, 177  
 D Slit Technologies, 571, 728  
 Damian Markham, 726, 793  
 Damien Stehlé, 623  
 Daniel Bernstein, 617, 625  
 Daniel Esteve, 11, 64, 65, 66, 69, 189, 254, 606, 700, 792, 793  
 Daniel Gottesman, 74, 210  
 Daniel Lidar, 241, 248  
 Daniel Vert, 244  
 Daniele Micciancio, 623  
 Dark count, 344, 361  
 Dark silicon, 25  
 DARPA, 242, 330, 403, 407, 408, 439, 533, 610, 653, 681, 754

- David Awschalom, 628, 682  
 David Bohm, 43, 58, 75, 746, 747, 755  
 David Chalmers, 741  
 David Dean, 682  
 David Deutsch, 73, 442, 463, 687, 748, 806  
 David DiVincenzo, 65, 180, 181, 210, 606  
 David H Meyer, 668  
 David Hilbert, 37  
 David Jao, 623  
 David Lewis Anderson, 124  
 David Mermin, 746  
 David Pointcheval, 698  
 David Simon, 73, 464  
 David Wineland, 64, 315, 318, 683  
 Delft Circuits, 232, 242, 277, 380, 384, 712  
 Dell, 508  
 Decrypt, 635  
 DenseLight Semiconductors, 399  
 Density matrix, 131, 137, 138, 139, 140, 141, 142, 143, 172, 173, 174, 175, 176, 184, 200, 206, 500, 505, 508, 806, 811, 812, 815, 816, 819  
 DiamFab, 405  
 Diamond Materials, 406  
 Dieter Zeh, 61  
 Diffraction, 34, 47, 53, 55, 438, 439, 456, 662, 770  
 Dilution refrigerator, 118, 225, 245, 365, 374, 376, 650, 807  
 Dirac constant, 50, 51, 361  
 Diramics, 393  
 Dirk R. Englund, 344  
 Dmitri Voronine, 662  
 Don Misener, 112  
 Doppler effect, 41, 100, 101, 114, 188, 308, 310, 312, 318, 320, 362, 379, 785, 804, 807  
 Dorit Aharonov, 75, 142, 215, 471, 494, 497, 763  
 DTU, 635  
 Duality Quantum Photonics, 359, 391  
 D-Wave, 12, 16, 31, 33, 78, 86, 89, 98, 107, 179, 183, 184, 197, 202, 224, 226, 229, 231, 232, 235, 237, 240, 241, 242, 243, 244, 245, 247, 248, 249, 250, 251, 252, 254, 262, 265, 272, 274, 279, 281, 309, 357, 371, 373, 381, 390, 393, 417, 423, 426, 431, 444, 449, 467, 470, 473, 475, 476, 483, 494, 503, 513, 514, 515, 519, 523, 524, 534, 538, 542, 543, 545, 546, 547, 548, 550, 551, 553, 554, 555, 556, 557, 559, 560, 562, 563, 565, 566, 567, 569, 570, 571, 572, 573, 574, 576, 577, 578, 579, 580, 582, 583, 584, 592, 638, 644, 669, 670, 673, 684, 686, 687, 695, 725, 728, 730, 735, 739, 753, 759, 793, 799, 802, 807, 809, 811, 815, 819, 820  
 Earle Hesse Kennard, 50, 104  
 Ecole des Mines de Paris, 4, 698  
 Edward Farhi, 64, 484  
 Edward Fredkin, 63, 428  
 EeroQ, 290  
 Eigenstate, 132, 807  
 Eigenvalues, 91, 92, 132, 134, 139, 140, 144, 169, 448, 450, 818  
 Eigenvectors, 91, 92, 132, 133, 135, 140, 142, 169, 450, 473, 474, 802, 803, 806, 807  
 Elementsix, 405  
 Elena Calude, 78, 534  
 Eleni Diamanti, 11, 68, 77, 345, 401, 535, 557, 558, 608, 609, 613, 628, 698, 718, 793, 801  
 eleQtron, 322  
 Elham Kashefi, 11, 71, 75, 76, 352, 353, 355, 474, 478, 525, 526, 625, 626, 631, 642, 698, 718, 763, 793, 801  
 Elisabeth Foley, 657  
 Elisabeth Giacobino, 66, 116, 118, 717  
 Elizabeth Rauscher, 750  
 Elliptic curves, 468, 593, 594, 596, 623, 807  
 Elvira Shishenina, 793  
 Elyah, 572  
 Emanuel Knill, 57, 210, 343, 349  
 Emilio Del Giudice, 775  
 Emmy Noether, 33, 45, 762  
 Enrico Fermi, 48, 543  
 Enrique Solano, 123, 573  
 ENS Lyon, 36, 67, 69, 255, 261, 278, 427, 487, 626, 632, 704, 705  
 Entropica Labs, 524, 555, 572, 731  
 Entropy, 36, 54, 177, 268, 427, 535, 598, 601, 602, 604, 605, 630, 634, 640, 788, 796, 803  
 EPFL, 261, 265, 291, 292, 385, 404, 715, 716  
 EPSRC, 688, 689, 691  
 equal1.labs, 289  
 Erbium, 70, 114, 415, 416, 468, 699, 700  
 ERC Grants, 697, 808  
 Ergotropy, 176  
 Ernest Rutherford, 43, 44, 687  
 Ernst Rasel, 648  
 Erwin Schrödinger, 31, 48, 51, 53, 152, 356, 744, 745  
 ETH Zurich, 66, 77, 198, 201, 252, 257, 260, 261, 265, 292, 309, 311, 312, 314, 393, 406, 477, 478, 480, 509, 511, 626, 715, 716, 800  
 Ettore Majorana, 55, 305, 812  
 EuroHPC, 329, 420, 507, 719  
 EUV lithography, 25, 26  
 Evaporative cooling, 101  
 Evgeny Morozov, 751  
 evolutionQ, 594, 635, 715  
 Ewin Tang, 78, 473, 485, 534, 562, 806  
 ExaQai, 572  
 Excellitas, 404  
 EYL, 602, 604  
 Fabio Sciarrino, 70, 268, 347, 348, 402, 714  
 FAccTs, 572  
 Fanny Bouton, 11, 792, 801  
 FAR Biotech, 572  
 Feihu Xu, 661  
 Felix Bloch, 57, 109, 119, 138, 152  
 FemTum, 399  
 FinFET, 26, 276, 388  
 FISBA, 400  
 Flipscloud, 635  
 Fluxonium, 240, 277  
 FND Biotech, 406  
 Fock space, 53, 350, 808  
 Fock state, 176, 334, 335, 342, 808  
 FocusLight Technologies, 399  
 FPGA, 232, 257, 290, 320, 383, 384, 387, 388, 393, 406, 421, 471, 618, 622, 636, 639  
 fragmentiX, 635  
 France, 4, 9, 10, 11, 16, 19, 20, 37, 46, 52, 55, 60, 64, 66, 67, 69, 70, 72, 75, 76, 77, 83, 117, 118, 127, 152, 177, 188, 190, 193, 194, 221, 222, 224, 234, 251, 252, 255, 260, 265, 274, 278, 280, 281, 282, 292, 294, 295, 299, 304, 308, 314, 326, 327, 329, 330, 338, 341, 346, 347, 356, 359, 363, 373, 375, 376, 380, 381, 384, 385, 395, 398, 399, 400, 401, 405, 407, 411, 412, 418, 419, 420, 427, 435, 436, 438, 440, 483, 506, 507, 509, 521, 522, 535, 549, 551, 556, 557, 563, 564, 568, 572, 577, 579, 580, 581, 582, 584, 603, 609, 610, 614, 617, 618, 621, 623, 632, 634, 637, 641, 642, 646, 647, 648, 649, 654, 655, 657, 663, 670, 673, 675, 693, 695, 696, 697, 698, 701, 702, 708, 709, 710, 711, 712, 714, 717, 718, 719, 730, 731, 732, 735, 739, 747, 750, 751, 753, 758, 764, 773, 775, 776, 778, 788, 790, 793, 798, 799, 818  
 Francesca Ferlaino, 70, 114  
 Franck Laloë, 59, 202, 794, 795  
 Franco Nori, 510, 726  
 François Le Gall, 727  
 Frédéric Grosshans, 71, 96, 607  
 Frédéric Magniez, 77, 698  
 Freedom Photonics, 399  
 Friedrich Paschen, 43, 94, 745  
 Fritz Albert Popp, 771  
 Fujitsu, 28, 224, 277, 281, 419, 423, 424, 427, 561, 567, 568, 574, 577, 726, 728, 729  
 Gallium, 23, 66, 117, 282, 288, 292, 350, 396, 413, 416, 631, 701, 810  
 Geordie Rose, 235, 242  
 Georges Uhlenbeck, 48  
 Gerald Moore, 123  
 Gerard Milburn, 19, 57, 343, 349, 818  
 Germanium, 56, 109, 282, 284, 285, 288, 289, 292, 300, 345, 387, 413, 416, 781  
 Germany, 10, 16, 37, 45, 62, 65, 66, 76, 94, 117, 180, 181, 188, 208, 224, 242, 248, 260, 263, 265, 274, 281, 289, 291, 295, 299, 300, 308, 314, 322, 326, 328, 329, 347, 369, 370, 374, 375, 377, 378, 385, 394, 398, 399, 400, 401, 404, 405, 406, 408, 415, 419, 420, 477, 548, 551, 553, 569, 571, 572, 573, 581, 604, 610, 626, 632,

- 636, 639, 640, 642, 653, 655, 656, 659, 661, 662, 673, 675, 679, 692, 693, 694, 695, 696, 707, 708, 712, 717, 718, 719, 720, 722, 730, 753, 771, 799, 818  
 Gifford-McMahon, 365  
 Gil Kalai, 74, 233, 234, 268, 360, 721  
 Gilbert Lewis, 40  
 Gilles Brassard, 36, 76, 462, 605, 612, 685  
 Giuliano Preparata, 775  
 Glauber states, 56  
 GLOphotonics, 399  
 Google, 10, 13, 15, 21, 66, 74, 77, 79, 80, 81, 83, 84, 85, 179, 189, 197, 203, 205, 206, 213, 214, 216, 223, 224, 225, 227, 230, 233, 235, 237, 239, 240, 241, 247, 248, 249, 250, 252, 254, 255, 257, 258, 261, 263, 265, 266, 267, 268, 269, 270, 271, 272, 275, 276, 277, 278, 280, 287, 300, 305, 315, 317, 321, 329, 349, 359, 362, 363, 373, 381, 382, 393, 417, 421, 430, 439, 471, 473, 478, 480, 484, 497, 500, 503, 505, 506, 508, 509, 510, 511, 519, 520, 521, 523, 525, 533, 534, 535, 544, 550, 551, 563, 565, 569, 573, 576, 578, 579, 580, 581, 585, 586, 591, 623, 669, 673, 677, 678, 684, 685, 721, 724, 735, 739, 742, 756, 759, 761, 765, 811, 816  
 GoQuantum, 636  
 Graphcore, 26, 575  
 Grenoble, 11, 52, 66, 67, 68, 118, 146, 177, 188, 190, 193, 194, 230, 234, 242, 251, 281, 290, 291, 292, 293, 294, 295, 304, 326, 369, 370, 376, 377, 381, 385, 389, 390, 405, 411, 435, 436, 501, 663, 681, 697, 698, 702, 703, 704, 708, 713, 714, 718, 747, 749, 792, 793, 797, 799  
 Griffith University, 332  
 Groovenauts, 572, 728  
 Guillaume Endignoux, 624  
 Hafnium Labs, 572  
 Haiyun Xia, 661  
 Hamamatsu, 404  
 Hans Albrecht Bethe, 123  
 Han-Sen Zhong, 351  
 HaQien, 636  
 Harald Weinfurter, 819  
 Harmonic oscillator, 98, 177, 255, 334, 804  
 Harvard, 75, 118, 326, 331, 381, 481, 483, 522, 586, 614, 662, 680, 684, 764  
 Heike Kamerlingh Onnes, 62, 108, 112, 710  
 Heike Riel, 793  
 Heindrick Lorentz, 41  
 Heinrich Hertz, 35, 41, 695  
 Hélène Perrin, 68, 298, 702, 798  
 Helium, 35, 42, 49, 60, 62, 66, 89, 108, 111, 112, 113, 114, 118, 119, 126, 232, 290, 320, 332, 363, 364, 365, 366, 367, 368, 369, 370, 371, 376, 377, 378, 379, 396, 401, 403, 409, 410, 411, 415, 646, 803, 804, 806, 807, 809, 810, 816  
 Helmut Hauser, 437  
 Hendrik Antoon Lorentz, 38, 710  
 Hendrik Casimir, 121  
 Henri Poincaré, 37, 38, 41, 152, 696  
 Henry P. Stapp, 750  
 Hermann Minkowski, 41  
 Hideyoshi Nishimori, 241, 423, 725  
 High Precision Devices, 377  
 Holevo theorem, 72, 151, 607  
 Honeywell, 10, 78, 85, 87, 160, 188, 203, 214, 233, 239, 266, 310, 311, 312, 314, 316, 318, 319, 320, 321, 322, 379, 521, 523, 524, 528, 531, 555, 570, 571, 572, 583, 587, 673, 677, 683, 684, 685, 692, 713, 763, 818  
 Horizon Quantum Computing, 573, 731  
 HQS, 214, 242, 321, 546, 548, 573, 695, 696, 718, 818  
 Huawei, 504, 506, 522, 523, 632  
 Hub Security, 636  
 Hugh Everett, 58, 746, 748  
 Hui Khoon Ng, 228, 731  
 Hyperfine, 47, 201, 298, 299, 310, 319, 323, 325, 327, 645, 650, 746, 806, 810  
 Hypres, 390, 428, 432, 434  
 IARPA, 28, 242, 260, 275, 390, 434, 509, 510, 528, 565, 681, 734  
 IBM, 10, 13, 15, 16, 25, 26, 65, 71, 79, 85, 148, 161, 171, 173, 179, 180, 181, 189, 194, 197, 199, 205, 206, 212, 213, 214, 218, 223, 224, 227, 228, 230, 232, 233, 235, 237, 239, 240, 241, 247, 252, 254, 255, 261, 262, 263, 264, 265, 266, 267, 268, 271, 272, 274, 277, 278, 280, 287, 292, 300, 309, 317, 318, 329, 330, 342, 362, 363, 365, 371, 373, 385, 393, 402, 417, 418, 419, 422, 423, 427, 428, 431, 434, 435, 462, 467, 477, 478, 479, 483, 497, 500, 502, 503, 506, 508, 509, 510, 513, 515, 517, 518, 523, 524, 525, 528, 529, 530, 531, 532, 533, 534, 535, 536, 538, 544, 548, 549, 550, 551, 552, 555, 559, 560, 563, 565, 567, 568, 570, 571, 572, 573, 574, 575, 578, 579, 580, 582, 583, 584, 585, 586, 603, 609, 621, 622, 632, 669, 670, 673, 677, 678, 681, 682, 684, 685, 694, 705, 706, 715, 724, 727, 730, 732, 734, 735, 738, 739, 742, 753, 759, 761, 764, 788, 790, 792, 793, 799, 811  
 ID Quantique, 602, 604, 614, 636, 639, 640, 689, 715, 725, 731, 732, 735  
 IDQ, 65, 551, 591, 600, 604, 608, 609, 630, 634, 635, 636, 637, 661, 671, 715, 815  
 Igor Dotsenko, 177  
 Immanuel Bloch, 194  
 Indeterminacy, 104  
 India, 42, 73, 296, 308, 414, 507, 554, 569, 570, 580, 582, 605, 636, 641, 673, 676, 721, 734, 735, 753, 764, 778, 787, 799, 817  
 Indium, 23, 110, 117, 269, 273, 350, 370, 386, 390, 393, 413, 416, 810  
 InfiniQuant, 604, 636, 696  
 Infotecs, 637, 721  
 InGaAs, 404  
 InnoLume, 400  
 Innovatus Q, 573, 731  
 Inria, 76, 83, 177, 255, 278, 280, 420, 521, 549, 591, 609, 617, 618, 623, 634, 697, 698, 699, 705, 708, 718, 726  
 Institut Néel, 11, 36, 67, 118, 177, 188, 193, 202, 230, 242, 251, 281, 292, 295, 304, 363, 369, 373, 376, 377, 381, 385, 389, 390, 405, 603, 703, 704, 718, 731, 747, 793, 797  
 Intel, 13, 15, 24, 65, 71, 84, 148, 156, 179, 180, 183, 189, 190, 224, 225, 235, 240, 249, 250, 252, 255, 275, 276, 281, 284, 288, 289, 368, 374, 385, 387, 388, 408, 419, 420, 421, 504, 505, 506, 507, 522, 550, 591, 598, 618, 634, 669, 673, 677, 679, 682, 685, 711, 735, 798  
 Intelline, 377  
 Intermodulation Products, 385  
 IonQ, 31, 64, 78, 87, 162, 181, 188, 213, 230, 233, 235, 239, 279, 287, 309, 310, 311, 313, 314, 315, 316, 317, 318, 321, 357, 360, 378, 476, 516, 521, 522, 524, 525, 528, 531, 570, 578, 580, 582, 633, 650, 669, 673, 683, 684, 685, 713, 759, 763, 810, 818  
 Jordanis Kerenidis, 11, 77, 78, 223, 473, 474, 476, 477, 535, 558, 559, 579, 698, 709, 718, 793, 806  
 iPronics, 399  
 iqClock, 653  
 IQM, 233, 252, 274, 507, 522, 695, 717, 793  
 Irfan Siddiqi, 64, 148, 258, 682  
 IRIF, 77, 698  
 ISARA, 637, 671, 687  
 Israel, 10, 55, 75, 255, 308, 384, 402, 440, 462, 557, 571, 636, 638, 639, 653, 715, 717, 721, 722  
 Italy, 10, 70, 104, 224, 261, 292, 301, 347, 369, 390, 402, 404, 405, 411, 419, 420, 556, 568, 608, 610, 647, 648, 673, 714, 717, 718, 719, 722, 753, 799, 832  
 ITMO University, 642, 720  
 Jacqueline Bloch, 66, 116, 118, 479, 793  
 Jacques Salomon Hadamard, 46  
 Jacqueline Romero, 69  
 James Chadwick, 44, 54, 687, 745  
 James Clerck Maxwell, 34, 121  
 James Clerk Maxwell, 41  
 Janine Splettstoesser, 177  
 JanisULT, 374  
 Japan, 10, 16, 43, 62, 85, 111, 117, 189, 193, 231, 241, 242, 248, 250, 252, 254, 255, 258, 260, 263, 281, 290, 299, 300, 308, 347, 375, 377, 380, 400, 404, 411, 414, 419, 436, 507, 510, 553, 568, 569, 571, 572, 573, 579, 583, 584, 586, 611, 632, 673, 675, 708, 725, 726, 727, 728, 729, 730, 753, 769, 800  
 Jason Alicea, 68, 217  
 Jason Petta, 284, 288  
 Jaw Shen Tsai, 725  
 Jay Gambetta, 213, 263, 529, 759  
 Jean Dalibard, 59, 60, 808, 811  
 Jean-Christophe Gougeon, 793, 801  
 Jean-François Roch, 71, 96, 190, 191, 655  
 Jean-Michel Gérard, 66  
 Jean-Michel Raymond, 59

- Jean-Philip Piquemal, 545, 582, 583  
 Jean-Philippe Poizat, 176  
 Jeffrey Hoffstein, 623  
 Jelena Vucokic, 70  
 Jérémie Guillaud, 278, 793  
 Jian-Wei Pan, 277, 351, 471, 612, 613, 628, 661, 723, 724  
 Jij, 246, 524, 573, 728  
 Jill Pipher, 623  
 Johann Balmer, 43, 745  
 John Bardeen, 56, 109  
 John Clauser, 58  
 John Frank Allen, 112  
 John Hartnett, 654  
 John Martinis, 64, 66, 241, 253, 265, 267, 271, 276, 287, 305, 754  
 John Pople, 544  
 John Preskill, 65, 74, 82, 89, 91, 184, 217, 233, 248, 255, 266, 267, 279, 305, 306, 449, 461, 479, 497, 524, 533, 538, 576, 812, 816  
 John Robert Schrieffer, 109  
 John Smolin, 529  
 John Stewart Bell, 43, 56, 58  
 John Von Neumann, 31, 37, 54, 56, 168, 745  
 John Watrous, 77  
 John Wheeler, 58, 96, 748  
 Jonas Landman, 473, 474, 477, 793  
 Jonathan Dowling, 19, 57, 247, 305, 348, 666, 679, 818  
 Jonathan Koomey, 25  
 JoS Quantum, 561, 573, 696  
 Jose Ignacio Latorre, 251  
 Joseph Bardin, 270, 382  
 Joseph Fitzsimons, 355, 526, 626  
 Joseph John Thomson, 44, 687  
 Joseph Larmor, 38  
 Joseph Silverman, 623  
 Joshua Nunn, 642  
 Juan Ariel Levenson, 176  
 Juan Cirac, 62, 308  
 Julia Kempe, 206, 472, 494  
 Julien Laurat, 221, 324  
 Jürgen Mlynek, 47, 66, 719  
 Kae Nemoto, 207, 209, 726  
 Kapton, 370, 380  
 Karoline Wiesner, 763  
 Katsumi Midorikawa, 726  
 Keio University, 727  
 Kelvin Nanotechnology, 275, 391, 406  
 Ketita Labs, 573  
 KETS Quantum Security, 637  
 Kevin Hartnett, 493, 495  
 Keysight Technologies, 406, 580  
 KiPu Quantum, 573  
 Kirill Tolpygo, 116  
 Kiutra, 369, 696  
 Klaus Mattle, 819  
 Kohei Itoh, 293, 316, 727  
 Kohki Okabe, 658  
 Konstantin Likharev, 428  
 Krishna Natarajan, 429  
 Kristel Michelsen, 76, 86, 183, 693, 719  
 Kristof Vandoorne, 437  
 Krysta Svore, 77, 307, 354, 451, 456, 763  
 Kuano, 574  
 Kun Huang, 116, 340  
 Labber Quantum, 406, 580  
 Lake Shore, 374, 394  
 LakeDiamond, 406  
 Lamb shift, 123  
 Laure le Bars, 719  
 Laure Le Bars, 763  
 Lawrence Livermore National Laboratory, 506  
 Le Si Dang, 118  
 Léa Bresque, 177, 793  
 Leiden Cryogenics, 373, 376, 378, 712  
 Leo Ducas, 623  
 Leo Kouwenhoven, 303, 305, 306, 711, 713  
 Léon Brillouin, 36, 55, 109  
 Leon Neil Cooper, 109  
 Leslie Lamport, 624  
 Lieven Vandersypen, 65, 284  
 Lighton, 182, 346, 438, 439, 670  
 LIGO, 50, 104, 650, 666  
 Lijun Ma, 628  
 Linus Pauling, 53, 543  
 LIP6, 11, 68, 71, 75, 76, 607, 610, 629, 631, 634, 698, 699, 726, 793  
 LORIA, 698  
 Louis de Broglie, 31, 32, 43, 44, 46, 47, 696, 747  
 Louis Néel, 703  
 Louisiana State University, 679  
 Lov Grover, 73, 465  
 Low Noise Factory, 385  
 LPMMC, 67, 326, 390, 703, 793  
 LSQC, 207, 214, 225, 226, 227, 597, 811  
 Luca De Feo, 623  
 Lucigem, 406  
 Ludwig Boltzmann, 36, 746  
 Lumibird, 398, 710  
 Luna Innovations, 400  
 Luxembourg University, 67  
 Lyman series, 94  
 Lytid, 400  
 Macquarie University, 406, 734  
 Madrid University, 67  
 Magic states, 74, 217, 807  
 MagiQ, 604, 637  
 Magneto-optical trap, 101, 221  
 Magnons, 57, 89, 108, 119  
 Majorana fermion, 305, 388, 483, 560, 812  
 Marc Kaplan, 75, 595, 642, 643, 793  
 Marco Lanzagorta, 665  
 Marcus Huber, 70  
 Maria Maffei, 176  
 Maria Schuld, 76, 358, 451, 477  
 Marie Curie, 31, 44, 56, 762  
 Marie-Anne Bouchiat, 66  
 Mark Keil, 648  
 Marki Microwave, 393  
 Martin Karplus, 544  
 Martin Weides, 390  
 Masahide Sasaki, 728  
 Masahiro Kitagawa, 727  
 Masahito Hayashi, 727  
 Matter waves, 746  
 Matthias Troyer, 77, 480, 481, 509  
 Maud Vinet, 11, 67, 282, 284, 290, 291, 292, 293, 294, 295, 389, 703, 704, 718, 792, 799, 801  
 Max Born, 31, 38, 44, 49, 50, 51, 53, 91, 98, 109, 149, 151, 152, 543, 747, 802, 804  
 Max Kelsen, 288, 673  
 Max Planck, 30, 31, 35, 38, 39, 40, 41, 88, 94, 121, 176, 572, 636, 659, 692, 695, 720, 745, 803  
 Maxime Richard, 118  
 Max-Planck Institute, 194, 326  
 Mazayr Mirrahimi, 76, 177, 203, 207, 208, 216, 255, 278, 280, 698  
 MDR, 569, 728  
 Meissner effect, 110  
 Menten.ai, 574  
 Mercury, 52, 108, 109, 307, 335, 416  
 MetaboliQs, 661, 695  
 Michael Freedman, 55, 73, 74, 305  
 Michael Levitt, 544  
 Michael Nielsen, 89, 352, 761, 796, 798  
 Michael P. Frank, 160, 229, 427, 430  
 Michael Rose, 623  
 Michel Bitbol, 744, 750  
 Michel Brune, 59  
 Michel Devoret, 64, 76, 189, 216, 253, 261, 278, 279, 281, 284  
 Michel Kurek, 673, 676, 793  
 Michele Mosca, 177, 248, 450, 585, 593, 594, 597, 598, 635, 797  
 Michelle Simmons, 66, 68, 285, 287, 733, 734, 763  
 Micro-Photons-Devices, 404  
 MicroQC, 717  
 Microsoft, 4, 13, 55, 68, 73, 74, 77, 78, 119, 157, 185, 192, 205, 216, 225, 232, 235, 240, 261, 281, 285, 287, 303, 304, 305, 306, 307, 315, 316, 317, 321, 354, 357, 373, 380, 383, 387, 388, 408, 421, 442, 444, 466, 480, 513, 518, 521, 522, 523, 524, 525, 550, 554,

- 560, 573, 574, 575, 579, 582, 585, 586, 623, 632, 633, 655, 669, 677, 679, 682, 685, 711, 713, 733, 734, 735, 738, 739, 753, 759, 763, 764, 790, 792, 796, 800, 802, 812  
 Mike Lazaridis, 637  
 Miklos Ajtai, 622  
 Miles Padgett, 662  
 Mio Murao, 727  
 Mirax, 404  
 Mirco Kutus, 668  
 Mixed state, 49, 136, 137, 138, 140, 141, 142, 143, 174, 175, 805, 812, 816  
 M-Labs, 406  
 Molecular Quantum Solutions, 574  
 Moritz Forsch, 627  
 Mosquito, 292  
 MPD, 404, 602  
 MtPellerin, 637  
 Multimode, 332, 334, 346, 400, 468, 490  
 Multiverse Computing, 329, 524, 574  
 Muquans, 20, 327, 563, 647, 648, 649, 650, 654, 706, 709, 719, 793  
 Nano-Meta Technologies, 407, 671  
 NASA, 85, 125, 203, 248, 250, 265, 267, 330, 403, 506, 563, 684  
 Nathan Rosen, 42, 55  
 Nathanaël Cottet, 257  
 NbTi, 111, 380  
 NEASQC, 718  
 neoLASE, 400  
 Netherlands, 10, 11, 16, 38, 48, 62, 65, 69, 108, 117, 121, 240, 242, 254, 275, 276, 277, 281, 295, 299, 304, 306, 308, 346, 363, 373, 376, 380, 383, 384, 385, 402, 403, 408, 420, 429, 477, 519, 571, 577, 579, 583, 610, 617, 618, 627, 650, 653, 670, 673, 681, 708, 709, 710, 711, 713, 718, 719, 753, 754, 757, 764, 799  
 NetraMark, 574  
 NextGenQ, 314  
 Niccolò Somaschi, 342, 401  
 Nicolas Gisin, 65, 222, 604, 614, 636, 735  
 Nicolas Treps, 71, 400, 665, 698  
 Nicole Hemsoth, 289, 360  
 Nicole Yunger Halpern, 756  
 NICT, 632, 726, 728, 729  
 Niels Bohr, 31, 42, 43, 44, 45, 51, 53, 55, 58, 88, 94, 104, 109, 121, 251, 290, 306, 403, 713, 744, 745, 746, 747, 803, 805  
 Niels Henrik Abel, 33  
 Niobium, 109, 110, 111, 112, 189, 232, 245, 273, 370, 380, 405, 409, 414, 415, 416, 432, 626  
 Niraj Kumar, 535  
 NISQ, 65, 84, 184, 185, 199, 207, 226, 252, 305, 322, 327, 350, 391, 445, 451, 453, 460, 468, 473, 480, 507, 538, 542, 545, 547, 570, 573, 582, 583, 584, 585, 586, 670, 681, 691, 706, 709, 718, 812  
 NIST, 20, 50, 64, 65, 101, 253, 286, 303, 321, 330, 344, 395, 397, 398, 406, 408, 434, 556, 565, 593, 597, 603, 605, 617, 618, 619, 620, 621, 623, 628, 631, 632, 633, 634, 635, 638, 642, 645, 646, 650, 652, 653, 658, 667, 679, 680, 681, 683, 684, 693, 699  
 Nitrogen, 26, 100, 109, 110, 111, 182, 190, 191, 192, 232, 296, 297, 298, 299, 300, 322, 363, 368, 370, 376, 377, 379, 394, 415, 416, 446, 479, 481, 544, 654, 655, 659, 661  
 NMR, 65, 177, 188, 299, 655, 761, 796  
 Nobuyuki Imoto, 728  
 Nokia, 261, 288, 304, 307, 610, 689, 718, 731, 786  
 Non-classical light, 813  
 Non-commutativity, 50, 54, 175  
 Non-destructive measurement, 106, 170, 208, 290  
 Nord Quantique, 281, 685  
 Nordic Quantum Computing Group, 574  
 Northwestern University, 212, 261, 684  
 Novariant, 574  
 NQCC, 690, 691  
 NSA, 22, 85, 243, 431, 433, 467, 564, 565, 590, 591, 593, 618, 621, 634, 681, 683, 684, 688, 705, 723, 735, 752  
 Nuclear magnetic resonance, 111, 188  
 NuCrypt, 638  
 NuQuantum, 638  
 Nvidia, 22, 26, 223, 224, 281, 408, 419, 420, 421, 506, 507, 508, 510, 523, 535, 544, 570, 582, 610, 799, 809  
 Oak Ridge, 223, 267, 417, 483, 484, 506, 521, 533, 566, 605, 682  
 ODE L3C, 574  
 Oded Regev, 622, 623  
 OEwaves, 400  
 Oleg Mukhanov, 390, 391, 392, 432  
 Oliver Heaviside, 35  
 Olivia Chen, 432  
 Olivier Guia, 375  
 ONISQ, 330, 681  
 Openreach, 632  
 OpenSuperQ, 260, 385, 695, 717  
 Optical molasses, 101  
 Orano, 710  
 Orbital angular momentum, 333, 343, 813  
 ORCA Computing, 357  
 Orch-OR, 768, 769, 770, 773  
 Origin Quantum Computing, 575  
 Origone, 638  
 Orbital angular momentum, 343  
 Oskar Langendorff, 775  
 OTI Lumionics, 575  
 Oxford Instruments, 274, 275, 283, 373, 375, 376, 378, 381, 391, 692  
 Oxford Ionics, 310, 322, 391  
 Oxford Quantum Circuits, 275, 390, 570, 671, 691, 692, 763  
 ParityQC, 329, 330, 575, 793  
 Pascal Febvre, 435  
 Pascale Senellart, 11, 67, 70, 118, 334, 337, 342, 343, 346, 350, 401, 403, 700, 763, 793, 799, 801  
 Paschen series, 94  
 Pascual Jordan, 44, 50, 53, 335, 749, 750, 818  
 Pasqal, 60, 67, 182, 184, 185, 188, 222, 225, 233, 237, 266, 275, 326, 327, 328, 329, 330, 331, 420, 472, 507, 522, 524, 564, 576, 583, 586, 648, 670, 675, 698, 701, 709, 717, 793, 801  
 PASQuanS, 328, 507, 717  
 Patrice Bertet, 11, 69, 222, 300, 793  
 Patrice Camati, 176  
 Paul Benioff, 36, 63, 72  
 Paul Dirac, 31, 37, 48, 51, 119, 120, 335, 687, 745, 746, 747, 804, 818  
 Paul Ehrenfest, 39, 48  
 Paul Kwiat, 819  
 Perimeter Institute for Theoretical Physics, 126, 686  
 Perola Milman, 69  
 Peter Selinger, 459, 508, 510  
 Peter Shor, 13, 64, 73, 74, 77, 155, 164, 467, 468, 484, 529, 585, 591, 593, 817, 818  
 Peter Zoller, 62, 177, 308, 321, 575, 576, 614  
 Phase Space Computing, 576  
 PhaseCraft, 576  
 Philipp Lenard, 41, 53  
 Philippe Duluc, 11, 792  
 Philippe Grangier, 11, 59, 60, 67, 71, 96, 176, 323, 338, 607, 641, 701, 702, 749, 793, 811  
 PhoG, 661  
 PhoQuS, 717  
 Photon number, 176, 331, 333, 334, 335, 336, 337, 338, 339, 342, 343, 344, 350, 662, 808, 818  
 Photon Spot, 407  
 Photanonometra, 406  
 Photonic, 68, 75, 89, 118, 236, 242, 300, 301, 313, 314, 317, 332, 340, 342, 345, 346, 347, 348, 351, 352, 356, 357, 358, 390, 399, 403, 404, 406, 437, 444, 447, 471, 574, 580, 601, 602, 603, 611, 615, 626, 628, 631, 633, 636, 637, 644, 650, 652, 653, 667, 682, 692, 693, 695, 702, 712, 717, 729, 771  
 Physically Unclonable Functions, 630, 631, 635  
 PicoQuant, 601, 604, 696  
 PiDust, 576  
 Pierre Bessière, 436  
 Pierre Rouchon, 698  
 Pieter Zeeman, 37  
 Pine.ly, 576  
 Planck constant, 40, 104, 235, 645, 646, 814  
 Planck distance, 40  
 Planck mass, 40  
 Planck time, 40  
 Plassys Bestek, 407, 710  
 Pol Forn-Díaz, 251, 793  
 POLARISqb, 576  
 Polaritons, 14, 66, 89, 108, 114, 115, 116, 117, 118, 340, 627, 717, 814, 816

- Post-Quantum, 588, 596, 597, 604, 616, 617, 618, 620, 623, 624, 625, 638, 683  
 PQ Solutions, 638  
 PQSecure Technologies, 638  
 PQShield, 638  
 Prevision.io, 577, 709, 792  
 Princeton, 55, 75, 181, 261, 281, 284, 288, 290, 303, 469, 492, 510, 657, 684  
 Projective-Valued Measures, 169, 175, 814  
 Projective measurement, 107, 147, 168, 169, 170, 207, 353, 354, 808  
 ProteinQure, 524, 546, 577  
 PsiQuantum, 64, 87, 185, 193, 213, 233, 235, 272, 332, 343, 345, 347, 355, 356, 357, 359, 447, 528, 673, 793, 808  
 Public key, 589, 590, 814  
 Purdue University, 154, 285, 306, 341, 385, 436, 683, 810  
 PVMs, 169, 175, 814  
 Pyotr Kapitsa, 112  
 Python, 358, 383, 406, 438, 501, 502, 507, 509, 510, 513, 514, 515, 518, 519, 520, 523, 524, 525, 569, 570, 572, 578, 586  
 Q.ANT, 399  
 Q1t, 577  
 Qabacus, 639  
 QAFS, 242, 681  
 Qaisec, 638  
 QAOA, 271, 274, 328, 384, 445, 468, 484, 532, 553, 555, 576, 578  
 Qasky, 639, 725  
 QBaltic, 581  
 QbitLogic, 578  
 Qblox, 182, 225, 232, 258, 277, 383, 712, 793  
 QBricks, 526  
 QC Ware, 77, 267, 318, 476, 477, 508, 524, 525, 551, 553, 579, 738, 798  
 QCaaS, 275, 523, 814  
 QCI, 64, 189, 233, 255, 281, 316, 521, 524, 715  
 Q-Ctrl, 277, 384, 578, 580  
 QDevil, 374, 381  
 QEO, 242, 565  
 QEYnet, 638  
 QFLAG, 718  
 QiKE Quantum, 639  
 Qilimanjaro, 237, 241, 242, 251, 390, 462, 715, 722, 793  
 Qindom, 579  
 Qiskit, 264, 265, 287, 288, 329, 330, 462, 464, 502, 504, 508, 515, 516, 517, 518, 524, 525, 549, 555, 559, 570, 575, 578, 582, 585, 586  
 QKD, 36, 60, 69, 70, 71, 339, 346, 397, 400, 403, 404, 405, 408, 428, 541, 551, 556, 582, 597, 604, 605, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 621, 624, 625, 632, 633, 634, 636, 637, 638, 639, 640, 641, 642, 643, 647, 648, 665, 670, 679, 682, 685, 686, 689, 695, 696, 698, 700, 701, 702, 707, 718, 720, 721, 722, 724, 725, 727, 728, 729, 730, 731, 732, 733, 738, 810, 811, 814, 816  
 Q-Lion, 407  
 QLSI, 67, 291, 292, 295, 691, 695, 712, 718  
 QMA, 461, 494, 527, 536, 815  
 QMICS, 718  
 Qnami, 655, 663, 670  
 Qombs, 717  
 Qontrol Systems, 400  
 QPhoX, 627, 670, 671, 712  
 QRANGE, 695, 718  
 Qrate Quantum Communications, 639, 721  
 Qrithm, 579  
 QRNG, 96, 582, 598, 599, 600, 601, 602, 603, 604, 605, 630, 634, 636, 637, 639, 640, 679, 743, 787, 815, 832  
 Qrypt, 600, 605  
 Qsimulate, 525, 547, 581  
 Qu&co, 579  
 Quacoon, 581  
 Quandela, 11, 60, 67, 70, 118, 182, 193, 225, 233, 341, 342, 344, 346, 347, 359, 401, 402, 403, 670, 675, 700, 709, 712, 763, 793, 799  
 Quantastica, 581  
 QuantERA, 255, 715, 719  
 Quanterro Labs, 580  
 QuantFi, 561, 580, 709  
 Quantica Computacao, 580  
 QuantiCor Security, 639, 696  
 Quantinuum, 87, 188, 321, 571  
 Quantiq, 581  
 QuantLR, 638  
 Quantonation, 281, 329, 357, 472, 580, 583, 627, 641, 663, 670, 709, 792, 793, 801  
 Quantopo, 582  
 Quantopticon, 580  
 Quantropi, 604, 605  
 Quantum Advantage, 22, 175, 204, 473, 534, 536, 682, 815  
 Quantum annealing, 91, 98, 107, 183, 184, 240, 241, 242, 243, 244, 245, 247, 248, 249, 250, 252, 265, 307, 417, 423, 424, 431, 436, 444, 447, 449, 467, 473, 475, 480, 494, 507, 514, 548, 562, 565, 566, 568, 573, 576, 579, 582, 586, 681, 722, 725, 726, 728, 729, 730, 802, 807, 809, 811, 815  
 Quantum Base, 631  
 Quantum Benchmark, 205, 215, 424, 580, 670  
 Quantum Blockchains, 639  
 Quantum Brilliance, 191, 239, 299, 300, 301, 581, 733  
 Quantum channel, 174, 175, 606, 613, 805  
 Quantum Computing Inc, 578  
 Quantum Dice, 605, 691  
 Quantum eMotion, 640  
 Quantum emulator, 265, 506, 510, 527, 555, 586, 815, 816  
 Quantum engineering, 10, 68, 759  
 Quantum Exchange, 632, 684  
 Quantum Factory, 322, 696  
 Quantum Field Theory, 119, 145  
 Quantum Impenetrable, 640  
 Quantum Internet Alliance, 68, 69, 647, 648, 718  
 Quantum Machines, 225, 384, 406, 503, 578, 721, 726, 799  
 Quantum Mads, 581  
 Quantum Matter Institute, 685  
 Quantum Microwave, 393, 718  
 Quantum Motion, 190, 233, 240, 258, 291, 295, 671, 692, 718, 793  
 Quantum Numbers Corp, 640  
 Quantum Open Source Foundation, 582  
 Quantum Opus, 403  
 Quantum postulates, 102, 796  
 Quantum Strategy Institute, 758  
 Quantum Thought, 581, 641  
 Quantum Trilogy, 640  
 Quantum Valley Investment Fund, 686  
 Quantum Xchange, 610, 640  
 QuantumCTek, 611, 639, 725  
 Quantum-South, 301, 581  
 QuantyCat, 582  
 Quaxys, 385  
 QuBalt, 581, 640, 696  
 Qubit Engineering, 524, 582  
 Qubit Pharmaceuticals, 582, 583, 709  
 Qubit Reset, 177, 459, 640  
 Qubitkk, 403  
 QuCube, 375, 704  
 Qudits, 148, 149, 188, 340, 343, 817  
 QuDoor, 639  
 QuDot, 583  
 QuEra Computing, 326, 331  
 Quintessence Labs, 601, 641  
 Quix, 346, 347, 402  
 QunaSys, 524, 583, 728  
 Qunat, 185, 817  
 Qunnect, 641, 670  
 QuNu Labs, 641  
 QuSecure, 641  
 Quside, 601, 604, 605  
 QuSoft, 533, 583, 709, 712  
 QuTech, 65, 185, 222, 276, 284, 285, 289, 383, 387, 408, 504, 511, 583, 711, 712, 761, 799  
 Qutrit, 817  
 QxBranch, 274, 583, 671, 691, 733, 734  
 Radboud University, 632  
 Radiall, 232, 380, 710  
 Rahko, 329, 472, 524, 525, 583  
 Rainer Blatt, 63, 308, 312, 314, 321, 526, 713  
 Raith, 408  
 Ralph Merkle, 429

- Raman, 310, 320, 325, 647, 774, 817  
 Raman transition, 817  
 Randomized benchmarking, 268  
 Ravel Technologies, 641  
 Ray Kurzweil, 27, 769  
 Rayleigh scattering, 817  
 Raymond Laflamme, 57, 210, 343, 349, 450, 686, 797  
 Raytheon, 330, 393, 427, 434, 563, 565, 632  
 ReactiveQ, 583  
 Rebecca Krauthamer, 581, 641  
 Reduced Planck constant, 51, 813  
 Rémi Richaud, 655  
 Renaud Sidney, 244  
 reversibility, 162, 228, 428  
 Reversibility, 35, 135, 162, 180, 228, 229, 230, 427  
 Review paper, 64, 114, 115, 253, 282, 297, 323, 338, 340, 345, 382, 427, 436, 485, 526, 557, 559, 560, 596, 605  
 Reza Azarderakhsh, 638  
 Richard Feynman, 12, 29, 57, 58, 62, 63, 72, 109, 119, 125, 442, 461, 617, 624  
 Rigetti, 31, 87, 161, 179, 189, 232, 235, 240, 252, 254, 272, 273, 274, 277, 278, 279, 281, 357, 373, 393, 430, 483, 499, 502, 503, 509, 513, 518, 519, 521, 522, 523, 524, 533, 551, 560, 568, 570, 574, 578, 579, 580, 582, 583, 584, 585, 586, 669, 671, 673, 678, 691, 733, 734, 739, 759, 799  
 RIKEN, 277, 281, 290, 419, 510, 726, 727, 729, 800  
 Riverlane, 391, 524, 583, 584, 671  
 Rob Schoelkopf, 236, 254, 255, 279, 281  
 Robert Andrews Milikan, 41  
 Robert Boyd, 662  
 Robert Dennard, 24  
 Robert McDermott, 259, 390, 391, 392  
 Robert McEliece, 617, 621, 638  
 Robert Young, 631  
 Roberto Ferrara, 614  
 Robin Cantor, 655  
 Rodney Van Meter, 316, 614  
 Roger Penrose, 750, 769, 770, 772, 815  
 Rolf Landauer, 26, 36, 63, 427, 428  
 Romain Alléaume, 609, 700  
 Romain Guérout, 124  
 RQuanTech, 584  
 RSA, 22, 85, 206, 217, 446, 458, 467, 468, 496, 558, 588, 589, 590, 591, 592, 593, 594, 596, 617, 622, 634, 681, 807, 817, 818  
 Rubidium, 20, 59, 66, 101, 103, 114, 148, 188, 221, 239, 323, 325, 326, 327, 408, 409, 413, 416, 628, 647, 650, 653, 654, 655, 657, 661, 721, 804  
 Rüdiger Schack, 746  
 Rudolph Clausius, 819  
 Ruhr-Universität Bochum, 193, 343, 632  
 Russia, 10, 289, 401, 403, 406, 411, 412, 432, 435, 637, 639, 641, 720, 721, 771, 776, 818  
 Ryan Babbush, 77  
 Rydberg, 69, 94, 118, 310, 323, 324, 325, 326, 327, 328, 329, 413, 524, 564, 654, 655, 668, 696, 705, 708, 714, 784, 817  
 Ryo Okamoto, 660  
 S2QUIP, 695, 718  
 Saarland University, 717  
 Saint-Louis University, 67  
 Samsung, 25, 26, 281, 293, 315, 321, 600, 604, 630, 632, 732, 790  
 Sandia Labs, 229, 230, 288, 314, 317, 680  
 Sapienza University, 70, 347  
 Sara Ducci, 69, 699  
 Sarah Sheldon, 71, 213, 536  
 Satyendranath Bose, 42  
 Scale-out, 20, 227, 237, 628  
 Scontel, 403, 721  
 Scott Aaronson, 12, 30, 75, 77, 82, 234, 267, 268, 315, 347, 426, 461, 492, 495, 526, 531, 579, 625, 741, 755  
 Sébastien Tanzilli, 70, 345, 707  
 Secure-IC, 618, 641, 709  
 SeeQC, 226, 229, 258, 275, 280, 385, 390, 391, 392, 393, 432, 584, 684  
 Semi-classical light, 818  
 Semicyber, 584  
 SeQureNet, 641  
 Serge Haroche, 59, 64, 65, 69, 234, 256, 466, 606, 683, 696, 776, 817  
 Serge Reynaud, 124  
 Sergey Bravyi, 74, 214, 217, 529, 534, 536, 812  
 Seth Lloyd, 63, 74, 75, 143, 175, 185, 218, 220, 341, 470, 473, 474, 476, 477, 485, 557, 664, 665  
 S-Fifteen Instruments, 408, 731  
 SFQ, 247, 390, 391, 392, 393, 431, 432, 433, 435, 436  
 Shabir Barzanjeh, 665  
 Shane Mansfield, 401  
 Shi Yaoyun, 76, 505  
 Shigeki Takeuchi, 660  
 SHYN, 585  
 Sigma-i Labs, 584  
 Silentsys, 399  
 Silicon Quantum Computing, 68, 287, 733, 734, 763  
 Silvano de Franceschi, 67, 282, 295, 389  
 Simon Gröblacher, 627  
 Singapore, 10, 16, 65, 67, 85, 118, 251, 308, 381, 399, 408, 437, 572, 573, 586, 611, 642, 648, 708, 713, 722, 730, 731, 734, 753, 757, 793  
 Single Quantum, 64, 102, 116, 136, 342, 403, 428, 461, 469, 712  
 SIRTEQ, 702  
 Sisyphus cooling, 101  
 Skyrmions, 89, 108  
 Smarts Quanttelecom, 641  
 Softbank, 729  
 SoftServe, 673  
 SoftwareQ, 585  
 SolidState.AI, 584  
 Sophia Economou, 78, 480, 484  
 South Korea, 10, 315, 419, 731, 753  
 South-Korea, 375  
 SPAD, 344, 404, 639  
 Sparrow Quantum, 342, 378, 403  
 Spectra Physics, 400  
 Spectral decomposition, 91, 132, 818  
 SpeQtral Quantum Technologies, 642  
 Spin Quantum Tech, 584  
 Spontaneous emission, 119, 120, 201, 325, 333, 601, 818  
 SQC, 66, 68, 190, 233, 240, 282, 285, 287, 734, 763  
 SQUID, 245, 254, 260, 280, 390, 428, 432, 655, 705, 709, 729, 819  
 SSH.COM, 642  
 Stabilizer codes, 207, 210, 211, 212, 217  
 Stable Laser Systems, 398  
 Stacey Jeffery, 472, 625  
 Stanford, 65, 70, 71, 76, 119, 216, 242, 250, 280, 303, 355, 359, 491, 510, 576, 580, 666, 727, 787, 800  
 State tomography, 149, 168, 172, 173, 206, 220, 816  
 Stefanie Barz, 71  
 Stefano Scotto, 655  
 Stéphane Louise, 244  
 Stephanie Wehner, 69, 625, 627  
 Stephen Shankland, 244, 318  
 Stephen Weisner, 819  
 Stephen Welsh, 663  
 Stephen Wiesner, 558, 629  
 Steve Lamoreaux, 122, 123  
 STFC, 265, 507, 691  
 Stimulated emission, 41, 333, 395, 396, 811, 813, 819  
 Stirling, 365, 373, 379  
 Strangeworks, 518, 574, 585, 793, 797  
 Stratum.ai, 585  
 Strontium, 415, 416  
 Stuart Hameroff, 769, 772  
 Sturm–Liouville, 92, 819  
 Super.tech, 585  
 Superoperator, 819  
 Supremacy, 12, 16, 65, 66, 74, 81, 85, 205, 223, 233, 249, 257, 265, 266, 267, 268, 271, 277, 305, 347, 349, 417, 497, 532, 533, 534, 535, 536, 585, 763, 765, 816, 832  
 Surrey Satellite Technology, 642  
 Taiwan, 10, 406, 635, 732  
 Takafumi Ono, 660  
 Taki Kontos, 296, 698  
 Tampere University, 399  
 Tanja Lange, 617, 618, 622, 625

- Technical University of Denmark, 635  
 Technical University of Munich, 369, 534, 692  
 Technion University, 55  
 Teledyne E2V, 385  
 TensorFlow Quantum, 266, 271, 329, 520  
 Terra Quantum AG, 574, 585  
 Thales, 11, 20, 71, 117, 248, 292, 376, 379, 477, 564, 610, 618, 621, 632, 641, 648, 655, 667, 668, 699, 701, 706, 709, 710, 718, 719, 793  
 Théau Peronin, 278, 704, 793, 801  
 Theodore Lyman, 43, 94, 745  
 Theodore Maiman, 56, 396  
 Thibaut Jacqmin, 627  
 Thierry Lahaye, 323, 324, 326  
 Thomas Kornack, 657  
 Thomas Vidick, 461  
 Thomas Young, 32, 687  
 Threshold theorem, 75, 215, 763  
 TII, 251, 722  
 Titanium, 109, 110, 111, 112, 232, 294, 370, 380, 414, 415, 416, 626, 653  
 Tohoku University, 436, 553, 584, 611  
 Tokyo Quantum Computing, 586, 728  
 Tommaso Calarco, 11, 693  
 Tommaso Toffoli, 63, 228, 428  
 Tomoyuki Morimae, 354, 626  
 Toptica Photonics, 398  
 Toshiba, 497, 556, 611, 613, 632, 636, 689, 729  
 Tracy Northup, 70, 614  
 Tradeteq, 586  
 Tristan Meunier, 11, 67, 282, 293, 295, 704, 792  
 Tsirelson's bound, 606  
 TSMC, 25, 26, 272, 296, 655, 732  
 TU Delft, 65, 69, 222, 251, 281, 282, 284, 285, 289, 295, 299, 303, 304, 385, 387, 407, 408, 478, 511, 548, 579, 583, 627, 681, 710, 711, 712, 713, 718, 797  
 TundraSystems, 357, 692  
 Two-Level Systems, 820  
 UCL, 281, 291, 292, 295, 649, 687, 689, 691, 718  
 UKRI, 556, 584, 691  
 Ultimaco, 642  
 Umesh Vazirani, 73, 248, 315, 461, 464, 526  
 Unconventional Computing, 14, 15, 27, 112, 361, 417, 793, 820  
 Uniform superpositions, 451  
 UnikLasers, 399  
 Uniqorn, 695, 718  
 Unitary Fund, 329, 560, 582, 586  
 Universal Quantum, 55, 74, 164, 179, 183, 185, 188, 207, 216, 233, 234, 248, 261, 278, 292, 314, 315, 322, 327, 353, 359, 448, 471, 479, 494, 499, 514, 519, 523, 533, 542, 577, 739, 750  
 University College London, 576  
 University of Alberta, 221, 686  
 University of Barcelona, 251, 714, 715, 722  
 University of Bath, 720  
 University of Birmingham, 649  
 University of Bristol, 359, 450, 576, 601, 606, 628, 634, 637, 691, 763, 764  
 University of British Columbia, 242, 685  
 University of Calgary, 686, 720  
 University of Cambridge, 62, 222, 291, 326, 340, 439, 576, 583, 638, 729  
 University of Chicago, 119, 212, 283, 511, 626, 684  
 University of Colorado, 65, 101, 321, 398, 680, 683  
 University of Copenhagen, 304, 381, 713, 718  
 University of Geneva, 222, 609, 614, 716  
 University of Glasgow, 53, 103, 242, 275, 390, 391, 400, 663  
 University of Illinois, 109, 506, 521, 534, 568, 683, 684  
 University of Innsbruck, 63, 70, 114, 177, 188, 213, 255, 308, 312, 313, 314, 321, 326, 507, 575, 681, 712  
 University of Maryland, 10, 20, 188, 239, 261, 309, 313, 315, 321, 442, 450, 526, 527, 565, 617, 662, 680, 681, 682, 683, 684, 713, 810  
 University of Michigan, 64, 76, 290, 505, 510, 656  
 University of Nottingham, 657  
 University of Oxford, 275, 314, 580, 605, 666  
 University of Queensland, 69, 149, 749  
 University of Science and Technology of China, 277, 639  
 University of Sheffield, 116, 633  
 University of Sherbrooke, 281, 626, 640, 656, 685, 686  
 University of Strathclyde, 688, 689  
 University of Stuttgart, 71, 326, 656  
 University of Sussex, 314, 322  
 University of Tennessee, 417, 582, 797  
 University of Tokyo, 119, 570, 726, 727, 729, 730  
 University of Twente, 346, 718  
 University of Washington, 78  
 University of Waterloo, 77, 526, 534, 597, 635, 665, 671, 686, 755  
 University of Wisconsin, 259, 326, 365, 390, 684  
 UNSW, 68, 281, 285, 286, 287, 314, 363, 368, 388, 466, 682, 686, 732, 733, 734  
 Urmila Mahadev, 526, 625  
 USA, 10, 11, 16, 27, 38, 47, 48, 54, 55, 66, 67, 73, 81, 85, 104, 112, 114, 117, 177, 188, 189, 229, 235, 241, 244, 253, 260, 265, 272, 274, 276, 279, 281, 285, 288, 289, 290, 299, 300, 301, 304, 307, 308, 309, 315, 321, 326, 330, 331, 347, 355, 356, 357, 368, 373, 374, 375, 376, 377, 378, 379, 385, 390, 393, 395, 398, 399, 400, 403, 404, 406, 407, 408, 413, 414, 415, 416, 419, 421, 424, 426, 432, 434, 435, 439, 456, 462, 471, 491, 503, 506, 507, 508, 516, 533, 543, 547, 549, 554, 555, 556, 563, 568, 569, 572, 574, 576, 578, 579, 580, 581, 582, 583, 584, 585, 586, 593, 604, 605, 608, 610, 627, 633, 634, 635, 637, 638, 639, 640, 641, 650, 653, 654, 656, 657, 658, 662, 665, 666, 669, 670, 673, 675, 676, 677, 678, 679, 681, 682, 684, 685, 686, 687, 691, 708, 713, 720, 721, 727, 728, 735, 739, 744, 753, 754, 755, 756, 757, 758, 761, 762, 764, 765, 776, 778, 780, 782, 787, 790, 810, 832  
 USTC, 277, 298, 612, 639, 723, 725  
 Valentina Parigi, 698  
 Valérian Giesz, 401, 793  
 Van der Waals, 124  
 Vapor Cell Technologies, 408  
 Vasilii Semenov, 428  
 VeriQloud, 11, 75, 76, 357, 629, 642, 643, 698, 709, 763, 793  
 Verizon, 556, 632  
 Virginia D'Auria, 70  
 Virginia Tech, 78, 684  
 VIRGO, 104  
 Vladimir Fock, 50, 53, 119, 335, 802, 818  
 Vladimir Soukharev, 623  
 VLC Photonics, 404  
 VQA, 483, 820  
 VQE, 186, 274, 356, 384, 444, 445, 473, 480, 483, 484, 503, 546, 555, 579, 815, 820  
 Walter Kohn, 543  
 Walther Meissner, 110  
 Walther Nernst, 121  
 Wavepackets, 94, 133, 339, 804  
 Wave-particle duality, 12, 14, 32, 44, 47, 56, 61, 66, 88, 89, 96, 97, 100, 102, 104, 107, 130, 145, 646, 744, 745, 747, 755, 772, 804, 832  
 Werner Heisenberg, 31, 44, 48, 50, 51, 53, 104, 109, 126, 692, 744, 745, 746, 747  
 whurley, 585  
 Wien's displacement law, 94  
 Wilhelm Wien, 94, 821  
 Willard Gibbs, 35  
 William Hurley, 585, 797  
 William Rowan Hamilton, 33  
 William Wootters, 106, 612  
 Willis Eugene Lamb, 123  
 Wojciech Zurek, 58, 61, 106, 212, 741  
 Wolfgang Paul, 62, 308, 311  
 Wolfgang Pauli, 47, 48, 53, 119, 121, 745, 747, 802  
 Xanadu, 76, 193, 338, 347, 358, 524, 525, 574, 577, 582, 586, 610, 673, 675, 687, 712  
 Xilinx, 383, 385, 387, 421  
 Xofia, 586  
 XT Quantech, 643  
 Yakov Frenkel, 116  
 Yanhua Shih, 20, 662  
 Yasuhiko Arakawa, 727  
 Yasunobu Nakamura, 189, 254, 725, 726, 727  
 Yianni Gamvros, 552, 579  
 Yonsei University, 262  
 Yoshihisa Yamamoto, 242, 727

- Ytterbium, 222, 261, 307, 313, 315, 318, 319, 320, 400, 409, 414, 416, 614, 653  
Yuichi Nakamura, 730  
Yulin Wu, 277  
Yuri Alexeev, 669  
Yuri Manin, 57, 63, 73, 442  
Yuri Pashkin, 725  
Zaki Leghtas, 76, 177, 207, 216, 255, 278, 280, 698
- Zapata Computing, 75, 321, 555, 586, 820  
Zeno Toffano, 701  
Zheng Tan, 177  
Zheng-Ping Li, 661  
Zurich Instruments, 182, 198, 225, 232, 258, 382, 383  
ZX calculus, 501, 570, 821  
ZY4, 643  
Zyvex Labs, 408

# ***Revisions history***

This ebook improved over time with successive revisions. The first editions from September 2018, 2019 and 2020 were published in French and this fourth one is the first published in English, as will be the next ones. It is freely downloadable with the latest version on:

<https://www.oezratty.net/wordpress/2021/understanding-quantum-technologies/>

Three different PDF formats are available: **A4 in full resolution** (71 Mb), **A4 in reduced resolution** (but it doesn't fit under the 32 Mb threshold for some ebook readers) and in **Letter format** for USA and Canada readers who would like to print it. It's also available in Letter format on **Arxiv** at <https://arxiv.org/abs/2111.15352>.

You can also order printed paperback editions on most **Amazon** market place sites.

Version and date	Modifications
1.0 (332 pages) September 29th, 2018	First version of this document published in French and consolidating 18 posts published between May and September 2018 on <a href="http://www.oezratty.net">www.oezratty.net</a> .
2.0 (504 pages) September 20th, 2019	Second edition, also in French. New content on superconductors, superfluidity, quantum sensing, quantum supremacy, quantum computing emulation, cryogeny, hybrid algorithms, algorithms certification, quantum teleportation, blind computing. Addition of a glossary and bibliography.
3.0 (684 pages) September 7th, 2020	Third edition, also in French. New content on Maxwell, Schrödinger and Dirac's equations, relativistic quantum chemistry, how research works, lasers and masers, polaritons, extreme quantum, linear algebra, quantum gates classes, quantum error correction codes, cryo-electronics, MBQC, quantum cloud, qubits technologies, unconventional classical computing, quantum hype cycle, quantum foundations and on the influence of science fiction.
4.0 (800 pages) September 27th, 2021	Fourth edition, the first one in English. Main new features vs the 3.0. on top of updates nearly everywhere:  New section on <a href="#">quantum physics postulates</a> , page 89.  More on <a href="#">wave-particle duality</a> , page 95 and on <a href="#">photon qubits physics</a> , page 332.  Improvements and extensions on <a href="#">linear algebra</a> , page 130, on <a href="#">quantum measurement</a> page 168, and <a href="#">quantum memory</a> , page 218. New part on <a href="#">vacuum</a> in enabling technologies, page 394.  Much improved section on <a href="#">algorithms</a> , including <a href="#">data preparation</a> and <a href="#">debugging</a> , page 451 and page 527.  Expanded part on <a href="#">QRNG</a> , page 597.  Went from 265 to over 450 vendors covered in the various sections of the ebook.  More on <a href="#">ethical issues</a> , page 751, and <a href="#">gender balance</a> , page 762.  Additional covered countries: <a href="#">Belgium</a> , <a href="#">Portugal</a> , <a href="#">Italy</a> and <a href="#">Abu Dhabi</a> and nice ecosystems maps for the USA and the UK.  Added an <a href="#">index</a> with company names, people and some scientific terms and many terms in the <a href="#">glossary</a> (from 179 to >280).

4.1 (836 pages) October 5th, 2021	<p>Added 36 (single volume)/48 (two volumes) pages for the sake of making it easier to print the document and in two volumes for Amazon printing services.</p> <p>In order to fit Letter format printing, I had to shorten a bit the page height, adding more pages. I also enlarged many illustrations to make it readable in printed version.</p> <p>The two-volumes printed version of the ebook is made available to purchase at an affordable price on most <b>Amazon</b> sites.</p> <p>Added a new graph explaining Dirac <math>\langle A B C \rangle</math> notations in the <a href="#">measurement section</a> starting page 168.</p> <p>Added a roadmap for managing the <a href="#">energetic footprint</a> of quantum computing, after page 226.</p> <p>Added American Binary (Ambit) in the <a href="#">quantum cryptography</a> vendors section that starts page 631.</p> <p>Some company logo updates like with Qilimanjaro.</p> <p>Some additional spellchecks and scattered text edits.</p>
4.2 (836 pages) October 10th, 2021	<p>Added some logos in the qubits vendors map page 239 and some US universities in the US map on page 684.</p> <p>Added a small update related to D-Wave gate-based quantum computing announcement in the quantum annealing section that starts page 241.</p> <p>Added Energetics of quantum technology, Quantum postulates, QML, QLM and scale-out in the glossary. Corrected wrong naming for Atos QLM (instead of Atos QML or Atos aQML).</p> <p>Update on Origin Quantum and their cloud quantum emulation offering.</p> <p>Small scattered edits elsewhere.</p>
4.3 (836 pages) October 11th, 2021	<p>Added StarX Electronics in the inventory of <a href="#">enabling technology vendors</a>, starting page 405 and Chipiron in quantum sensing imaging, starting page 658.</p> <p>Added Two-Level Systems in glossary.</p>
4.3 (836 pages) October 17th, 2021	<p>Minor edits, in quantum management, page 784, and various other places.</p> <p>Added a nice chart from Joseph Bardin describing the various microwave and other signals used to drive superconducting, electron spin and trapped ions qubits, on page 382.</p>
4.4 (836 pages) November 2nd, 2021	<p>Added Algorithmic qubit, anharmonic oscillator, cQED, CQED, fluxonium, Q-factor, Dirac and Reduced Planck constants, homodyne detection and Universal quantum computer in the glossary. Updated some funding data with some startups (with the help of TheQuantumInsider). Some minor spelling tweaks. News on D-Wave Clarity roadmap. Some technical details additions to superconducting qubits.</p>
4.5 (836 pages) December 1st, 2021	<p>Many updates on IBM and its 127 qubits processor announced in November 2021, the related <a href="#">qubits fidelities chart</a> with the best-in-class IBM 27, 65 and 127 QPUs.</p> <p>Some updates on IQM and OQC (on Amazon Braket).</p> <p>Updates on Kipu Quantum and on Quantinuum (new name for HQS/CQC merger).</p> <p>Added a mention on Alexia Auffèves <a href="#">quantum energetics initiative</a>.</p> <p>Some typos corrections submitted by Wyman Kwok from Hong Kong.</p>

I update the book on a regular basis as I find editorial issues, mistakes, misspellings and the likes. You can submit me any comment, correction suggestion or even request for digging into some un-tapped topic ([olivier@oezratty.net](mailto:olivier@oezratty.net)).

back-cover flip page

# le lab quantique

|0>

|1>

|0>

|1>