Understanding Quantum Technologies

Sixth edition

Key takeways

2023

Olivier Ezratty

le lab quantique

le lab quantique

Le Lab Quantique is a supporter and promoter of this book, but not its publisher or editor.

Understanding Quantum Technologies

Sixth edition

Key takeaways

2023

Olivier Ezratty

About the author

Olivier Ezratty
consultant and author
0000-0003-3944-2896
olivier (at) oezratty.net, www.oezratty.net, @olivez
+33 6 67 37 92 41

Olivier Ezratty advises and trains various public and industry organizations in the development of their innovation strategies in the quantum technologies realm. He brings them a rare 360° understanding of the scientific, technology, market and ecosystems dimensions of this burgeoning and complex domain.

He covered many other topics since 2005, like digital television, Internet of things and artificial intelligence. As such, he carried out various strategic advisory missions of conferences or training in different verticals and domains such as **media and telecoms** (Orange, Bouygues Telecom, TDF, Astra), **finance and insurance** (BPCE, Société Générale, Swiss Life, Crédit Agricole, Crédit Mutuel-CIC, Generali), **industry and services** (Schneider, Camfil, Vinci, NTN-STR, Econocom, ADP, Air France, Airbus) and the **public sector** (CEA, Météo France, Bpifrance, Business France).

He became a quantum technologies specialist in 2018 with many complementary activities:

- **Author** of the reference book **Understanding Quantum Technologies** (September 2021, 2022 and 2023) following three previous editions in French in 2018, 2019 and 2020. The 2021, 2022 and 2023 editions are also available in paperback version on Amazon.
- **Trainer and teacher** on quantum technologies for **Capgemini Institut** and for **CEA INSTN**. In September 2021, he took in charge an elective curriculum on quantum technologies for **EPITA**, an IT engineering school in France.
- **Speaker** in a large number of quantum technology events since 2018 such as the Q2B Paris organized by QC Ware, France Quantum and other events, on top of presentations at Société Générale, BNP, Crédit Agricole, Michelin, Adéo, L'Oréal, FIECC, IHEDN, Business France, CentraleSupelec, Avolta Partners, IHEDN, etc.
- **Producer** of two series of podcasts on quantum technologies along with Fanny Bouton (in French): a monthly « Quantum » on tech news (since September 2019) and Decode Quantum, with entrepreneurs and researchers since March 2020, with a total of over 100 episodes as of July 2023.
- **Cofounder** of the **Quantum Energy Initiative** with Alexia Auffèves (CNRS MajuLab Singapore), Robert Whitney (CNRS LPMMC) and Janine Splettstoesser (Chalmers University, Sweden).
- **Expert** for **Bpifrance** to evaluate quantum collaborative projects and startups.
- **Ambassador** for France 2030 since February 2022, the French government innovation strategy plan.

He also lectures in various universities such as CentraleSupelec, Ecole des Mines de Paris, Telecom Paristech, Les Gobelins, HEC, Neoma Rouen and SciencePo, on artificial intelligence, entrepreneurship and product management (until 2020) and on quantum technologies (since 2018), in French and English as needed. He is also the author of many open source ebooks in French on entrepreneurship (2006-2019), the CES of Las Vegas yearly report (2006-2020) and on artificial intelligence (2016-2021).

Olivier Ezratty started in 1985 at **Sogitec,** a subsidiary of the Dassault group, where he was successively 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 a strong experience in many areas of the marketing mix: products, channels, markets and communication. He launched in France 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, 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 CentraleSupelec 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

Credits

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

This document contains nearly 900 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 credited 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 in that case.

Table of contents

About these key takeaways

“Understanding Quantum Technologies” was released at the end of September 2023 in its 6th edition. This version is 1360 pages long and is available as a free to download PDF in various formats (A4, Letter, single or three volumes) here:

https://www.oezratty.net/wordpress/2023/understanding-quantum-technologies-2023/

This book is a kaleidoscope for quantum technologies with a 360° perspective encompassing historical, scientific, technological, engineering, entrepreneurial, geopolitical, philosophical, and societal dimensions. It is not a quantum for dummies, babies, or your mother-in-law book. It mainly targets three audiences: information technologies (IT) specialists and engineers who want to understand what quantum physics and technologies are about, and decipher its ambient buzz, all participants to the quantum ecosystem from researchers to industry vendors and policy makers, and at last scientific students who would like to investigate quantum technologies as an exploratory field.

It is a very large book but it can also be considered as a collection of books. One on quantum physics (140 pages), another on quantum computing hardware (344 pages), one on quantum computing programming and software (270 pages), yet another one on quantum communication and cryptography (94 pages), on quantum sensing (49 pages, we are here in the "novel" format), on quantum geopolitics (99 pages), a directory of quantum industry vendors (664 are described in the book), etc. But they are all tied together in a consistent manner!

For your convenience, I have extracted the key takeaways that are at the end of each part and included a key illustration in this short version to create this special edition of the book.

Olivier Ezratty

September 2023

Why…

- This book is unique in its shape, structure and length. It covers quantum technologies with a 360° approach. It is more scientific than most broad-reach publications, outside research review papers. It is a good appetizer for those who want to investigate the matter whatever the angle. It contains an extensive bibliography with over 3,200 scientific papers. It tries to answer many commonplace questions that are not well addressed in broad audiences scientific publications.
- All existing digital technologies are already based on quantum physics. They are part of the "first quantum revolution" including transistors, lasers and the likes, leveraging our control of light-matter interactions with large ensembles of quantum objects (electrons, atoms, photons). So, your laptop, smartphone, digital camera, television and other digital objects are already "quantum". The "second quantum revolution" corresponds to a new generation of technologies that are using a variable mix of superposition, entanglement and individual quantum objects control. It usually contains quantum computing, quantum telecommunications, quantum cryptography and quantum sensing. Quantum matter applications are a new addition to this list.
- Quantum technologies are at the crossroads of many scientific domains encompassing physics, mathematics, computing, social and economics 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 book targets broad audiences with a technical background, including computer science engineers, but also quantum physicists and quantum information scientists who want to have a look at what is happening broadly in the field and its burgeoning ecosystem.
- Quantum computing is based on a promise to solve so-called intractable problems whose (classical) computing complexity grows exponentially with their size. These can't be solved with classical computing, whatever happens with Moore's law. But we are not there yet since there are several enormous challenges to overcome to scale quantum computers beyond what can be done today. In the interim, some marginal improvements may come with noisy intermediate scale computers, including better and more precise solutions in several domains. Analog quantum computers may be first to bring a moderate quantum advantage.
- Moore's law has not ended yet, particularly with regards to the number of transistors per chips. Classical computing still strive compared to existing and future quantum computers when dealing with large volumes of data.
- 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, particularly with superconducting qubits.

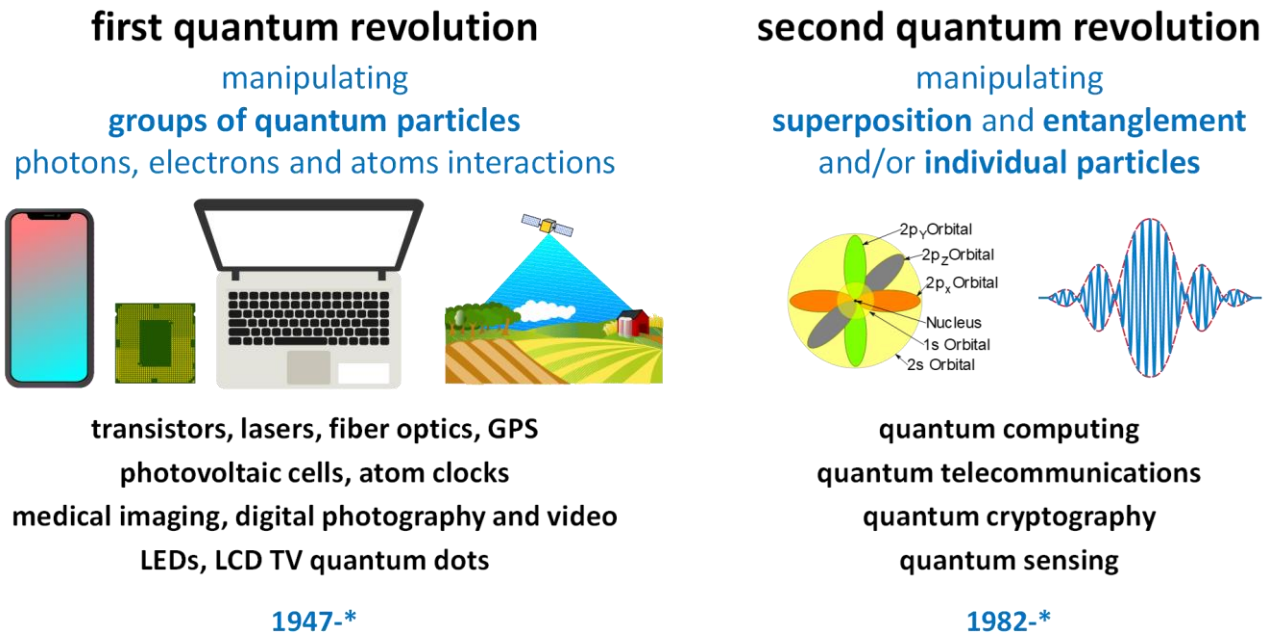


Figure 1: first and second quantum revolution definition and related use cases. (cc) Olivier Ezratty, 2020-2023.

Quantum physics history and scientists

- A first wave of 19th 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 19th century unexplained physics experiments.
- These scientists were theoreticians while many lesser-known researchers were experimentalists with landmark discoveries (superconductivity, electron interferences, Stern-Gerlach experiment, ...). Quantum physics also relies on a significant body of mathematics like linear algebra and group theory.
- 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, new breeds of technologies were created, most of them belonging to the "quantum information science" field and being part of the second quantum revolution. Many of these research programs were funded by governments after Peter Shor's integer 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 countries across several continents (North and South America, Europe, Asia/Pacific).
- This book also describes how research works in general and particularly in quantum physics and information science. It explains how scientific papers are written and communicated, how researchers are evaluated, and how quantum technologies readiness level can be assessed.

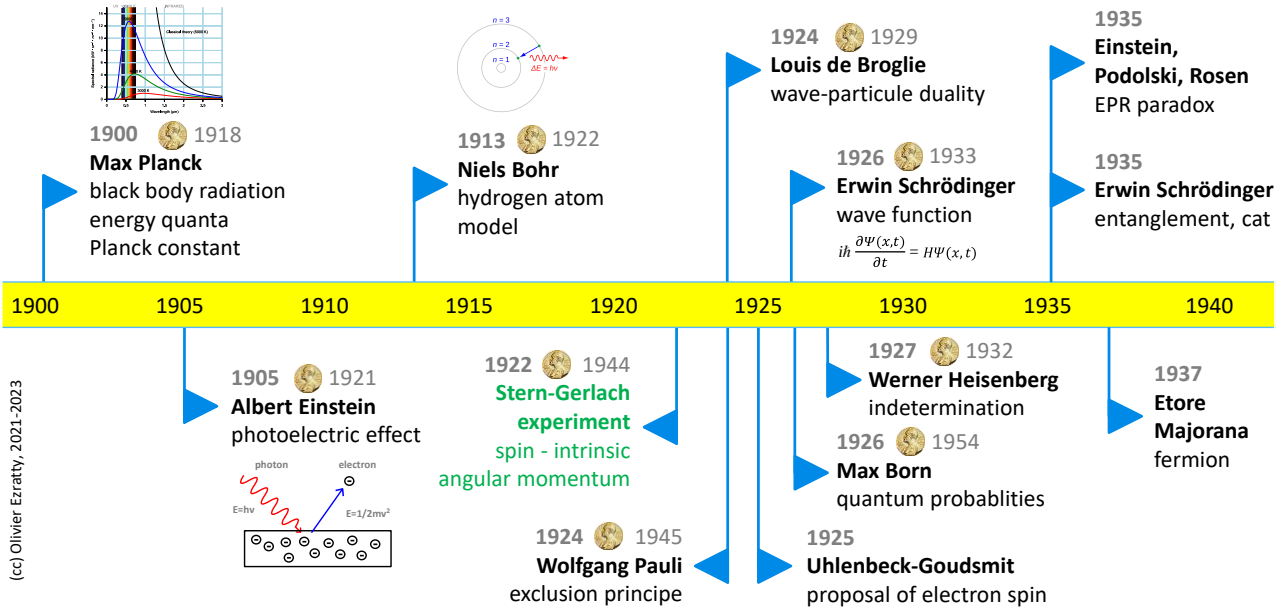
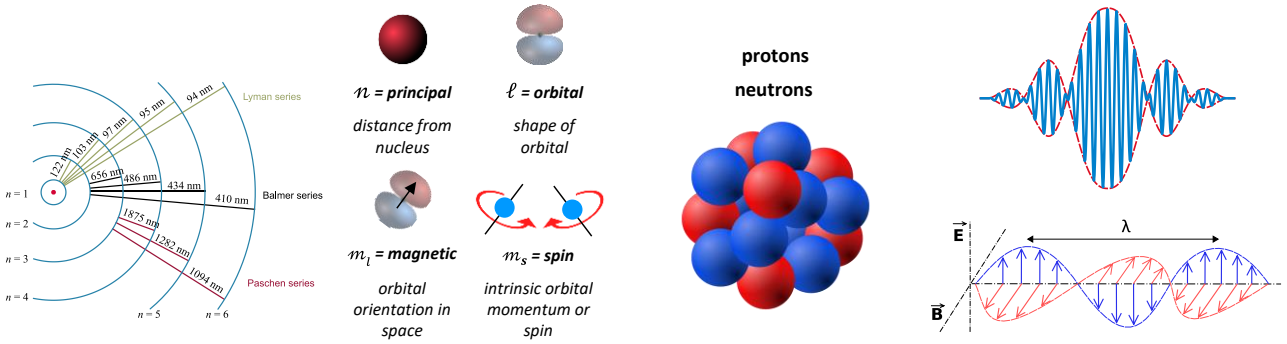


Figure 2: quantum physics foundational years timeline. (cc) Olivier Ezratty, 2021-2023.

Quantum physics 101

- 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 interpretations in quantum physics. One big underlying question is "what is reality". But although deemed incomplete, the theory has been validated by an incredible number of experiments and with extreme precision.
- Quantum physics describes the behavior of matter and light at nanoscopic levels, but it can in some conditions extend to larger objects like molecules or even artificial atoms like superconducting current, Bose Einstein condensates and the likes. 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, ...). We however don't use this level of granularity in quantum technologies.
- 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 its consequences like superposition and entanglement. Atoms, electrons, nucleons and photons have several quantum numbers describing their properties. However, quantum objects can have continuous variables. By the way, a cat cannot be both alive and dead since it is not a nanoscopic quantum object. Forget the cat and instead, learn Schrodinger's equation!
- The Heisenberg indetermination principle states that it is 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 and in other quantum photonics fields and sensing.
- 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. You find there a wealth of strange phenomenon such as skyrmions, magnons, topological insulators and quantum batteries. They could lead to a new chapter in the second quantum revolution.
- 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.



atoms and ions	electrons		nucleons		photons
discrete transitions energy levels between electron shells observed in spectrography	principal number	———	shell number		mass and electric charge = 0
	orbital quantum number	—	orbital angular momentum	———	orbital angular momentum wavelength
	magnetic quantum number	—	magnetic quantum number		
	spin projection (up, down)	———	spin	———	spin angular momentum (polarization)

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

Figure 3: quantized properties of atoms, electrons, nucleons and photons, and some quantum numbers correspondence between electrons, nucleons and photons. (cc) Olivier Ezratty, 2022-2023, with Wikipedia images source.

Gate-based quantum computing

- 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. Algorithms are implemented with series of quantum gates called "cirtuits". The main 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, complex numbers, vectors and matrices. 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 with using conditional multi-qubit gates like the CNOT gate. These relationships are persistent in time during the execution of an algorithm.
- A qubit register of N qubits can store a linear superposition of 2^N basis states corresponding to the qubit computational basis, each associated with a complex number. But surprisingly, this exponential growth in size is not enough to create a potential polynomial or exponential speedup with quantum computing. You need a lot of entanglement and some non-obvious quantum gates like the T gate and so-called maximally entangled states to obtain interesting speedup. The non-locality of quantum entanglement can also explain part of the speedup of quantum computers.
- 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. You have to deal with it when designing quantum algorithms.
- Computation must usually be done a great number of times (at least in the NISQ regime) and its results averaged due to the probabilistic nature of qubits measurement. The number of "shots" however depends on the algorithm results, programming paradigm and type of error correction or error mitigation.
- Qubits measurement can be done in various ways, the main one being a classical projective measurement, if possible, a non-demolition one (QND) that will maintain the qubit in its collapsed state after measurement and not destroy it. Other techniques are used that are useful for qubits quality characterization and for quantum error corrections like a quantum state or quantum gate tomography.

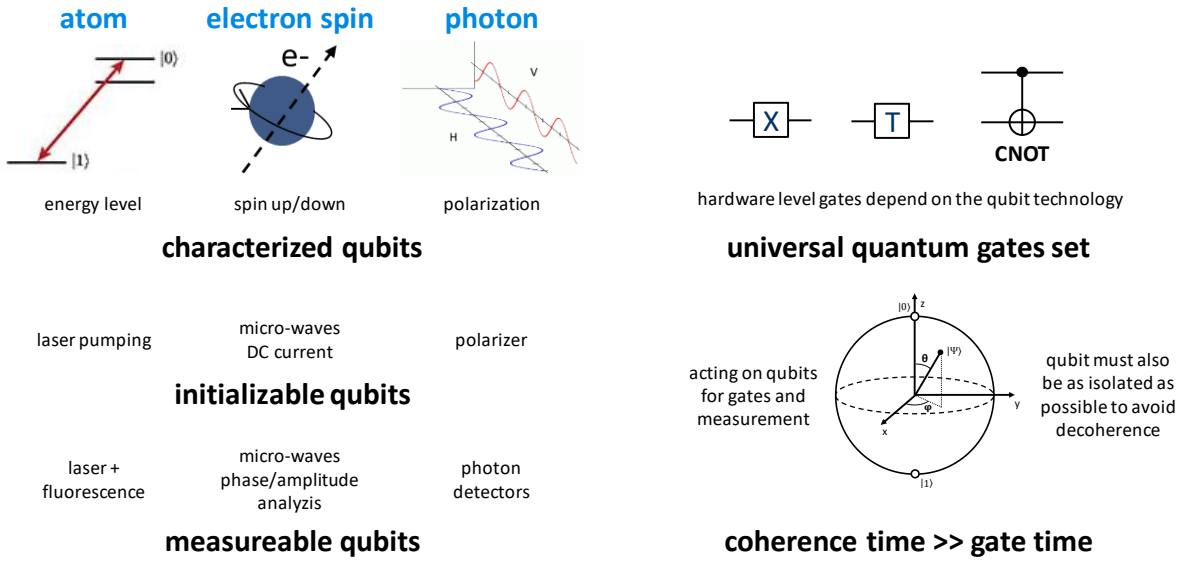


Figure 4: DiVincenzo gate-based quantum computing criteria. (cc) Olivier Ezratty, 2021, inspired by Pascale Senellart.

Quantum computing engineering

- 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-levels 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 (for solid-state qubits but also for trapped ions), vacuum enclosures (particularly with cold atoms and trapped ions) or waveguides (photons), usually housed in a cryogenic vacuum chamber (with the exceptions of photons and some NV centers), some electronics sending laser beams or coaxial cables guided microwaves or direct currents onto qubits and a classical computer driving these electronic components.
- Since qubits are noisy, scientists have devised quantum error correcting (during computing) and quantum error mitigation (after computing) schemes. Quantum error correction relies on creating logical "corrected" qubits composed of a lot of physical qubits, up to 10,000. The number of physical qubits per logical qubit depends on many parameters: the algorithm size and its error rates requirements, the quantum error correction code type and the qubits connectivity. This creates huge scalability challenges, many of them with classical enabling technologies like cabling, electronics and cryogeny. The science of quantum error correction, quantum error mitigation and fault-tolerant quantum computing is a realm in itself.
- 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 and are at a very early research stage.
- 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, control electronics, cabling as well as the available space to house cabling and cryo-electronics. This explains the creation of the Quantum Energy Initiative in 2022, which created a community of researchers and industry vendors and organizations working collectively on this topic.
- 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 actual algorithm speedups when including all end-to-end computing operations.

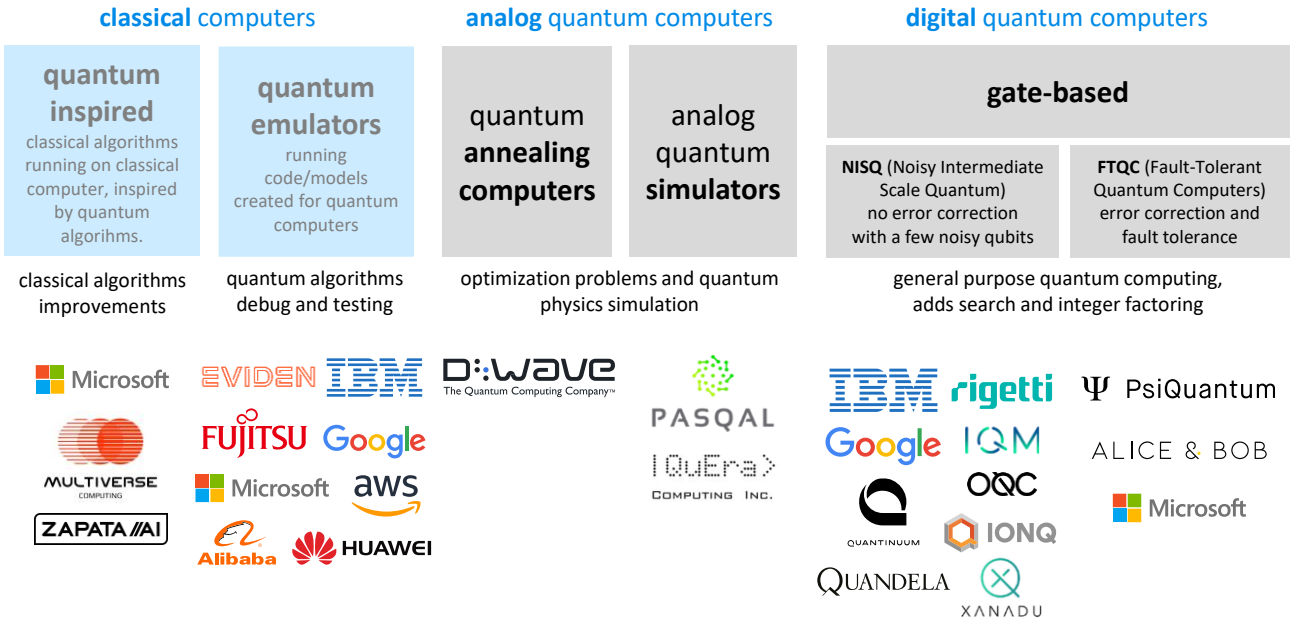


Figure 5: the different computing paradigms with quantum systems, hybrid systems and classical systems. (cc) Olivier Ezratty, 2022-2023.

Quantum computing hardware

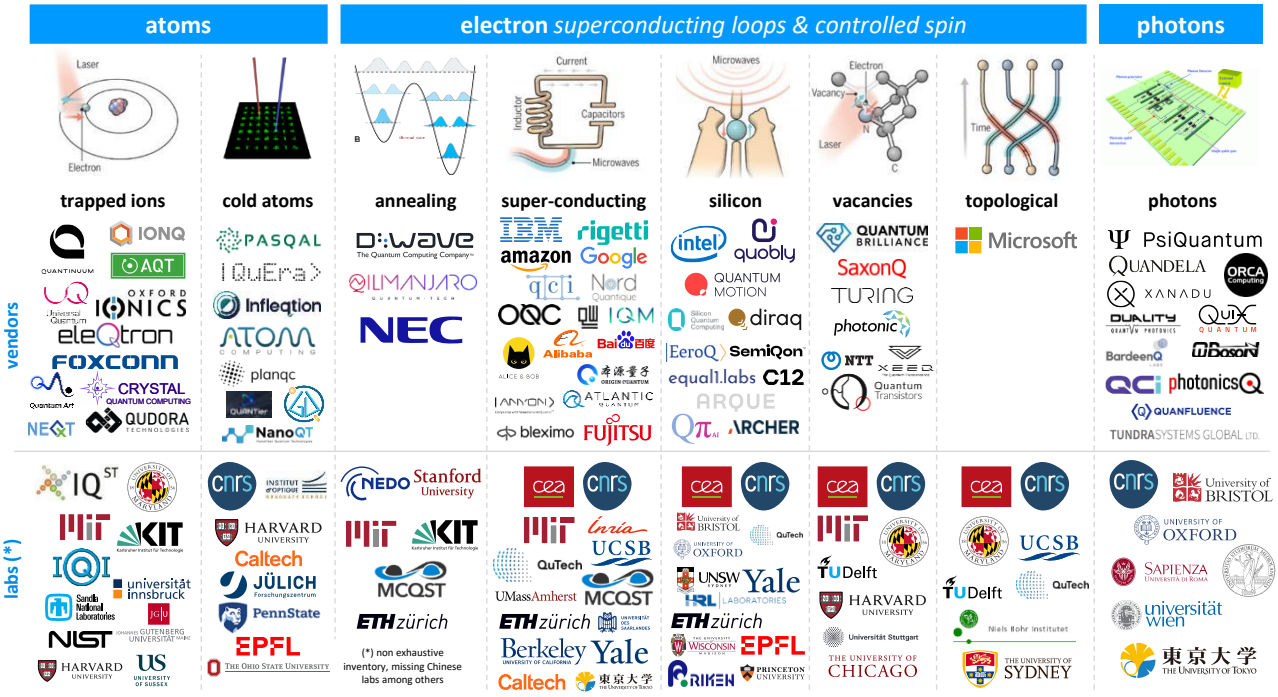


Figure 6: a map of key research lab and industry vendors in quantum computing hardware per qubit type. (cc) Olivier Ezratty, 2023. Qubits drawing source: Scientists are close to building a quantum computer that can beat a conventional one by Gabriel Popkin in Science Mag, December 2016. I consolidated the logos lists since 2018. It is incomplete for the research labs at the bottom but rather exhaustive for the vendors at the top. It doesn't list China academic labs.

- Superconducting qubits are the most common nowadays, implemented by IBM, Google, Rigetti, IQM and Origin Quantum among others. But they are noisy and do not scale well. One solution may be bosonic qubits like the GKP and cat-qubits which combine trapped microwave photons in cavities and superconducting qubits for their manipulation and readout (Alice&Bob, AWS and Nord Quantique). Also, the fluxonium qubits breed seems to generate some traction with work from Alibaba (China) and Atlantic Quantum (Sweden/USA).
- Quantum dots 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 however been demonstrated only at a very low scale at this stage.
- NV centers qubits have the benefit to be stable and to work potentially at ambient temperature. An increasing number of startups are playing in this field, like Quantum Brilliance (Australia and Germany).
- Topological qubits could bring the benefit of being resilient to some quantum errors and to scale better than other solid-state qubits. 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 about 40 qubits, at least with their main vendor, IonQ, Quantinuum and AQT.
- Cold atoms qubits are mostly used in quantum simulation where it could scale up to a thousand qubit and it could potentially also be used in gate-based quantum computing although it's not really demonstrated at a large scale. Pasqal (France), QuEra (USA), Atoms Computing (USA) and Planqc (Germany) are the key industry vendors 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 2022. Quandela (France), Xanadu (Canada) and QuiX (The Netherlands) are other key players in that space. One key capability to implement MBQC is the generation of deterministic high volume cluster states of entangled photons. It is still in its infancy.

Quantum enabling technologies

- 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 and are used with photon sources and detectors for photon qubits systems as well as with trapped ions and cold atoms setups.
- Cabling and filters play another key role, particularly with solid-state qubits. Superconducting cables are expensive with 3K€ per meter and come from a single vendor source from Japan. Signals multiplexing may be on the way.
- Microwave generation and readout systems used with superconducting and quantum dots electron spin qubits are other key enabling technologies. The challenge is to miniaturize it and lower their power consumption and, if that makes sense, to put them as close as possible to the qubits, operate them at cryogenic temperatures and simplify system cabling. It is a key to physical qubits scalability, particularly to implement quantum error correction. A lot of different technologies compete here, mostly around cryo-CMOS and superconducting electronics. Other components deserve attention like circulators and parametric amplifiers that we cover in detail in this new edition. At last, error correction requires extensive classical processing that is frequently forgotten in the resource estimations of fault-tolerant quantum computing.
- Many lasers and photonics equipment are used with cold atoms, trapped ions, and photon qubits and also quantum telecommunications, cryptography and sensing. It includes single indistinguishable photon sources as well as single photon detectors. The lasers field is also very diverse with products covering different ranges of wavelengths, power, continuous vs pulsed lasers, etc.
- Manufacturing electronic components for quantum technologies is a strategic topic covered extensively in this book with a description of generic fab techniques and some that are specific to quantum technologies like with the fabrication of superconducting qubits and quantum dots.
- Quantum technologies use a lot of various raw materials, some being rare but used in very small quantities. While 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. The next challenge will be to analyze full product lifecycle costs and reduce the overall environmental footprint of emerging quantum technology, particularly for those who may be used in volume.

Figure 7: a market map of key enabling technology vendors. (cc) Olivier Ezratty, 2022-2023.

Unconventional computing

- Various non-conventional computing technologies may compete with classical and quantum computing or even bring some help, like reversible and superconducting technologies that may be useful to create cryogenic electronics enabling the creation of scalable quantum computers. These technologies are so diverse and with different underlying science that they would deserve a lot of time and energy to be properly evaluated and benchmarked by both physicists and computer science specialists.
- Digital annealing computing is mostly proposed by Japanese companies like Fujitsu and Hitachi, using classical CMOS chipsets. These solutions are supposed to solve intractable problems faster than classical-classical computers, but their scalability remains questionable.
- Reversible and adiabatic computation has been researched for a long time and has not yet turned into commercial products. It could probably be more interesting to create energy saving solutions more than faster solutions with some potential use case in quantum computing enabling technologies.
- Superconducting computing is an interesting area of research to create more energy efficient supercomputers, despite the cooling cost that, hopefully is not as expensive as with superconducting qubits quantum computers. There are synergies between this research area and superconducting logic electronics that could be used to control superconducting and quantum dots spin qubits at low temperatures.
- Probabilistic and optical computing are interesting research areas. These solutions may be competitive to solve specific problems.
- Optical processors are mainly used in the deep learning space, to accelerate the training and inferences in some layers of convolutional networks. Some variants can solve combinatorial problems.
- Chemical computing is one of the many other areas in unconventional computing that may be interesting but have probably various scaling limitations.

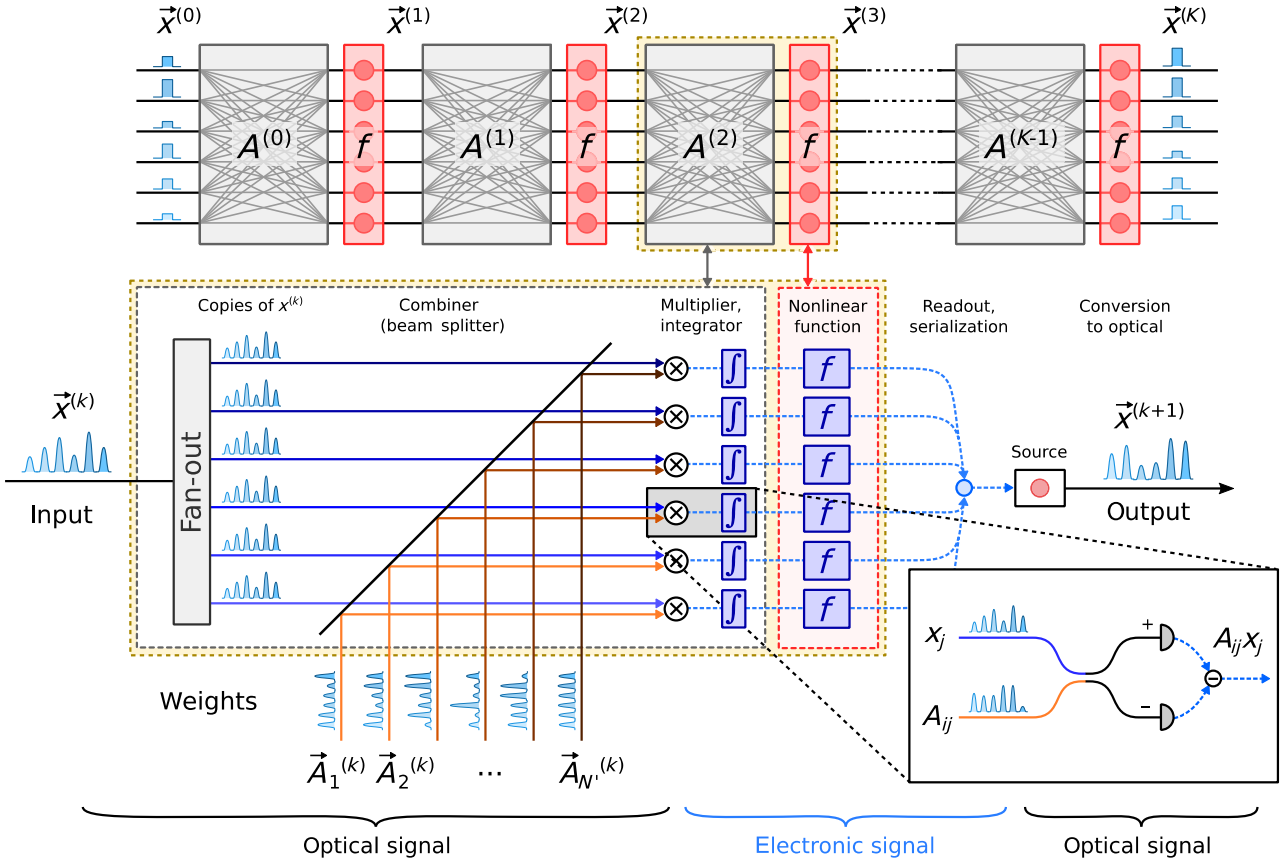


Figure 8: Source: [Large-Scale Optical Neural Networks Based on Photoelectric Multiplication](#) by Ryan Hamerly, Dirk Englund et al, MIT, PRX, 2018 (12 pages). Added in 2023.

Quantum telecommunications and cryptography

- Quantum computing poses a theoretical threat to many existing cryptography systems, particularly those using public key distribution in asymmetric cryptography. This is due to Peter Shor's integer factoring algorithm that could efficiently break RSA public encryption keys in the far distant future. But other algorithms than Shor are creating various threats, including for symmetric key distributions. However, these threats are usually exaggerated, particularly by security solutions vendors.
- As a result, two breeds of solutions have been elaborated that use either mathematical or physical protection. The first one is based on quantum key distribution, requiring a photonic transmission channel (terrestrial, free-to-air, satellite or fiber-based), and using either prepare-and-measure key transmission or quantum entanglement resources for the next generation adapted to the quantum Internet connecting quantum computers and sensors together. Beware of a common misconception: these solutions are not based on quantum computers. Quantum computers are not (yet) making cryptography safer although some solutions are proposed to secure data transmission, but, interestingly, without any encryption in the classical meaning.
- The second option is to create classical cryptographic protocols generating public encryption keys that are not breakable by quantum computers. The USA NIST launched in 2016 an international competition to standardize a set of post-quantum cryptography (PQC) protocols. Four finalists were selected as NIST standard in July 2022, one for a public key interface (PKI) and three for signatures and they are now draft standards. Solutions deployments should happen next and be done way before the quantum computing menace will materialize, if it does some day. NIST may select other PQC solutions in the future. PQC solutions are popping up in various fields like to secure blockchains and Internet of things (IoT).
- Quantum random numbers generation is/will be used for classical cryptography, and quantum cryptography. It provides sources of both random and non-deterministic numbers used in cryptography systems. It has other used cases when randomness is mandatory in classical computing like with lotteries and various 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. Distributed quantum sensing can enable better accuracy sensing.
- 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 with both landline fiber and satellite links. Europe is also experimenting quantum communication networks.

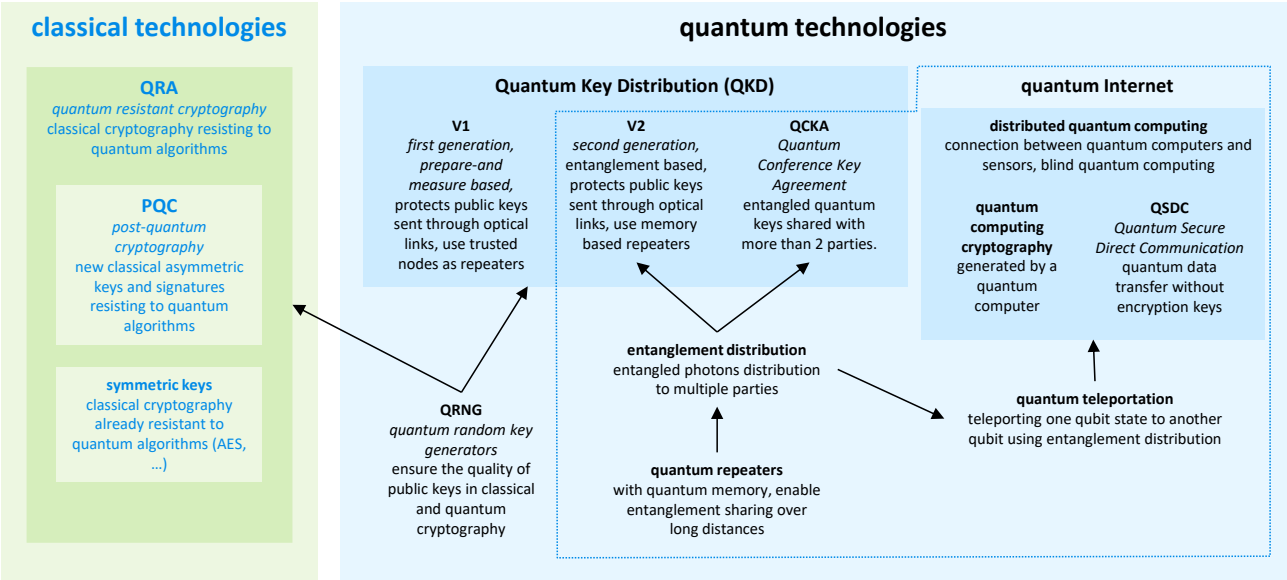


Figure 9: the four classes of technologies covered in this part. (cc) Olivier Ezratty, 2023.

Quantum sensing

- Quantum sensing is the most mature and underlooked market of quantum technologies, one potential reason being its fragmentation and currently limited broad scale use cases.
- Quantum sensing enables better precision measurement of nearly any physical parameter: time, distance, temperature, movement, acceleration, pressure and gravity, magnetism, light frequency, radio spectrum and matter chemical composition.
- Quantum sensing has been extensively used to update the new international metric system put in place in 2019.
- Lasers and the frequency combs technique are 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 helps measure variations of magnetism and has applications in many domains like in medical imaging and non-destructive control. Indirectly, measuring magnetism can help measure many other physical parameters like temperature and pressure.
- Another one is cold atoms based interferometry that is implemented in micro-gravimeters, accelerometers and inertial sensors. Cold atoms 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 real performance of these devices is questionable and is driving a lot of skepticism in the Western world. But the related research is still going on and quantum LiDARs seem to make progress.

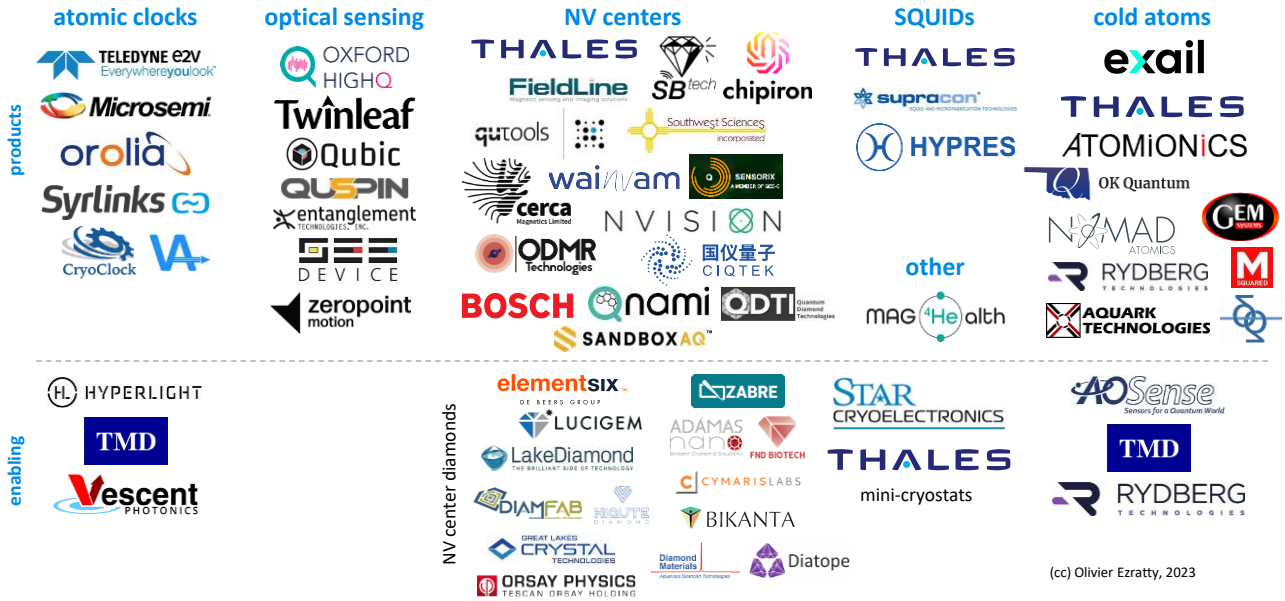


Figure 10: a market map for quantum sensing, including some of their enabling technologies. (cc) Olivier Ezratty, 2023.

Quantum algorithms

- 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 those used in classical programming, even including artificial intelligence development tools or object oriented programming. They are 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 theorical 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, quantum annealers and quantum simulators algorithms are all hybrid, combining a classical (preparation) part and a quantum part. A special breed of quantum algorithms are the variational quantum algorithms (VQA) and their variants for optimizations (QAOA), chemical simulations (VQE) and machine learning (QML) that targets the NISQ systems (noisy intermediate quantum computers). These combine the classical preparation and adjustment of a Hamiltonian that computes a cost function with several classical optimization steps and quantum computing circuit executions. All algorithms requiring a Quantum Fourier Transform (QFT) require a fault-tolerant quantum computer with quantum error correction. They are thus for the long term (red in Figure 11).
- Quantum inspired algorithms are running on classical computers and are using some form of quantum mathematical models and are based on tensor networks classical computing methods (MPS, DRMG). They can drive performance improvements in classical computing.

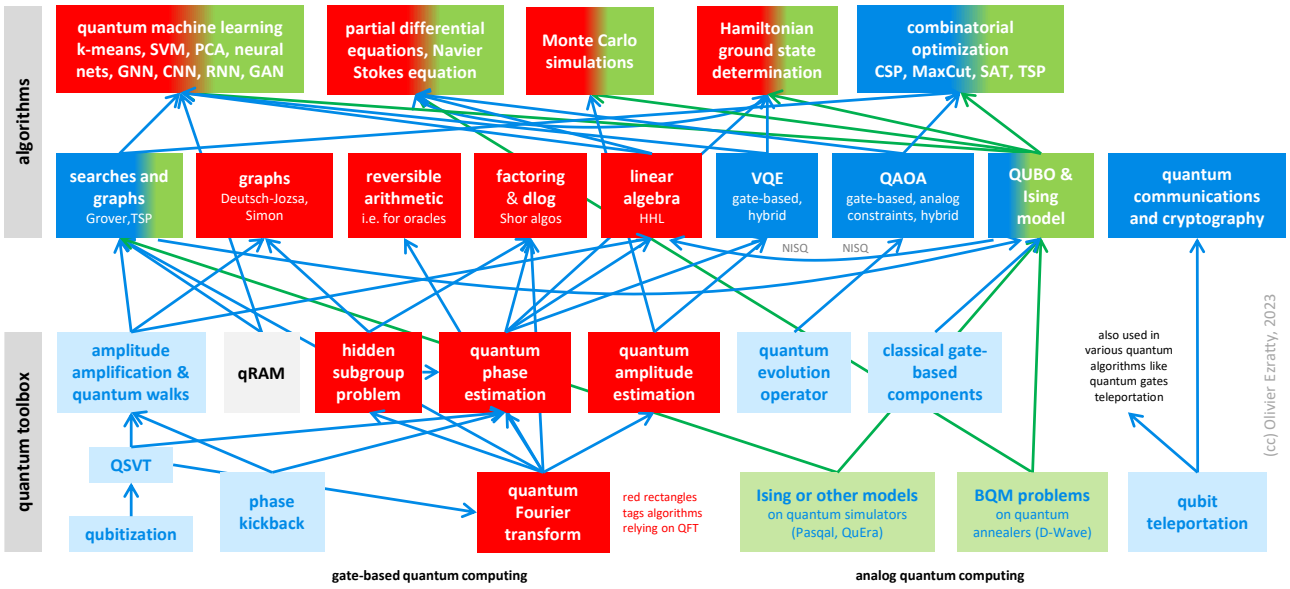


Figure 11: a quantum algorithms map and their interdependencies. The color code is the following: red corresponds to FTQC algorithms relying on the QFT (quantum Fourier transform). Blue algorithms correspond to other gate-based algorithms that may work in NISQ QPUs. Green algorithms relate to analog quantum computing paradigms like quantum annealing (ala D-Wave) and quantum simulations (ala Pasqal). Many high-level algorithms have an FTQC QFT based version and some analog equivalent, usually based on a QUBO or Ising model. (cc) Olivier Ezratty, 2023, inspired by a schema found on Quantum Computing Algorithms by Andreas Baertschi, 2019 (45 slides).

Quantum software development tools

- Gate-based programming involves either graphical circuit design (mostly for training purposes) and (usually) Python based programming when qubit gates structures must be designed in an automated way.
- Python based programming relies 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.
- Currently, NISQ quantum computing is based on running algorithms multiple (thousands if not more...) times and averaging the results. A single individual run yields a probabilistic outcome while many run averages will converge into deterministic ones. It is even more complicated with VQE (variational quantum eigensolvers) which require millions of circuit shots to reconstitute a many-body system Hamiltonian to measure its ground state energy level.
- Most quantum computers are used in the cloud, through offerings coming from the computer vendors themselves like IBM or D-Wave or from cloud service providers like Amazon, Microsoft, Google and OVHcloud.
- Quantum emulators are very useful to learn programming, test it until it reaches the limits of classical emulation (about 40-50 qubits) and also help debug small-scale quantum algorithms. When these emulators include physical simulators of the underlying qubit physics like with Bosonic Qiskit and Quandela Perceval, they help create algorithms that are error-resilient and also design new quantum error correction codes. 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 2023, did show a real computing advantage compared to classical computing. The reasons were multiple, the main ones being that these experiments usually do not implement any algorithm using some input data. But starting in 2022, we see appearing some relevant quantum advantage with actual data and useful algorithms running on NISQ hardware, including with the boson sampling method used with photon qubits.

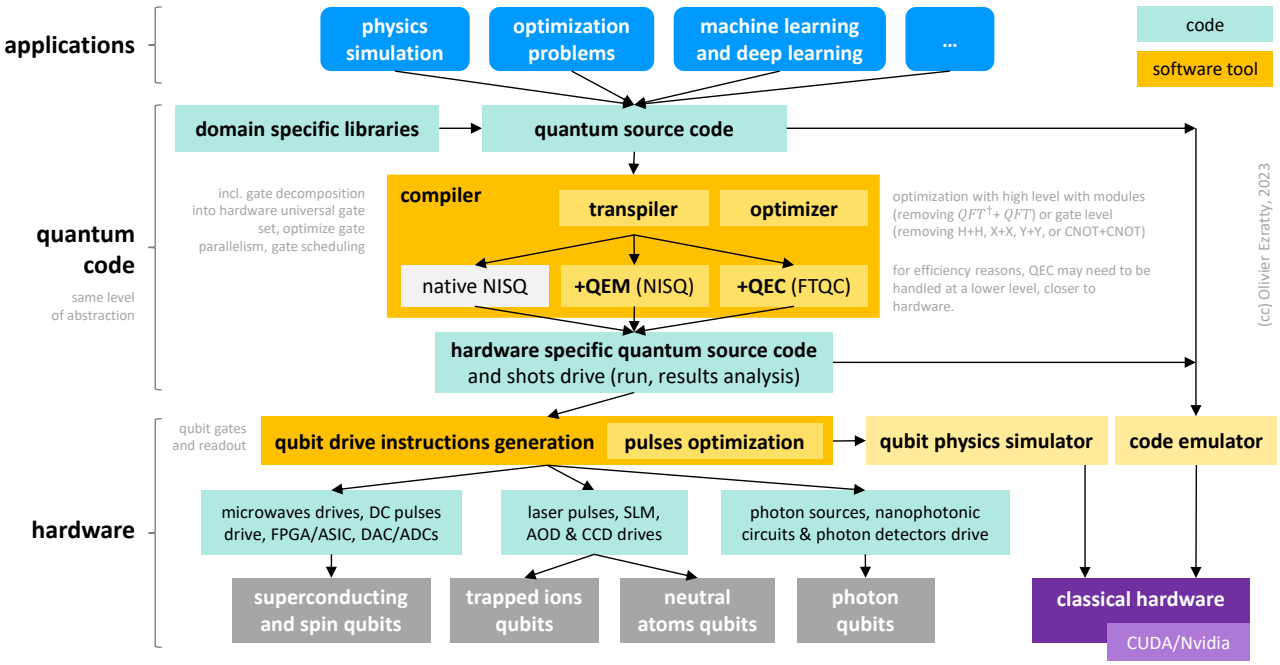


Figure 12: classification of quantum software engineering tools. (cc) Olivier Ezratty, 2023.

Quantum computing business applications

- Most quantum computing market forecasts are highly optimistic and plan for an early advent of scalable quantum computers. They also sometimes tweak forecasts by 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.
- This book contains a framework proposal to assess the interest and relevance of published use cases. It helps separate the marketing from the real practicality of these use cases given that, as of 2023, no quantum application is running live in production in any corporation.
- 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 and developers since 2016. IonQ and Quantinuum are also publicizing case studies, but they are usually was below a quantum advantage level, using only fewer than 25 qubits.
- 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! We also cover in this book the burgeoning IT and consulting services in quantum technologies.

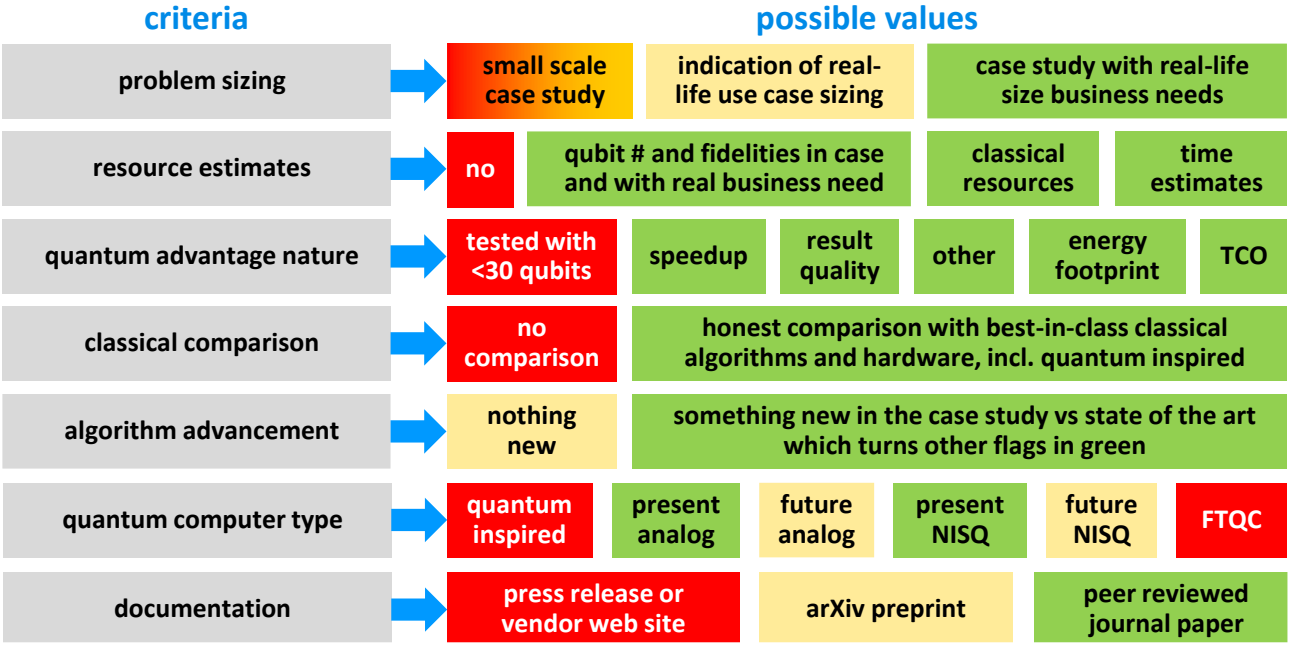


Figure 13: how to evaluate a quantum computing case study. Red flags indicate key missing points in the case study making it irrelevant to show any advantage for quantum computing for the given business problem. Orange flags are intermediate situations but not real showstoppers. Green flags are indications of a serious use case. Quantum inspired use cases are not using quantum computing and therefore should not be presented as such. TCO means total cost of ownership, an economic concept coming from the classical information technology world. (cc) Olivier Ezratty, 2023.

Quantum technologies around the world

- 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 "national quantum plans" and want to lead that space, particularly with quantum computing. 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 plus incremental, private sector included or not, European Union investments included or not). All these plans invest a lot in fundamental research and on developing a startup and industry ecosystem, including workforce training.
- 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 seems to persist with the Biden administration.
- Europe and the USA are the greatest investors in quantum science so far. The European Union as a whole is the largest region for public investments in quantum research. The USA has a larger industry investment than Europe due to its large IT vendors investments (IBM, Google, Microsoft, Intel) and a traditional lead 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.

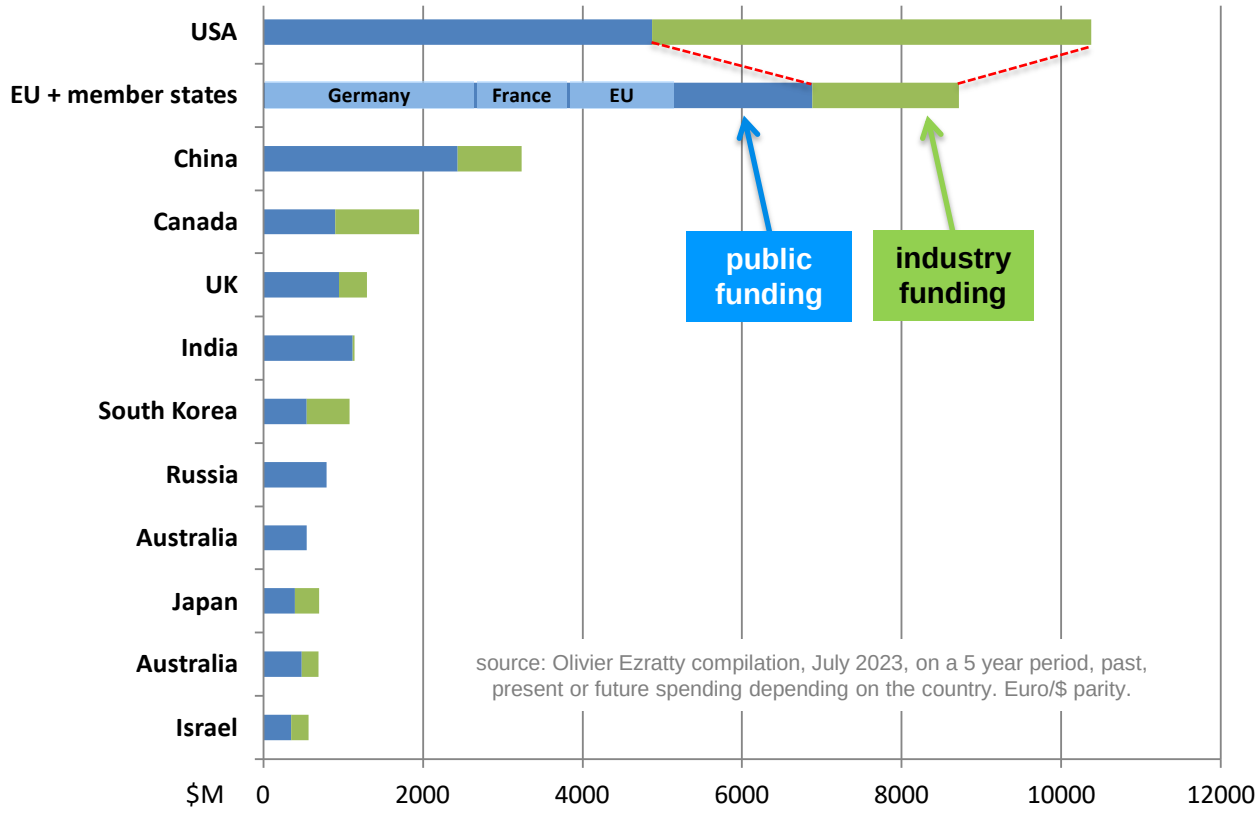


Figure 14: a consolidation of quantum technologies public and private investments with some raw estimated for large IT vendors. It creates a very different picture than what is commonly thought about the place of China and Europe. (cc) Olivier Ezratty, July 2023.

Quantum technologies and society

- 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 can persist.
- Science fiction has built an imaginary of what quantum technologies could achieve, with teleportation, supraluminal traveling speeds, various entanglement 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.

Figure 15: some women role models around the world, from research to the industry. (cc) Olivier Ezratty, 2021-2023.

Quantum fake sciences

- 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.

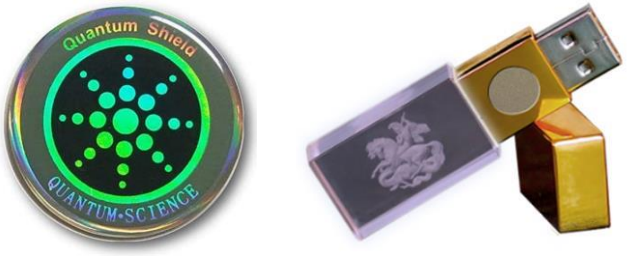
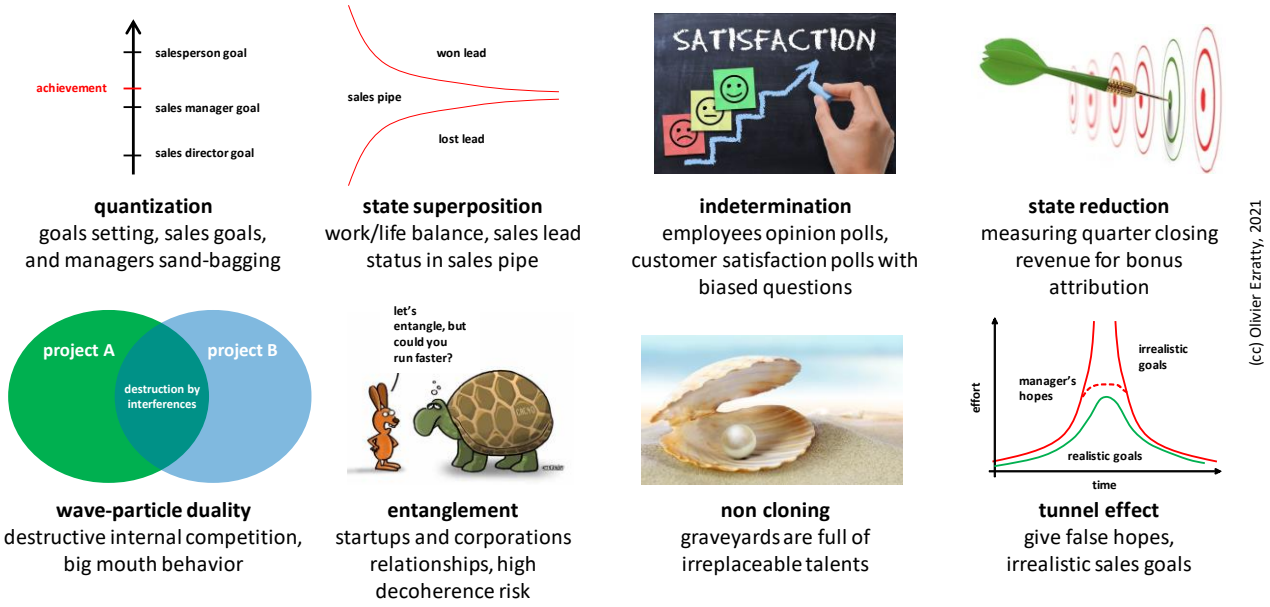


Figure 16: quantum medallions and 5G quantum keys are fancy gadgets for the gullible. That's a huge market!

- Quantum physics is sometimes used in management and marketing. This book offers you a nice in-depth parody of these methodologies.



quantization
goals setting, sales goals, and managers sand-bagging

state superposition
work/life balance, sales lead status in sales pipe

indetermination
employees opinion polls, customer satisfaction polls with biased questions

state reduction
measuring quarter closing revenue for bonus attribution

wave-particle duality
destructive internal competition, big mouth behavior

entanglement
startups and corporations relationships, high decoherence risk

non cloning
graveyards are full of irreplaceable talents

tunnel effect
give false hopes, irrealistic sales goals

Figure 17: my useless framework for quantum management. (cc) Olivier Ezratty, 2022.

- At last, we showcase a few companies using quantum in their branding when they have nothing quantum at all to offer.

back-cover flip page.

⟨ Aage Niels Bohr | Abner Shimony | Adi Shamir | Akira Furusawa | Alain Aspect | Alain Ravex | Alain Sarlette | Alan Aspuru-Guzik | Alastair Abbott | Albert Einstein | Alberto Bramati | Alexander Andreev | Alexander Holevo | Alexander Prokhorov | Alexandre Blais | Alexandre Zagoskin | Alexei Bylinskii | Alexei Grinbaum | Alexei Kitaev | Alexia Auffèves | Alfred Kastler | Alfred Pérot | Alonzo Church | Amir Naveh | André Luiz Barbosa | Andrea Morello | Andrea Rodriguez Blanco | Andreas Wallraff | Andrew Childs | Andrew C | Andrey | Andrey Steane | Andrew G. White | Andy Matuschak | Anne Br | Anton Zeilinger | Aram Harrow | Arieh Warshel | Arthur Holly Compton | Arthur Leonard Schawlow | Artur Ekert | Astrid Lambrecht | Audrey Bienfait | Axel Becke | Benjamin Huard | Benoît Valiron | Bettina Heim | Bob Wiens | Boris Podolsky | Brian Josephson | Bruce Kane | Bruno Desruelle | Bryce DeWitt | Carl Wieman | Carlo Rovelli | Chad Rigetti | Charles Bennett | Charles Fabry | Charles Hard Townes | Charles Hermite | Chien Shiung Wu | Christiaan Huygens | Christian Weedbrook | Christine Silberhorn | Christophe Jurczak | Christophe Solomon | Christophe Vuillot | Christopher Monroe | Christopher Papile | Claude Cohen Tannoudji | Claude Weisbuch | Clauss Jönsson | Clinton Davisson | Cornelis Dorsman | Craig Gidney | Cristian Calude | Cristina Escoda | Cyril Allouche | Damien Stehlé | Daniel Esteve | Daniel Gottesman | Dave Wecker | David Bohm | David Deutsch | David DiVincenzo | David Gosset | David Hilbert | David J. Thouless | David Wineland | Dennis Dieks | Dieter Zeh | Dirk Bouwmeester | Don Coppersmith | Don Misener | Donna Strickland | Dorit Aharonov | Douglas James Scalapino | Earle Hesse Kennard | Ed Sperling | Edward Farhi | Edward Fredkin | Edward Tang | Elena Calude | Eleni Diamanti | Elham Kashefi | Elisabeth Giacobino | Elvira Shishenina | Emanuel Knill | Emmy Noether | Enrico Fermi | Eric Cornell | Ernest Rutherford | Ernst Ising | Erwin Schrödinger | Etienne Klein | Ettore Majorana | Ewin Tang | Fabio Sciarrino | Faye Wattleton | Felix Bloch | Francesca Ferlaino | Franck Balestro | Frank Wilczek | François Le Gall | Frédéric Grosshans | Frédéric Magniez | Freeman John Dyson | Friedrich Hund | Friedrich Paschen | Geordie Rose | George Uhlenbeck | Georges Paget Thomson | Georges Zweig | Georges-Olivier Reymond | Gerard Milburn | Gerrit Jan Flim | Gil Kalai | Gilles Brassard | Gilles Holst | Giorgio Frossati | Gordon Baym | Gordon Gould | Guang-Can Guo | Haig Farris | Hans Albrecht Bethe | Hans Jürgen Briegel | Hantaro Nagaoka | Harald Fritzsch | Hartmut Neven | Heike Kamerlingh Onnes | Heinrich Hertz | Hélène Bouchiat | Hélène Perrin | Hendrik Anthony Kramers | Hendrik Casimir | Hendrik Lorentz | Henri Poincaré | Hermann Minkowski | Hermann Weyl | Hugh Everett | Hui Khoon Ng | Ilana Wisby | Ilya Mikhailovich Lifshitz | Immanuel Bloch | Iñigo Artundo | Iordanis Kerenidis | Irfan Siddiqi | Isaac Chuang | Isaac Newton | Itamar Sivan | Jacqueline Bloch | Jacques Salomon Hadamard | Jacquiline Romero | James Chadwick | James Clarke | James Clerk Maxwell | James Park | Jared Cole | Jason Alicea | Jay Gambetta | Jean Dalibard | Jean Michel Raimond | Jean-François Roch | Jean-Michel Gérard | Jean-Philip Piquemal | Jian-Wei Pan | Jelena Vučković | Jelena Vucokic | Jeremy O'Brien | Joannes van der Waals | Joe O'Gorman | Johann Balmer | Johannes Pollanen | Johannes Rydberg | John Bardeen | John Clauser | John Frank Allen | John Hall | John Levy | John Martinis | John Morton | John Robert Schrieffer | John Rowell | John Smolin | John Stewart Bell | John Von Neumann | John Watrous | Jonathan Dowling | Jonathan Koomey | Jonathan P. Home | José Capmany | José David Domenech | Jose Latorre | John Hopfield | Joseph John Thomson | Josh Nunn | Juan Ignacio Cirac | Julia Kempe | Julian Schwinger | Julien Bobroff | Jürgen Mlynek | Kenneth Appel | Kenneth Regan | Kevin Young | Kirill Tolpygo | Kohei Itoh | Kristel Michielsen | Krysta Svore | Kun Huang | Kurt Gödel | Le Si Dang | Lee Smolin | Léon Brillouin | Leon Neil Cooper | Leonard Adleman | Lester Germer | Leslie Ishop | Lev Landau | Lieven Vandersypen | Linus Pauling | Llewellyn Thomas | Loïc Henriet | Louis Couchy | Louis de Broglie | Lov Grover | Lu Jeu | Lucien Hardy | Ludwig Boltzmann | Luigi Frunzio | Magdalena Hauser | Marcus Doherty | Marcus Huber | Maria Schuld | Marie-Anne Bouchiat | Marina Huerta | Martin Karplus | Masahide Sasaki | Masahiro Kitagawa | Masahito Hayashi | Mathieu | Matthew Hutchings | Matthias Troyer | Matthieu Desjardins | Maud | Max Born | Maxime Richard | Mazyar Mirrahimi | Menno Verdhorst | Michael Ben-Or | Michael Frank | Michael Freedman | Michael L | Michael Nielsen | Michel Brune | Michel Devoret | Michelle Simmons | Mikhail Dyakonov | Mio Murao | Murray Gell-Mann | Nathan Gemelke | Nathan Rosen | Nathanaël Cottet | Nicolas Gisin | Nicolas Roch | Niels Henrik Abel | Nikolay Basov | Nir Minerbi | Oleg | Oskar Painter | Pascale Senellart | Pascual Jordan | Pascual Muñoz | Patrick | Patty Lee | Paul Hiriart | Perola Milman | Pete Shadbolt | Peter Higgs | Peter Knight | Peter Shor | Peter Zoller | Philip W. Anderson | Philipp Lenard | Philippe Duluc | Philippe Grangier | Pierre Hohenberg | Pranav Gokhale | Pyotr Kapitsa | Qingfeng Wang | Rainer Blatt | Raphaël Lescanne | Raymond Laflamme | René Descartes | Richard Feynman | Richard Holt | Richard Karp | Richard Murray | Rob Schoelkopf | Rob Whitney | Robert Andrews Millikan | Robert Dennard | Robert König | Robert McDermott | Roy J. Glauber | Robert Rauss | Robert William Boyd | Robin Blume-Kohout | Roger Penrose | Roland Gähler | Roman Lutsiv | Ron Rivest | Roy Glauber | Ronald Walsworth | Rudolf Grimm | Ryan Babbush | Samuel Goudsmit | Sandu Popescu | Sara Ducci | Sarah Sheldon | Satyendranath Bose | Scott Aaronson | Sébastien Balibar | Serge Haroche | Sergey Bravyi | Seth Lloyd | Shengtao Wang | Shi Yaoyun | Shin'ichirō Tomonaga | Silvano de Franceschi | Simon Benjamin | Simon Perdrix | Simone Severini | Sophia Economou | Stefanie Barz | Stephanie Wehner | Steve Girvin | Steve Lamoreaux | Taki Kontos | Tauqir Abdullah | Terry Rudolph | Théau Peronnin | Theodor Hänsch | Theodore Lyman | Theodore Maiman | Thibault Jacqmin | Thierry Lahaye | Thomas Monz | Thomas Young | Tommaso Calarco | Tommaso Toffoli | Tracy Northup | Travis Humble | Tristan Meunier | Umesh Virkumar Vazirani | Urmila Mahadev | Valerian Giesz | Vasilis Armaos | Vincent Bouchiat | Virginia D'Auria | Vlad Anisimov | Vladan Vuletic | Vladimir Fock | Walter Brattain | Walter Kohn | Walter Houser Brattain | Walther Meissner | Walther Nernst | Wassim Estephan | Werner Heisenberg | Wilhelm Wien | William Rowan Hamilton | William Shockley | William Wootters | Willis Eugene Lamb | Winfried Hensinger | Wojciech Zurek | Wolfgang Haken | Wolfgang Lechner | Wolfgang Paul | Wolfgang Pauli | Wolfgang Ketterle | Xavier Waintal | Yakov Frenkel | Yasuhiko Arakawa | Yasunobu Nakamura | Yehuda Naveh | Yoshihisa Yamamoto | Yuichiro Minato | Yuri Alexeev | Yuri Manin | Zaki Leghtas ⟩

le lab quantique