Politische Analyse
1/2020

White Paper: Quantentechnologie in der Schweiz

Considerations and recommendations by the Swiss Science Council SSC

Report by Cathal J. Mahon and the SSC secretariat

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizerischer Wissenschaftsrat
Conseil suisse de la science
Consiglio svizzero della scienza
Swiss Science Council

The Swiss Science Council

The Swiss Science Council SSC is the advisory body to the Federal Council for issues related to science, higher education, research and innovation policy. The goal of the SSC, in conformity with its role as an independent consultative body, is to promote the framework for the successful development of the Swiss higher education, research and innovation system. As an independent advisory body to the Federal Council, the SSC pursues the Swiss higher education, research and innovation landscape from a long-term perspective.

⟵

Code scannen und
die digitale Version
herunterladen.

www.wissenschaftsrat.ch

About this White Paper

The Swiss Science Council (SSC) publishes this White Paper with the declared goal to make sure that Switzerland is able to exploit its full potential and strategic advantages in the domain of quantum technology. The first part of the White Paper contains considerations and recommendations by the SSC that are based on a workshop with leading Swiss quantum scientists organised by the SSC secretariat in January 2019,[3] an external expert report, as well as eleven interviews with various stakeholders conducted by the SSC secretariat. The second part of the White Paper consists of an expert report. Section 1 of the report provides an introduction to quantum technology, Section 2 gives an overview on important international developments, and Section 3 describes the Swiss situation. The insights gained in the interviews by the SSC secretariat are included in Section 3 of the expert report. The SSC thanks all workshop participants and interview partners for their contributions. The following considerations and recommendations do not necessarily reflect the opinion of the experts or interview partners.

[1] The participants of this workshop were: Tilman Esslinger (ETH Zurich), Nicolas Gisin (University of Geneva, ID Quantique), Sadik Hafizovic (Zurich Instruments), Daniel Loss (University of Basel), Adrian Perrig (ETH Zurich), Ulrich W. Suter (ETH Zurich, SATW), Matthias Troyer (ETH Zurich, Microsoft), Andreas Wallraff (ETH Zurich), Richard Warburton (University of Basel), Gabriel Aeppli (member of SSC working group), Gerd Folkers (president SSC), Jean-Marc Triscone (member of SSC working group), Tizian Fritz (secretariat SSC), Eva Herrmann (secretariat SSC).

What is quantum technology?

The term *quantum technology* refers to an array of novel technologies based on physical properties at the smallest possible scale. The most popularised application of quantum technology is quantum computing, which promises a novel and much faster approach to information processing. Quantum computers could enable new breakthroughs in science, foster the development of new materials and chemicals, including pharmaceuticals, or enable solutions to complex decision problems (for example in logistics). Quantum computing is still at an early stage of development and more basic research is required before quantum computers become commercially available.

Quantum technology also opens up the road to ultra-secure communication networks, in which all data channels would be safe from eavesdropping. The prospect of quantum-safe data-transfer is appealing to companies and institutions that rely on data safety and safe communications. First commercial applications in the domain of quantum encryption are already available.

Finally, quantum technology also provides ways to novel, highly sensitive sensors for a variety of physical quantities such as magnetic and electric fields, time and frequency, force and displacement, or temperature. Quantum sensors will be applicable in areas ranging from medical diagnostics and imaging through autonomous transportation and manufacturing systems to scientific instrumentation.

Quantum technology in Switzerland

Switzerland is in an excellent position to grow and foster a flourishing quantum technology ecosystem. One of the main challenges at the current moment concerns early-stage knowledge and technology transfer from basic research conducted at Swiss universities to industry. There are two main reasons for this. First, some of the potential applications of quantum technology are still at an early stage of development. This makes it often difficult for start-up companies to attract private investors that would provide the financial resources needed for research and development of novel applications. Second, knowledge about quantum technology among providers of venture capital in Switzerland seems to be scarce. Increased coordination and communication between academia, start-ups, potential capital donors as well as incumbent companies in industry sectors that are potentially affected by future developments in quantum technology are thus some of the most urgent needs at this point in time.

Part I – Considerations and recommendations by the SSC

Considerations

1) **Research**: Switzerland has outstanding research groups in quantum science with a world-leading research output. The ongoing NCCR QSIT and previous NCCRs have been crucial for the establishment of Swiss research institutions at the international forefront of quantum science. The high level of expertise in many subfields of quantum science (computing and simulation, algorithms, communication and sensing) at Swiss research organisations is a major asset that should be secured for the future. The exploitation of the full potential of quantum technology, and quantum computing in particular, will require further efforts in basic research. The SSC therefore welcomes the establishment of the new NCCR SPIN, which will help to secure for Switzerland a leading position in one important aspect of quantum science. Furthermore, the strong involvement of Swiss research groups in European programmes is important to maintain the high level of competitiveness of Swiss quantum science.

2) **Education:** Aside from excellent basic research, a growing quantum technology ecosystem requires an adequately trained workforce fit to tackle the engineering and computing challenges that accompany the development of quantum technology. The newly created master programme in quantum engineering at ETH Zurich constitutes a move in the right direction. But quantum technology requires a level of multi-disciplinarity that goes beyond physics, engineering and computer science alone. Technology transfer becomes more efficient if well-trained scientists and engineers also have a basic understanding of fundamental principles of management and entrepreneurship. Industrial PhDs or postdoc programmes can support the transfer of knowledge and technology. In the near future, the universities of applied sciences (UASs) could begin to play a role in the education and training of specialists required for quantum technology in industry.

3) **Technology transfer and industrial technology development:** Switzerland hosts a number of highly successful and promising start-up companies in the domain of quantum technology, some of which are already international leaders in their domain. However, there is a clear lack of early-stage funding for quantum start-ups. To support and expand existing assets and to further exploit strategic advantages, it is essential to take suitable measures to ensure a successful and swift transfer of knowledge and technology from academia to industry. Ideally, this will include the establishment of a network of private investors interested in advancing quantum technology in Switzerland. Swiss private-public research and development institutions like the Swiss Center for Electronics and Microtechnology (CSEM) play a crucial role in this regard. Networking and information platforms like the recently established Swiss Quantum Hub and events like the annual Quantum Industry Day in Zurich help to foster an exchange between academia, industry and investors and to accelerate the development of new quantum products. Procurement programmes by federal departments provide another way to strengthen bleeding-edge quantum technology development. Ultimately, the goal should be to create a flourishing quantum technology ecosystem in Switzerland that not only benefits national stakeholders but is also attractive for international partners and investors.

4) **Specialisation:** It is unlikely that the first commercial quantum computer will be built in Switzerland. Although Swiss universities should continue their world-class basic research on quantum computing, near-term efforts in technology development at the level of entire systems should focus on quantum communication and quantum sensing. In addition, Switzerland’s longstanding tradition in precision manufacturing, metrology and micro-technology in combination with its strong industrial base in other sectors, puts the country in a strong position for the development of key enabling technologies and subsystems of quantum technology, including quantum computing.

5) **Security:** Future developments in quantum computing and quantum cryptography are likely to have a direct impact on data security and *ipso facto* on infrastructures that are critically dependent on secure data communication channels. Such infrastructures include telecommunication networks, energy infrastructures and other private and public services like e-voting systems or financial services. There appears to be a lack of awareness among potentially affected industry sectors about the security implications of quantum technology. As of now, Swiss authorities have not taken any significant steps towards the assessment of risks that could emerge from future developments in quantum technology.[10]

6) **Societal impact:** Quantum technologies are likely to have impacts in various domains of society. The high disruptive potential of quantum technology necessitates a comprehensive assessment of the benefits and risks of quantum technology to prepare for a responsible implementation of quantum technology in society. This includes anticipating economic impacts on established industries, changes in various fields of research, as well as impacts on fields that might be affected by novel quantum sensing applications (e.g. medical diagnostics). Due to the strong implications for data security and privacy, future developments in quantum technology are likely to pose new legal and ethical challenges. It is critical that future decision-makers are scientifically well-informed. Economists, legal experts, sociologists, ethicists and experts from similar fields will have an important role to play when it comes to the responsible implementation of quantum applications in society.

Recommendations

Enabling and improving the development of novel technologies requires actions along the entire value chain from basic research through applied research to market-oriented innovation. Quantum technology is no different in this regard. However, each branch of technology has its specificities that determine how each stage of the value chain can be optimised. At the current moment, for quantum technologies these specificities are: 1) A broad range of potential applications; 2) different technology readiness levels (TRLs) for different aspects of quantum technology (low for computing and higher for sensing and communication); 3) potential implications for military and civilian security systems; 4) specifically in Switzerland, a lack of awareness of quantum technology among private investors and potentially affected industry sectors.

Fostering a successful quantum technology ecosystem in Switzerland thus requires continued support for basic research and education of new talents, in parallel with technology transfer promoted by increased communication and coordination among academia, start-ups, venture capital and potentially affected industry sectors. The government can support these efforts by addressing the security implications of quantum technology in various domains (such as data and communication systems, critical infrastructures or military applications). This might require additional funding opportunities (beyond the existing ones like SNSF, Innosuisse, ETH domain or European schemes). Based on these insights the SSC makes the following recommendations:

Government agencies

- To the Federal Council and the State Secretariat for Education, Research and Innovation: Take all necessary measures to ensure continued access for Swiss researchers to programmes within the FET Flagship Quantum Technologies and future European programmes under the umbrella of Horizon Europe.
- To the Federal Council: Instruct the Federal Office for Civil Protection to include a quantum risk assessment in the upcoming revision of the National Strategy for the Protection of Critical Infrastructures.

[4] A report of the Federal Council ("Rechtliche Grundlagen für *Distributed Ledger*-Technologie und Blockchain in der Schweiz", December 2018) highlights the fact that future developments in quantum computing could necessitate adjustments in current encryption technologies. See https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf.

- To the Federal Council: Instruct the Federal IT Steering Unit to include a quantum risk assessment in the upcoming revision of the National Strategy for the Protection of Switzerland against Cyber Risks.
- To the Federal Office of Energy: Assess the relevance of quantum encryption for the secure transmission of data within the energy infrastructure. Raise awareness among public and private service providers for potential vulnerabilities and for the potential benefits of establishing "quantum readiness". Monitor the energy use of the IT sector, noting both the potentially high initial energy consumption of quantum systems, as well as the long-term energy saving potential of quantum processors given by their intrinsic thermodynamics.
- To the Federal Office of Communication: Implement a quantum risk assessment in the strategy "Digital Switzerland". Assess the relevance of quantum encryption for 5G mobile communication. Raise awareness among private network and service providers for potential vulnerabilities and for the potential benefits of establishing "quantum readiness".
- To the Federal Office for Civil Protection and the Federal Commission on Telematics for Rescue and Security: Work with suitable partners to include an optical fibre-based quantum-secure test network in the pilot project "Secure Mobile Broadband Communications (MSK)".[11]
- To the Armed Forces Command Support Organisation and the Federal Office for Civil Protection: Assess the relevance of quantum encryption and metrology and implement a quantum risk assessment in the yet to be established "Secure Data Network (SDVN)".[12]
- To armasuisse: Assess the possibility of procurement activities in collaboration with domestic companies and quantum start-ups to secure domestic technology know-how.

To Swiss National Science Foundation and Innosuisse

- Continue to foster a diverse basic science ecosystem for supporting quantum technology. Maintain excellence in established areas, such as quantum simulation and encryption.
- Review and revise existing programmes (e.g. BRIDGE), with a strong focus on the needs of start-ups, SMEs and industrial partners in mind.

To universities and universities of applied sciences

- Increase the support for university spin-offs with respect to management capabilities and establishing connections to early-stage investors.
- Support industrial PhDs or postdoctoral schemes to strengthen the university-industry link.
- Assess the requirements and needs for engagement of the UASs in quantum research and education.
- Consider the establishment of an interdisciplinary graduate school and/or master programme for quantum science and engineering as a collaborative educational project including federal institutes, universities and if possible the UASs.
- Facilitate access for start-ups to laboratory infrastructures (such as cryogenic facilities).

To the academies and TA-Swiss

- Develop roadmaps for quantum technology applications that are ready for commercialisation.
- Raise awareness among incumbent industries for the potential impact of quantum technology on their businesses.
- Foster a dialogue about the economic, legal, ethical and societal implications of quantum technology.
- Conduct an assessment of quantum technology.

[5] The Goals of the Federal Council for 2020 include a decision to establish a system for Secure Mobile Broadband Communications (MSK) that would provide a stable, resistant and safe network for mobile communication for rescue and security authorities and organisations (BORS). See Bundeskanzlei, "Ziele des Bundesrates 2020: Band I", Bern 2019, pp. 38–39; https://www.bk.admin.ch/dam/bk/de/dokumente/strategische-fuehrungsunterstuetzung/ziele-bundesrat/bandI/ziele_des_bundesrates_2020.pdf.download.pdf/JZ%202020%20-%20Band%20I%20-%20DE.pdf.

[6] On 21 November 2018 the Federal Council issued a dispatch concerning a Secure Data Network (SDVN) that was accepted by the parliament in September 2019. It is planned that investments of federal funds run until 2027. The Federal Office for Civil Protection and the Armed Forces Command Support Organisation are mainly responsible for the implementation. See: https://www.admin.ch/opc/de/federal-gazette/2019/241.pdf.

Part II – Report by Cathal J. Mahon & the SSC secretariat

About the author

Cathal J. Mahon is a quantum technology expert with extensive experience as an investment manager for venture capital funds specialising in high-tech start-ups – including quantum – and, prior to this, from a variety of managerial and R&D positions in the telecommunication industry. He served as interim CEO at Qubiz: Quantum Innovation Center in Copenhagen, Denmark, from 2016 to 2019 and is currently responsible for the commercialisation of quantum technology-based intellectual property created at the University of Copenhagen. Cathal J. Mahon has a scientific background in both engineering and physics holding a master degree in physics from Trinity College, Dublin, and a PhD in electronic engineering from the Technical University of Denmark. He has also been a guest lecturer at Copenhagen Business School and is the author of a textbook on the emergence of strategy in organisations.

1 Quantum technologies

Over the course of the 20th century, scientific insights into the behaviour of matter and energy at the smallest scale led to an array of technologies with far-reaching societal and economic impact. These technologies include the semi-conductor transistor, integrated circuits, and semi-conductor lasers which enabled applications like the personal computer, MRI scanners, GPS or LEDs, to name just a few. All these applications have now become an integral part of our everyday lives. In some instances, they are very visible; in other cases, they are at the core of the hidden infrastructure that makes our information society possible.

All of these technologies are based on the well-understood laws of a physical theory called quantum mechanics, and they all require, in some way or other, the manipulation of subatomic quantum particles (electrons in the case of the transistor and integrated circuits, or photons in the case of lasers).[13] It should be noted, however, that in all of the above-mentioned technologies, the particles are always manipulated in ensembles. Until recently, it was technically impossible to manipulate and control individual quantum systems. But developments in cryogenics, laser technology and material science have opened up the possibility to both control and measure the properties of individual quantum particles – i.e. the spin of individual electrons or the polarisation of individual photons – while simultaneously isolating them from the environment. This has paved the road to what is sometimes referred to as the "second quantum revolution".[14] The ability to manipulate and control individual quantum particles is the key to a second generation of quantum technologies which can be grouped into three main areas: quantum computing and quantum simulation, quantum communication, and quantum sensing.[15] As was the case with the first generation of technologies based on quantum mechanics, the new generation of quantum technologies also has a very high disruptive potential for many areas of society.

1.1 Quantum computing and quantum simulation

Quantum computing exploits the properties of so-called qubits (which stands for "quantum bits") to improve computing power far beyond the level of current computers. It is expected that the increased power of quantum computers will have paradigm-shattering impacts especially in domains where current computing power reaches its limits. This includes many areas of science such as physics, chemistry, biology, or material science. Some experts also expect quantum computers to be powerful tools for complex optimisation problems or machine learning methods (the hardware and software challenges are still significant though).[16] And much in the same way that it proved impossible to envisage all the current applications of the transistor and the laser when they were first invented, the same might be the case for quantum computing.

Quantum computing is, in many regards, the poster child for the paradigm-shattering potential of quantum technologies. The potential to perform calculations that are practically impossible with classical computing due to extensive computing times – including hacking public-key encryption in seconds (see Box 2, page 26) – has caught the public imagination at many levels. This potential is also what is driving the ever-increasing investments in quantum technology programmes by national states and tech giants alike.[17]

It is important to mention, however, that quantum computing is still at an early stage of development and that it will take many years of research and development before the potential of quantum computing can be realised. The greatest challenge at the moment is to build stable, error-free multi-qubit platforms. Simply put, the main problem consists in the fact that qubits rely on a physical phenomenon called "superposition" referring to a state in which a quantum system is in a combination of two states simultaneously (see Box 1 , page 22).

[13] For a comprehensive history of quantum mechanics and its main protagonists (including Max Planck, Albert Einstein, Erwin Schrödinger, Niels Bohr, Werner Heisenberg and others) see Baggott (2011).

[14] The term "second quantum revolution" was first introduced by MacFarlane, Dowling and Milburn (2003).

[15] For an intuitive explanation of the three areas see the *MIT Technological Review's* explainers on quantum technology: https://www.technologyreview.com/s/612844/what-is-quantum-computing.

[16] For quantum machine learning see Biamonte et al. (2017).

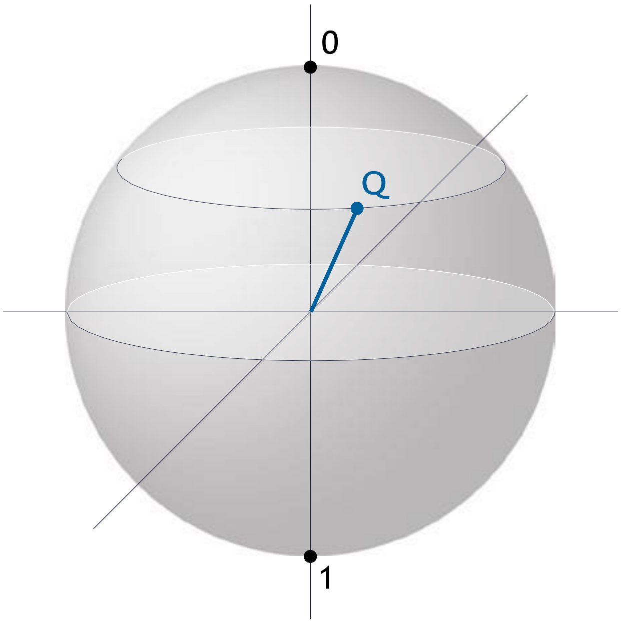
[17] See "The next decade in quantum computing and how to play", P. Gerberg and F. Ruess, Boston Consulting Group, November 2018. Retrieved from https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play.aspx.

1

Superposition

The so-called superposition principle is one of the fundamental principles of quantum mechanics. It says that if a quantum system has two well-defined states – let's call them [1] and [0], which could represent the spin of an electron along one spatial axis – then any combination of these states is also a well-defined state. Such a state is called a superposition state of the pure states [1] and [0]. We can write this state as [Ψ] = a[1] + b[0], where a and b are coefficients quantifying how much each of the pure states contributes to the superposition. This is often represented graphically on what is called a Bloch Sphere (see below). The poles of the sphere represent the pure states. The vector pointing at Q represents the superposition characterised by two angles (related to a and b) that can point anywhere between the north and the south pole.

Superposition states are highly counter-intuitive, because they do not exist in the world of our sensory experience. Think of a coin that can be in either of two states "heads" or "tails". It is very hard to imagine what it would mean for the coin to be in a superposition of "heads" and "tails". For quantum particles, however, such states are possible and quantum computing aims at exploiting them for computational purposes. In contrast to classical bits, which can only have values of either "1" or "0", qubits can be in either state "1" or "0" or any superposition of the two. This allows for more efficient information processing and thus results in increased computing speeds. The problem is just that superposition states are subject to a phenomenon called "decoherence", referring to the very strong propensity of superposition states to decay into pure states upon external perturbation. This makes building a quantum computer so difficult. Decoherence is also the reason why macroscopic objects (like coins) are never found in a superposition. It is virtually impossible to shield a coin from all interactions with its environment.



Unfortunately, superposition states are highly unstable and hard to produce experimentally (which is due to another phenomenon called "decoherence"). To obtain a durable qubit that could be used for computational purposes, one thus has to couple several thousand quantum particles and use error correction to compensate for the instability of the individual particles. This would be the first step on the way to an operational quantum computer and it already constitutes a remarkable engineering challenge. The next step would be to couple two qubits together and the final step would be to scale up to more qubits.

There are two main categories of potential hardware platforms for quantum computing. Atomic platforms that use elementary quantum particles such as single atoms or ions on the one hand (e.g. ion trap qubits), and solid-state platforms that use various types of integrated circuits in semiconductors, e.g in silicon, on the other. Spin qubits are an important implementation of a qubit in a semiconductor, which is considered by many as one of the most promising platforms for quantum computing, in particular because of their high potential for scalability. Much of current research is directed towards improving the quality of the qubits in terms of extending their operational lifetimes and minimising noise introduced by performing operations on the qubits. While scaling and control is a major challenge for atomic platforms, the main problem in solid-state systems is the realisation of quantum superposition and entanglement as well as their stabilisation over time.[18] The most complex programmable systems so far have been based on superconducting qubits. However, at this point in time, it is much too early to know which of the many platforms will ultimately prevail.

Although there remain many technological barriers to be overcome and it is still a very long way to a commercially available quantum computer, noisy intermediate-scale quantum (NISQ) computers with of the order of hundreds of physical qubits (but no error correction), operating in symbiosis with classical (super-) computers, could potentially demonstrate quantum advantage for some commercially valuable computational problems within a five-year timeframe. Among the largest currently available quantum computers are IBM's Q53 with 53 qubits and Google's Bristlecone with 72 qubits. At the same time, it is expected that the intrinsic quality of the qubits will improve over time as well, further increasing the capabilities of NISQ computers. As far as timing is concerned, the general consensus is that we are at least a decade away from an universal quantum computer (UQC) with full quantum error correction (QEC) – barring a major breakthrough in qubit quality. Despite the progress that has been made on the various hardware platforms in recent years, there are still non-trivial scientific and engineering challenges that will require creative solutions to reach this goal. A major breakthrough was achieved in October 2019, when Google published an article in *Nature,* in which they announced to have reached "quantum supremacy". This means that for the first time, researchers were able to solve a computational problem on a quantum computer that would have taken, according to Google, up to 10,000 years for a conventional supercomputer.[19]

It is important to note, however, that the field of quantum computing encompasses more than universal quantum computers – the quantum equivalent of today's classical digital computer – that have attracted so much attention. It also includes quantum simulators (QSs) and quantum annealers (QAs). Quantum annealers can be considered to be machines that run the quantum equivalent of simulated annealing from classical computing. "Annealing" refers to the process of finding the global minimum of a function via random sampling with probabilities constructed according to the rules of classical thermodynamics (simulated annealing) or quantum mechanics (quantum annealing). This is useful for a variety of optimisation problems in different contexts.[20] Although there exist commercially available quantum annealers from D-Wave, there is currently a limited class of potential use cases, and a definite proof for quantum speedup or scaling advantage over classical computers is still missing.[21] Nonetheless, the concept of quantum annealing is important, not only because it is much easier to realise in hardware than error-corrected gate-based quantum processing, but also because it can be implemented on classical hardware. This opens up the prospect of emulating quantum-inspired methods in already available hardware systems.

[18] See Wilhelm et al. (2019, p. 23).

[19] See Gibney (2019a) and Arute et al. (2019).

[20] See Finnila, et al. (1994) and Kadowaki and Nishimori (1998).

[21] Heim, et al. (2015).

Quantum simulators can be considered to be the quantum equivalent of the early (classical) analogue computers based on analogue circuit elements. In contrast to UQCs, which, in principle, could perform various computational tasks if fed with the appropriate algorithms, QSs are special purpose devices that are built to simulate and study specific physical systems. According to an original proposal by Richard Feynman, quantum computing could also model quantum mechanics itself.[22] Research on quantum simulators is being performed worldwide on a number of different physical platforms. The use of ultracold atoms to create synthetic models of many-body quantum systems plays an important role in this regard. Such models allow the study of quantum phase transitions or non-equilibrium dynamics. Quantum simulation research activities are primarily directed at understanding quantum phenomena rather than (directly) developing applications, and several interesting results and insights have been obtained, but there also seems to be increasing interest of late in more targeted activities using quantum simulators.[23] Quantum simulation could also lead to fundamentally new insights into quantum mechanical phenomena underlying biological processes.

It is reasonable to assume that the first generation of quantum computing devices will be special purpose quantum simulators. It is, however, at this point in time difficult to identify with certainty the areas in which quantum computing will actually outperform classical supercomputers. The likely first applications are expected to solve certain scientifically and economically significant problems in chemistry (e.g. simulation of reaction mechanisms),[24] material science (e.g. advanced mul- tifunctional materials and potentially also for supporting the search for potential room temperature superconductors), and particular commercial optimisation problems (e.g. for the solution of complex problems in logistics). A further application for quantum computers is verification and validation of code for various complex control systems. Although up to date, no quantum benefit has been demonstrated in this domain, this might become possible with the quantum computers of the future. Furthermore, Google's quantum supremacy experiment has shown, in principle, that quantum computers can be used to find highly improbable but possible states in complex state spaces, which does indicate their possible utility in the discovery of "black swan" events in complex systems.

There is a growing number of large corporates across a wide variety of industries that are already seriously looking at the potential of quantum computing. They engage with the growing number of quantum consultancies and quantum software start-ups to build use cases and develop algorithms to see if they can create a quantum advantage in their business. To name just a few examples: In 2019, Airbus launched a quantum computing challenge incentivising the quantum computing community to think about how quantum computing could help solving some of the most difficult problems for the aerospace industry such as wingbox design optimisation or aircraft loading optimisation among others.[25] Also in 2019, the car manufacturer Volkswagen, in collaboration with D-Wave and the public transport provider CARRIS, launched the world's first pilot project for traffic optimisation using a quantum annealer.[26]

Despite ongoing controversies among experts about the potential applications of quantum computing, one thing can be said with sufficient certainty: Because quantum computing is a step-change technology, early adopters might benefit disproportionally. As difficult as it might be at the moment to say what quantum computers will actually be used for, we may say with confidence that those who will be able to use them first, will have a significant competitive advantage.[27]

[22] See Feynman (1982).

[23] See "Novo Nordisk Foundation Challenge Programme 2020". Retrieved from: https://novonordiskfonden.dk/en/grants/challenge-programme-2020-natural-and-technical-sciences/.
See also https://pasqal.io.

[24] See Reiher et al. (2016).

[25] See https://www.airbus.com/innovation/tech-challenges-and-competitions/airbus-quantum-computing-challenge.html#ove.

[26] See https://www.volkswagen-newsroom.com/en/press-releases/volkswagen-optimizes-traffic-flow-with-quantum-computers-5507.

[27] See "Where Will Quantum Computers Create Value - and When?", M. Langione, C. Tillemann-Dick, Amit Kuman, and V. Taneja, Boston Consulting Group, May 2019. Retrieved from https://www.bcg.com/publications/2019/quantum-computers-create-value-when.aspx.

1.2 Quantum communication

Just as the universal quantum computer represents the holy grail of quantum computing, a worldwide quantum internet, providing 100% secure communication between all points and entities, is the corresponding holy grail of quantum communication. The ability to establish 100% secure communication channels, protected by the laws of quantum physics, will radically change the cybersecurity landscape and have huge implications for both society in general and national security in particular. However, as was the case for the universal quantum computer, it will take many years of research and development before a quantum internet, i.e. a quantum-safe network between quantum computers, allowing in principle distributed quantum computing becomes ubiquitous.

The technology underlying quantum communication is a method called quantum key distribution (QKD), which enables two parties to share a secret key and encrypt their data in such a way that any attempt by a third party to decrypt the message will be detected. This makes eavesdropping on a quantum encrypted data channel impossible, because any external interference would destroy the quantum information in the encryption key. In principle, there are two ways to implement QKD: terrestrial optical fibre-based systems or space-based systems using earth stations and drones or low orbit satellites. While fibre-based point-to-point QKD systems for short distances are already commercially available, space-based QKD is a technology that is still at an early stage of development. Any quantum encrypted communication over longer distances requires an additional component called a “quantum repeater” that would guarantee the stability of the quantum information over continent-wide distances.

In this context, research in quantum information systems groups at universities all around the world is consequently directed towards developing the quantum repeater. While key components and functionalities such as entangled photon sources and hi-fidelity, long-term quantum memories have been demonstrated, here, too, there still remain non-trivial scientific and engineering challenges that will require creative solutions to reach this goal.[28]

The general consensus is that we are five to ten years away from being able to deploy quantum repeaters in the field. An intermediate step towards this goal without needing quantum repeaters is a satellite-based communication network. This has been demonstrated in a Chinese-Austrian collaboration in 2017 and the European Commission has just (2019) announced an agreement with the European Space Agency to develop a quantum communication infrastructure (QCI) based on (point-to-point) QKD.[29] The time-to-deployment for such systems is of the order of a couple of years rather than the decade for quantum repeater-based systems.

However, as many of the commercially available QKD systems are based on attenuated lasers and therefore not true single-photon sources, they inherently operate at relatively low bitrates. Consequently, there is quite a lot of research worldwide into single-photon sources, typically based on quantum dots. Such improved single-photon sources would both increase the bitrate and the level of security of QKD systems and would accelerate the adoption of QKD technology for space and/or mass-market applications. Indeed, sufficiently fast QKD bitrates would make it feasible to distribute one-time-pads (OTPs) to encrypt and decrypt data instead of a shared secret key. This is particularly attractive since it has long been proven that one-time-pads guarantee 100% security, indefinitely, even with the advent of quantum computers.

Finally, another well-established and key application/technology within the sub-field of quantum communication is the quantum random number generator (QRNG) required to generate the 100% random keys for distribution but which also has uses outside of quantum cryptography, e.g. Monte Carlo simulations, betting sites etc. There are already quite a number of suppliers of QRNGs today, but here again the focus in the near-term will be on increased bitrates and smaller-form factors.

[28] See Touzalin et al. (2016).

[29] See “Real-world intercontinental quantum communication enabled by the Micius satellite", 2017. Retrieved from https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html; and "ESA and EC sign agreement on European quantum communications”. Retrieved from https://artes.esa.int/news/esa-and-ec-sign-agreement-european-quantum-communications.

2

Breaking encryption keys with quantum computers

In 1994, the American mathematician Peter Shor (Shor, 1994) developed a quantum algorithm that can be used to factorise a number into its prime factors (e.g. 15 into 3 and 5). Shor's algorithm is relevant for cryptography, because the asymmetric encryption keys that are currently used for electronic data encryption rely on prime number factorisation. Basically, if two parties exchange an asymmetrically encrypted message, they exchange a shared public key consisting of a number for the encryption, and the decoding party uses a private key that consists of the set of prime numbers needed to factorise that number. The security of the encryption process relies on the secrecy of these prime numbers. Whoever has access to these numbers is able to decrypt the message.

In 2019, researchers factored a 240 digit number in 900 core-years, i.e. it would have taken 900 years for a computer with one core to perform the factorisation. It is estimated that it would take about 500 times longer for a 309 digit number (which is equivalent to 1024 bits of information). By running Shor's algorithm on a quantum computer, the same operation would take significantly less time, which would seriously compromise current asymmetric encryption systems. Yet up to now, quantum computers are neither sufficiently large nor sufficiently error-free to perform such a task. The field of post-quantum cryptography aims at finding novel quantum-safe asymmetric encryption systems in case a quantum computer that can run Shor's algorithm becomes available (see Bernstein, 2009).

Another quantum algorithm proposed by Lov Grover in 1996 could be used to brute force symmetric keys (Grover, 1996). Mathematically speaking, Grover's algorithm allows finite functions to be "inverted", i.e. for a function $y = f(x)$ it produces x if y is given. Grover's algorithm is often referred to as a database search algorithm, because we can imagine a database search as a function that searches for the value of x for a given value of y. This is very similar to brute forcing a secret key (i.e. testing out each possible combination of the key), because it can be compared to finding the correct combination in a database that contains all possible combinations of the key. Brute forcing a 4-digit decimal key on a classical computer takes maximally 10^4 iterations (which is the number of possible combinations of a 4-digit decimal key). A quantum computer running Grover's algorithm would use maximally $\sqrt{}(10^4)$ iterations, which amounts to a quadratic speed up compared to a classical algorithm. Unlike with Shor's algorithm, increasing key sizes can effectively block attacks on symmetric keys with Grover's algorithm. Symmetric keys are thus relatively secure against attacks by quantum computers.

1.3 Quantum sensing

Quantum sensing opens up the ability to sense and measure physical quantities with precision which defies conventional classical intuition, providing new capabilities and insights across a wide variety of applications. Indeed, quantum sensing played an essential role in the successful realisation of the Laser Interferometer Gravitational-Wave Observatories (LIGO) that recently received the Nobel Prize in physics (2017) for the detection of cosmic gravitational waves.[30]

There are quite a number of quantum sensing applications that not only have been identified but have already been developed and deployed. This is perhaps not so surprising given that quantum sensing is a long-established field of research compared to quantum communication and quantum computing.

Quantum sensing typically improves, sometimes quite substantially, the sensitivity/accuracy for known applications, e.g. gravitometers for measuring gravitational fields, and/or provides a cheaper/smaller alternative to existing sensing technologies, e.g. cheaper and smaller magnetometers for measuring magnetic fields instead of large and expensive superconducting quantum interference devices (SQUIDs). In other instances, new, exciting applications that had not previously been possible, e.g. quantum imaging to see around corners can now be developed.

Some of the quantum sensing applications currently being developed and/or deployed across a wide variety of industries are:

- More precise atomic and quantum clocks for timing applications across multiple industries such as finance, energy, telecommunications, military, etc.
- Quantum imaging for autonomous vehicles, medical diagnostics, military surveillance, etc.
- Gravitometers for applications in construction industry, surveying in oil and gas industry, etc.
- Magnetometers (alkali vapour and NV centre-based) for applications in diagnostic medicine, surveying, etc.

Standards and sensing are inextricably mixed, and the most important standards are all based on quantum phenomena, the most recent of which to be discovered is the quantum Hall effect. The study of such macroscopic quantum phenomena underpins not only metrology but also read-out in quantum information systems. Because reliable and low-cost read-out remains a challenge, future advances here, from basic science to device engineering, are still needed for the overall development of quantum technologies.

In this context, national standards laboratories (and their university collaborators) have traditionally played – and will continue to play – a crucial role because of their focus on practical metrological benefits. This role will be strengthened with the recent (and radical) redefinition of the International System of Units (SI) that forms the basis of the metric system base units whereby all seven are now defined with respect to fundamental physical constants.[31] This will facilitate more precise definitions of the standards and quantum sensing will lead the way in terms of enabling more precise and decentralised embodiments of these standards to the benefit of both science and industry.

In the short term (0-5 years), we can expect to see the deployment of gravity sensors, magnetic field sensors and imaging sensors across a wide variety of industries along with the introduction of more precise atomic clocks for timing purposes in the financial sector, energy grids, and telecommunication networks. In the medium term (5-10 years), we can expect to see the introduction of said quantum sensors in high-volume (relatively speaking) markets (and perhaps even consumer applications) as well as quantum clocks. In the long term (10+ years), we may perhaps see a paradigm-shattering quantum sensing application with large-scale commercial potential.

[30] See Nobel Prize in physics 2017 “for decisive contributions to the LIGO detector and the observation of gravitational waves". Retrieved from https://www.nobelprize.org/prizes/physics/2017/summary.

[31] See "BIMP statement: Information for users about the redefinition of the SI.” Retrieved from https://www.bipm.org/utils/common/pdf/SI-statement.pdf.

	Years		
	0	5	10+
Sensing	Niche deployment of gravity, magnetic and imaging sensors Improved atomic clocks	Hi-volume (relatively) sensor applications, possibly consumer applications Quantum clocks	Paradigm-shattering quantum sensing/metrology applications
Communication	Widespread deployment of terrestrial fibre-based QKD systems Hi-speed, telecom-wavelength compatible single photon sources	Satellite-based QKD systems QKD systems with multi-point hops deployed Increased uptake of QKD systems across various data-intensive industries	Terrestrial-based quantum internet with quantum repeaters
Computing	Quantum advantage demonstrated First commercially available quantum annealers	First NISQs without quantum error correction First quantum simulation use cases in material science and chemistry	Universal quantum computer with full quantum error correction

Table 1: Quantum technologies timeline.

2 Activities and developments outside Switzerland

In the past few years, a number of important geopolitical developments related to quantum technology have taken place. In August 2016, China launched the Micius satellite for quantum experiments at space scale providing the basis for "quantum key distribution" (QKD) that makes it possible to encrypt information in such a way that it is impossible for an eavesdropper to decrypt it without being detected.[32] As a reaction to the Chinese programme, the United States Congress passed a *National Quantum Initiative Act* releasing 1.2 billion Dollars to boost US quantum technology.[33] *The Washington Post* recently published an opinion piece calling quantum technology "the most important tech contest since the space race" and comparing the Micius launch to the launch of Sputnik in 1957 that set off the space race between the Soviet Union and the United States.[34]

The European Union has initiated a 1 billion Euro flagship initiative in quantum technology within the European Horizon 2020 research and innovation framework programme involving a broad community of research institutes and industries in Europe. The goal of the initiative is to put Europe at the forefront of quantum technology development, thus creating new commercial opportunities and providing strategic capabilities for security.[35] In coordination and in addition to the efforts of the Union, several European countries have launched their own programmes and initiatives to advance quantum technology. Technology giants like Google, IBM, Intel, Microsoft and others are investing heavily in quantum research and development, and there is a growing international ecosystem of newly founded start-up companies and venture capital (VC) funds specialising in quantum technology.[36]

2.1 National and supranational initiatives

The reason for the relatively large number and geographical diversity of quantum initiatives is linked to the view that "quantum advantage", in particular within the fields of quantum computing and/or quantum communication, would confer an unassailable competitive advantage, both economic and societal, to the recipients.

China, the EU and the US currently run the largest quantum technology programmes. This is not just in terms of the scale and scope of the areas of research addressed, but also in terms of technology development activities pursued.

Of the three recently announced programmes, China's programme is the most centrally coordinated. The US programme is also quite focused on "national security and economic competitiveness" and involves several governmental agencies, each with their own sub-objectives and sub-goals.[37] Coordination between the agencies is achieved through a quantum information science subcommittee – with multi-agency representation – under the National Science and Technology Council.

By contrast, the recent EU initiative, the Quantum Flagship, while also focused on developing "long-term economic, scientific, and societal benefits [for Europe]", is more bottom-up than top-down.[38] This is best illustrated by the fact that the Quantum Flagship projects were selected based on peer review rather than strategic intent at the level of the EU Commission, resulting in a more fragmented strategy. The EU Commission and the Flagship's Board of Founders are the programme's decision-making authorities. In this context, it is also important to note that China and the US in particular have tech giants very actively involved in developing quantum computing hardware platforms. This is not the case in the EU to the same extent.

[32] See Popkin (2017).

[33] See Raymer and Monroe (2019).

[34] See "This is the most important tech contest since the space race, and America is losing", C. L. Nikias, *The Washington Post*, 2018. Retrieved from https://www.washingtonpost.com/opinions/this-is-the-most-important-tech-contest-since-the-space-race-and-america-is-losing/2018/05/11/7a4a4772-4e21-11e8-b725-92c89fe3ca4c_story.html?noredirect=on&utm_term=.0b69a28c136b.

[35] See Touzalin et al. (2016).

[36] See Gibney (2019b).

[37] See https://www.hpcwire.com/2018/09/17/house-passes-1-275b-national-quantum-initiative.

[38] See https://ec.europa.eu/digital-single-market/en/news/quantum-flagship-high-level-expert-group-publishes-final-report.

Other countries such as France, Germany and the UK in Europe, or Japan and South Korea in Asia have launched their own quantum technology programmes. The programmes in these countries are typically characterised by the same broad scope but on a smaller scale (and budget) compared to the larger programmes. There is often collaboration with the respective national industrial base and companies, e.g. ATOS and Thales in France, Bosch in Germany, Airbus in UK, Hitachi in Japan, etc. By and large, many of these companies are not in the same financial league as the tech giants and the advent of quantum technologies will not be, at least initially, so disruptive for their industry. For this reason, they are typically not yet as engaged at this point in time.

The national programmes in this category are typically more targeted, leveraging research areas of strength rather than any (quantum) strength of a national industrial base. Consequently, there are currently very modest levels of involvement (and investment) from national industries. Industrial involvement is typically limited to providers of key enabling technologies and services rather than large corporates. This is perceived as an acceptable and desirable objective in the short term as part of efforts to establish a quantum cluster that will ultimately lead to a quantum industrial base. The UK, which has a more "quantum-ready" industrial base than the smaller nations in Europe, is particularly clear on this score.[39]

Both the UK and Netherlands took a very strategic, long-term position with respect to quantum technologies at an early stage (over five years ago). Since then, several other nations have followed, including Denmark (2016), Germany (2017) and Sweden (2017). Because of the lack of a relevant industrial base, smaller nations are often more open to collaboration with tech giants and/or non-national partners despite concerns among some sectors of their respective societies. This is due to the tacit acknowledgement of the paradigm-shifting consequences of quantum technologies for a nation's societal wealth and security. Prominent examples in Europe include the Netherlands (Microsoft/Intel), Denmark (Microsoft), and Austria (Micius satellite).

Table 2 provides an overview of a selection of some of the most recent national initiatives and programmes to develop quantum technologies. The list is by no means comprehensive, even for a given country, but serves to highlight the increased level of activity in recent years.

[39] See "The Quantum Age: Technological Opportunities", UK Government Office for Science, 2016. Retrieved from https://www.gov.uk/government/publications/quantum-technologies-blackett-review.

Country	Programme Name	Initiated	Duration (years)	Government Funding (m€)
China	National Laboratory for Quantum Information Sciences	2017	10	9,000 (unconfirmed estimate)
USA	National Quantum Initiative Act[40]	2019	5	1,100
EU	EC Quantum Flagship[41]	2018	10	1,000
UK	UK Quantum Hub[42]	2014	10	700
Germany	QUTEGA[43]	2018	5	650
Japan	Q-LEAP[44]	2018	10	182
Netherlands	QuTech[45]	2015	10	115
Sweden	WACQT[46]	2018	10	80
Canada	QMFT[47] TQT[48]	2015 2016	10 10	46 52
Austria	QFTE[49]	2017	4	33
Australia	CQC2T[50] EQUS[51]	2017 2017	7 7	21 20
Denmark	Qubiz[52]	2016	3	11

Table 2: Overview of selected recent national initiatives and programmes to develop quantum technologies. Funding numbers do not include funding from university or industrial partners.

[40] See https://www.congress.gov/bill/115th-congress/house-bill/6227/text.

[41] See https://qt.eu/.

[42] See http://uknqt.epsrc.ac.uk.

[43] See https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf.

[44] See https://www.jst.go.jp/stpp/q-leap/en/index.html.

[45] See https://qutech.nl.

[46] See https://www.chalmers.se/en/centres/wacqt/Pages/default.aspx.

[47] See https://grex.ubc.ca/stewart-blusson-quantum-matter-institute.

[48] See https://tqt.uwaterloo.ca.

[49] See https://www.fwf.ac.at/en/research-funding/application/qfte/.

[50] See https://www.cqc2t.org.

[51] See https://equs.org.

[52] See http://qubiz.dk.

2.2 Tech giants

The fact that US tech giants (Google, Amazon, IBM, Intel, and Microsoft) – recently joined by Chinese tech giants Alibaba, Huawai and Tencent – have substantial research and development programmes for universal quantum computers has brought quantum technologies into the public eye, particularly during the last three years. In this perspective, the tech giants are almost perceived to be synonymous with quantum computing. This is not so surprising when one considers that each of them is spending more than many countries do on their national initiatives.

The majority of the tech giants are pursuing a platform based on superconducting circuits (generally considered to be the leading candidate at this point in the race) with the exception of Microsoft, which is betting on topological quantum computing. Google and Intel are, however, hedging their bets in that they both have additional activities on quantum annealers (Google) and spin qubits (Intel).

It is also interesting that all companies are either very dependent on computational power to run their businesses (Google, Alibaba, and Tencent), or their current business is to provide hardware, software and services (Microsoft, IBM, Intel). Their motivation is clearly strategic and/or defensive but there is no doubt that their businesses would be significantly impacted by a new computing paradigm such as quantum computing.

Within the last couple of years, IBM, Alibaba and Rigetti (one of several quantum computing start-ups that are beginning to appear), have made their quantum computers accessible on-line and are actively developing quantum computing ecosystems. In addition to securing intellectual property, some of them are now moving to secure the minds and hearts of corporate customers. IBM in particular with the IBM Q Network, bolstered by the recent announcement of its stand-alone System One quantum computer whereby customers can have their own quantum computing system in-house for their exclusive use. Even Microsoft, though it has not yet announced that it has a topological qubit, has developed a full-stack software suite (which is also compatible with the other technology platforms) and is engaging with customers and collaborators on, among other things, quantum inspired optimisation projects. Although IBM was first out of the gate with their “quantum readiness” mantra, it is clear that several others are now beginning to pick up the pace, including some start-ups.

It is interesting to note that while other quantum technologies such as quantum communication and quantum sensing have not received the same level of attention or funding from the tech giants listed above, these technologies have received significant interest (and funding) from various national initiatives because of the obvious importance of secure communications and superior defence capabilities for national security.

2.3 Education and skills

Much in the same way that physicists led the way during the first quantum revolution, right up to the invention of the semi-conductor transistor, the subsequent successful development of integrated circuits and the laser necessitated educating engineers about solid-state physics. Today, solid-state electronics is a standard – and integral – part of all electronic engineering degree programmes. Back then, engineers had to be educated – by physicists – about quantum physics. By learning the “language” of quantum physics and developing a basic intuition about it, the necessary basis for fruitful communication was established. We are in the same situation today, where cross-disciplinary skills are at an even greater premium given the inherent complexity of quantum technologies at this point in time.

Several universities and national initiatives have already recently established courses in quantum engineering while others have established centres for doctoral training (CDTs) in quantum technologies, some of them over five years ago, e.g. University College London (UCL) in the UK. At UCL, the participants in the first CDT (which was called “Developing Quantum Technologies”) were predominantly physicists – today there is a much greater proportion of engineers, computer scientists, chemists in the quantum CDTs.[53]

[53] See also the joint doctoral program QUSTEC at the European Campus: https://www.eucor-uni.org/de/qustec.

Another technique employed by several national initiatives is to engage with national standards laboratories, i.e. the local equivalents of NIST in the US. Both NPL and TNO in the UK and the Netherlands, respectively, have played – and continue to play – crucial roles in advancing the technological development of quantum technologies from academia while providing "on the job training" for their employees. It is also well-known that the tech giants are having difficulty recruiting qualified quantum engineers for their quantum computing programmes: they realise that engineering is essential to developing and producing stable, scalable and manufacturable quantum computing systems. Quantum engineers are a scarce resource, particularly those with significant and relevant experience.

Many of the quantum algorithm developers today are physicists, but just as the engineers who programmed the first mainframes have been supplanted by computer scientists and programmers, so too will the physicists over time. Developing and formulating quantum algorithms is – even with the levels of abstraction built into the software provided by IBM, Microsoft, Rigetti and others – a completely different programming paradigm. Even if the instruction set and programming environment seem familiar, the syntax is different. It will consequently require a new mindset to develop efficient and effective algorithms: the earlier the new generation can start, the better.

In addition, just as the programming languages of the first mainframes evolved in a symbiosis between hardware and software developers, so too is it expected to be the case for quantum computers. This time the quantum computers are on-line and accessible for a much larger group of users, accelerating this process. It is also interesting to note that IBM has approximately 300 high schools signed up to IBM Q Experience at this time.

This being said, it should be noted that quantum technology development requires a level of multidisciplinarity that goes far beyond physics, engineering and computer science alone. Because quantum technologies are likely to have paradigm-shattering consequences in many areas of society and the economy, it might be prudent to also include experts from the social sciences at an early stage. Economists, legal experts, sociologists, ethicists and experts from similar fields will have an important role to play when it comes to the responsible implementation of quantum applications in society.

2.4 The link to investors

Given the proliferation of unicorns – which are not so rare as they were just 5 years ago – and the significantly reduced time start-up companies require to reach valuations in excess of 1 billion US dollars, investments in deep tech i.e. quantum technologies are not yet as attractive from a risk/reward perspective. That said, some tier-1 VCs have already invested in quantum computing hardware start-ups, e.g. Andreesson Horowitz in Rigetti Computing, New Enterprise Associates in IonQ, and Sequoia in Quantum Circuits Inc.[54] All three investments in these US-based start-ups have taken place within the past three years but they are the only quantum computing investments these tier-1 VCs have made to date. Their first investments seem to have been exploratory investments.

Most of the VCs investing in quantum technology are typically smaller, early-stage VCs that are (or ought to be) familiar with deep tech. Some of them are corporate, e.g. Airbus, where there obviously is a strategic angle as well. However, an increasing number of VCs specialising in quantum technologies are beginning to appear (also in Europe), particularly during the past two to three years. The same is true in China, particularly within the field of quantum communication, although it is more difficult to quantify.[55] All of the above would seem to indicate that there is growing and real interest from the VC industry in this domain.[56] It is interesting to note that the EU, cognisant of the difficulty quantum technology start-ups have attracting capital, is aware of the need for a specialised "quantum innovation fund" to address this issue.[57]

[54] See https://www.rigetti.com/about, https://ionq.com/company#about and https://www.quantumcircuits.com/about.

[55] See https://www.nature.com/articles/d41586-019-02935-4.

[56] See https://quantumcomputingreport.com/players/privatestartup/.

[57] See https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-quantum-technologies.

Just as there are very few tier-1 VCs in quantum, there are very few quantum computing hardware start-ups: most of the quantum start-ups are typically software companies providing quantum algorithm-based consultancy services. There is, however, also a significant number of start-up companies providing hardware products within the key enabling technologies, primarily lasers and microwaves. Many of these companies also serve dual markets i.e. quantum customers and non-quantum customers that – in some cases – also benefit from the improved performance and/or capabilities required by their quantum cousins. Having a non-quantum customer segment serves to stabilise their business footing while the quantum market develops.

Many national initiatives include programmes to encourage and support quantum tech start-ups and are obviously aware that the entrepreneurship culture is typically not as prevalent in physics departments as it is in engineering departments, some even have incubator programmes exclusively for quantum tech start-ups, e.g. the University of Bristol in the UK. Here again the EU is aware of the need for incubation hubs with, not least, dedicated technological facilities given the capital-intensive nature of many quantum technology (hardware) companies.

The role played by a healthy quantum start-up environment in the creation of a new industry should not be underestimated. Just as start-ups like Fairchild Semiconductor and particularly Intel played a central role in the establishment of the semi-conductor industry as the force it is today, the start-ups of the second quantum revolution can be expected to drive innovation in much the same way.

2.5 The link to industry

Apart from the tech giants that have a clear strategic and business interest in actively engaging in research and development of quantum computing technology, there are two types of industrial partners (three for quantum computing) for which quantum technologies are particularly relevant:

- The early adopters, particularly within quantum computing (currently high performance computing users) and quantum communication (currently ultra-secure communication system users).
- Manufacturers and providers of both quantum technology (sub-)systems and key enabling technologies.
- Quantum software development companies and consultancies.

The diversity of the various industrial collaborators clearly illustrates the cross-disciplinary nature of quantum technologies at this point in time.

2.5.1 Quantum computing

For quantum computing (which includes quantum annealers and, to some extent, quantum simulators), the early adopters are expected to be organisations that are already heavy users of (or whose businesses depend upon) high-performance computing (HPC).

By way of illustration, D-Wave’s first publicly-known customers included organisations like NASA and Lockheed Martin that fit that profile. With the recent arrival of the on-line NISQ computers (led by IBM), companies such as Airbus, Barclays, Daimler, Samsung, etc. have already publicly started quantum computing pilot projects and many others are beginning to monitor the space. According to analysts at International Data Corporation (IDC), by 2021, 25% of the top 500 European corporations will have a budget for quantum computing, up from 5% in 2018.[58] It is also worth noting that these companies represent a very diverse selection of industries. As touched upon in the previous chapter, a number of industries and sectors, such as the pharma and chemical industries as well as the financial sector, will be among the first to be impacted because their businesses are already critically dependent on high performance computing.

[58] See “State of the Quantum Market and Ecosystem”, A. Elbak, International Data Corporation, April 2019. Retrieved from https://www-01.ibm.com/events/wwe/grp/grp308.nsf/Agenda.xsp?seminar=D53GP6ES&locale=da_DK.

In the second category, there are a host of providers of key enabling technologies that are typically enhanced and modified to match the specifications and requirements of research groups and companies working on the physical quantum computing platforms and quantum technologies in general. Their role has been compared to that of the suppliers of picks and shovels to prospectors looking for gold: only a few of the prospectors will strike gold, but all of the suppliers of picks and shovels will do very well irrespective of who actually strikes gold. These types of industries are valuable players in the quantum ecosystem and can form the basis of a (national) quantum industry, even if one does not have full universal quantum computing manufacturing capability. In some instances, it will be a case of existing companies adapting and/or upgrading their existing technology; in other instances, it will be a start-up precisely because existing companies do not address the need, considering it to be too niche and/or not of strategic value or interest. Either way, the ecosystem grows and expands.

In the context of quantum computing, there is, in fact, a third category: quantum software development companies and consultancies. This is because the vast majority of the early adopters do not, at this stage, have the necessary expertise to take their computational problems and parse them in a form for which quantum algorithms can be written. For this reason, there has been a rapid growth during the past couple of years in the number of software firms offering precisely these services and, by the same token, many of these firms have entered collaborative agreements with the Tech giants.[59] This trend is driven by the hope that it will be possible to deliver (quantum) value in the short term on the NISQ platforms currently available. In many regards, this could be a catalyst for continued and increased interest and investment in quantum computing: Unequivocal examples of quantum algorithms developed for and subsequently run on NISQ computers that provide real commercial value would be extremely effective arguments for this.

Finally, it is also pertinent to note that within the last twenty-four months alone, a slew of white papers from all of the major consultancies (Boston Consulting Group, Deloitte, Gardner, Accenture, and McKinsey) on what their clientele (typically large corporates) should do about quantum computing have been published.[60] While this can be viewed as a strategy to generate new business for themselves, IDC's predictions would seem to make this a profitable proposition for them. This notwithstanding, the fact remains that they are also an important part of the quantum ecosystem.

2.5.2 Quantum communication

The first customers of quantum cryptography (a sub-field of quantum communication) products such as QKD systems have been government organisations (including the military) and players in the financial sector. There are indications, however, that data centre owners are also becoming increasingly interested in deploying QKD systems.[61]

Although terrestrial quantum internet-like communication systems are not yet available today, it is expected that these customers will be among the early adopters here as well. In the interim, government agencies around the world are actively supporting a number of satellite-based QKD network projects and programmes with a view to substantially increasing the range of secure communication networks in this manner.

In general, however, there is a growing awareness of the importance of cybersecurity in an increasingly digitalised society that is moving beyond the traditional client/server IT infrastructure to encompass autonomous vehicles/robots, IoT, AI, etc. This increased awareness and concern is driving the introduction of improved (classical) security measures in many countries and generating genuine interest in QKD – the only way to provide 100% secure communication channels – along with it.

[59] See "Quantum Computing Software Partners". Retrieved from https://quantumcomputingreport.com/scorecards/software-partners.

[60] See "An Exponential Increase in Quantum White Papers for Enterprise End Users", The Quantum Computing Report. Retrieved from https://quantumcomputingreport.com/our-take/an-exponential-increase-in-quantum-white-papers-for-enterprise-end-users/.

[61] See "Quantum Key Distribution (QKD) Markets: 2019-2028", Inside Quantum Technology, April 2019. Retrieved from https://www.insidequantumtechnology.com/product/quantum-key-distribution-qkd-markets-2019-2028/.

This is encouraging news for the current suppliers of QKD systems (both larger companies with a broad telecommunications equipment product portfolio like Toshiba and smaller companies with a focused portfolio like ID Quantique in Geneva) and it will drive the demand for QKD systems that have longer reach and faster bit rates. One indication of this increased interest are the recent investments made by South Korea Telecom and Deutsche Telekom – both telecommunication network operators – in ID Quantique.[62]

2.5.3 Quantum sensing

Industrial engagement within the field of quantum sensing is much more fragmented given the broad nature of the potential applications across a large number of different industries combined with the fact that no killer application has yet been identified: quantum sensing typically improves the sensitivity/accuracy for known applications or provides a cheaper/smaller alternative to existing sensing solutions.

It is worth pointing out, however, that technologies such as quantum imaging (providing enhanced visibility in bad lighting conditions, including the ability to see around corners) and quantum timing (the ability to navigate autonomously without an operational satellite-based GPS infrastructure) are applications that are of great interest to the defence industry, where price often takes a second seat to performance.

In some instances, it may make more sense to incorporate the quantum sensors into an existing system thereby directly introducing quantum technologies into an existing industry. As many of these sensors measure parameters that are of interest across a broad range of industries and applications, many industries will become "quantum conversant" in this manner.

In other cases, it may make more sense to provide a complete stand-alone system (whole product), which may be a more suitable proposition for a start-up rather than an established company. Either way, the fragmented nature of the space represents an interesting niche for both start-ups and industrial partners already providing sensing solutions that could be enhanced by quantum technologies.

2.6 Case studies

2.6.1 Qubiz – Quantum Innovation Center (Denmark)

In 2016, Denmark established a national quantum initiative, the objective of which was to "bring quantum technologies to market" by "investing in activities that contribute as much as possible to the full application potential of quantum technology".[63] The consortium comprises three Danish universities (along with three non-Danish universities) and 16 industrial partners, half of which are non-Danish. The total budget for the first two-year phase of the initiative was approximately 21 mil- lion Euro: 10.5 million from the Innovation Fund Denmark (a Danish funding agency that invests in knowledge-based initiatives that will create growth and jobs) and 10.5 million from university and industrial partners in the form of cash and in-kind contributions.

The scope of the activities covers quantum computing (including quantum algorithms), quantum communication, and quantum sensing (including quantum metrology). A significant proportion of the funded activities were collaborative projects between university and industrial partners. In addition to the technical work packages, there is also a work package dedicated to business development, the objective of which is to:

[62] See "Deutsche Telekom plans to make a strategic investment in ID Quantique", October 2018. Retrieved from https://www.idquantique.com/deutsche-telekom-plans-to-make-strategic-investment-in-idq/.

[63] See http://qubiz.dk.

- train and build an innovation culture within the university community;
- provide business development support for new businesses (start-ups) or new products in existing businesses;
- create broader awareness and understanding among (non-quantum) stakeholders of the potential of quantum technologies.

Qubiz built upon a number of research centres of excellence within quantum technologies funded by the Danish National Research Foundation and two more were initiated shortly after Qubiz started.

Despite this and a number of positive results from the initial phase, the funding for the second (three-year) phase was not granted by the Innovation Fund Denmark, illustrating the importance of matching the expectations and investment horizon of the funding source with the maturity of the technology. It also underscores the importance of establishing a broadly-based coalition of stakeholders with a long-term, strategic funding perspective.

2.6.2 QuTech – Research and Development in Quantum Technology (The Netherlands)

In 2015, The Netherlands established a ten-year quantum initiative, QuTech, with the mission to "develop scalable prototypes of a quantum computer and an inherently safe quantum internet".[64] The initiative, which grew out of a two-year precursor project of the same name, is built up around several departments at the Technical University of Delft (TUD) and the Netherlands Organisation for Applied Scientific Research (TNO), but now also includes the Ministry for Economic Affairs, the Ministry for Education, Science and Culture, and the two Dutch organisations responsible for basic research (Netherlands Organisation for Scientific Research NWO) and high-tech investments (Top Sector Alliance for Knowledge and Innovation TKI), respectively. The presence of both Microsoft and Intel on campus at TUD has been instrumental in triggering some components of the funding from NWO and TKI.

The total budget for the ten-year period is 146 million Euro, of which approximately one-third is provided by TNO, one-third is provided by NWO and TKI combined, and the remaining one-third is provided by TUD itself. Approximately 80% of the total funding is cash. The programme is organised around three mission-driven science and technology road maps (led by TUD principal investigators):

- Fault tolerant quantum computing
- Quantum internet and networked computing
- Topological quantum computing.

In addition, there is an engineering road map (led by TNO): Shared technology development (SHD).

Since the establishment of QuTech, two new quantum initiatives (with a smaller scope but also mission-driven) have been established in the Netherlands: QuSoft at the University of Amsterdam and the Eindhoven Q Center at the Technical University of Eindhoven. Combined with the highly successful mid-term evaluation of QuTech earlier this year, there was a basis for establishing a quantum national agenda programme (four-year) to bring all relevant stakeholders in the Netherlands, including industry, together to accelerate the economic impact of quantum technologies and address common societal challenges.

The strength of a quantum national agenda developed in this manner is that it has grown organically, albeit over a longer period of time, but builds upon established collaborations and relationships and is therefore intrinsically more cohesive than otherwise would be the case.

[64] See https://qutech.nl.

2.6.3 QFTE – Quantum Research and Technology (Austria)

In 2016, the Austrian Council of Ministers announced a new national R&D funding programme for quantum research and technology, including demonstrators.[65] The objective of the programme was threefold:

- to further increase the cooperation of Austrian researchers and companies in European and international initiatives;
- to enable the development of quantum relevant skills and R&D infrastructure;
- to support the transfer of R&D results into value and demonstrators.

The budget for the initial four-year ramp-up phase (2017-2021) is 32.7 million Euro and is provided through the Austrian Research Promotion Agency, the national funding agency for industrial research and development, and the Austrian Fund for the Promotion of Scientific Research. Funding is allocated on a yearly basis through a competitive application process and projects are evaluated on an annual basis. 4.5 million Euro will be allocated during 2019. The scope of the programme is broad in that there are no pre-defined areas within quantum science and technology and it is not mission-driven. The Austrian initiative not only builds upon a number of early initiatives such as the Vienna Center for Quantum Science and Technology and the Erwin Schroedinger Center for Quantum Science and Technology but also specifically strengthens these initiatives as integral parts of the QFTE programme.

The strength of a funding programme of this nature is that it maintains a greater level of flexibility and agility compared to more mission-driven programmes but without the latter’s focus and concentration of resources on specific objectives and outcomes.

[65] See https://ec.europa.eu/newsroom/document.cfm?doc_id=43132.

3 The Swiss situation

3.1 National activities in quantum to date

Switzerland has a long and successful history in quantum science. Many scientists who made important contributions to the theoretical foundations of quantum physics in the first half of the 20th century, worked in Switzerland. Swiss researchers were also centrally involved in the development of nuclear magnetic resonance spectroscopy (NMR), one of the first quantum technologies, which led to three Swiss Nobel prizes (Felix Bloch in 1952, Richard Ernst in 1991 and Kurt Wuethrich in 2002). Today, the most powerful and arguably the world's best nuclear magnetic spectrometers are still manufactured in Switzerland. The IBM research laboratory in Rueschlikon has a long history of collaboration with Swiss universities, also within quantum science and technology. Switzerland also has a longstanding tradition in precision manufacturing and micro-technology development, especially in Western Switzerland, where some of the world's most advanced miniature atomic clocks (another technology that is based on quantum effects) are currently being developed. In combination with its strong advanced manufacturing and industrial base in other sectors, Switzerland is well-situated for supporting the complex engineering challenges of quantum technology development and commercialisation.

Furthermore, the establishment of a series of National Centres of Competence in Research (NCCRs) in the past two decades has put Switzerland in a leading position within a broad selection of research fields within quantum science.

The NCCR "Nanoscale Science" (2001-2013)[66] had a total core funding of around CHF 62 million (50 mio SNSF funding and 12 mio from the University of Basel as leading house) of which roughly a fifth went into quantum science and technology projects in Basel, at ETH Zurich and IBM Rueschlikon. The NCCR was later turned into the permanent Swiss Nanoscience Institute at the University of Basel and was a stepping stone for following NCCRs.

The NCCR "Quantum Photonics" (2001-2013)[67] with a core grant of approximately CHF 68 million (45 mio SNSF funding and 23 mio from EPF Lausanne as leading house) over the lifetime of the programme was the first large-scale programme of its kind for quantum information sciences in Switzerland. It enabled Switzerland in general, and the University of Geneva in particular, to strengthen its position within the entire field of quantum communication and quantum cryptography, both in terms of the science and the technology. The University of Geneva established this position of strength through a number of pioneering and ground-breaking quantum communication field demonstrations during the 1990s and continues to be at the forefront of this key research area.

Both of these programmes established a solid foundation for the ongoing **NCCR "Quantum Science and Technology QSIT" (2010-2021)**[68] with a core funding of approximately CHF 101 million (52 mio SNF funding, 34 mio from ETH Zurich and 15 mio from the University of Basel as co-leading houses). In terms of size, the NCCR QSIT encompasses about 40 professorships in Zurich, Basel, Lausanne and Geneva. The broadness of the programme is unique compared to the research efforts at other places in Europe that often focus on one or only a few technological approaches. As far as quantum computing is concerned, ETH Zurich has established a strong scientific and technological position regarding key aspects of superconducting qubit-based technologies through its collaboration with other members of the NCCR, not least IBM's research laboratory in Rueschlikon. Within the field of quantum simulators, the QSIT NCCR has been instrumental in establishing Switzerland as one of the pioneers and leaders in this field in terms of experiments and advancing the theoretical understanding of quantum systems. Within the field of quantum algorithms – the means by which the computational power of quantum computers can be realised – Switzerland is well positioned to build upon quantum algorithm research initiatives such as ProjectQ at ETH Zurich and interaction with both IBM Zurich and Microsoft Zurich on key components of their respective quantum computer software stacks.

[66] See http://www.snf.ch/en/researchinFocus/nccr/nccr-nanoscale-science/Pages/default.aspx.

[67] See http://www.snf.ch/en/researchinFocus/nccr/nccr-quantum-photonics/Pages/default.aspx.

[68] See http://www.snf.ch/en/researchinFocus/nccr/nccr-qsit/Pages/default.aspx#.

The establishment of a new **NCCR "SPIN: Spin Qubits in Silicon"**[69] in 2020 (leading house University of Basel) shows a sustained commitment to strong quantum science in Switzerland. The new NCCR encompasses collaborations between several research groups at different Swiss universities and IBM research in Rueschlikon. The goal of the programme is to develop small, fast, scalable silicon-based qubits that would enable the construction of a universally usable quantum computer.[70] In comparison to QSIT, which had strong pillars in all domains of quantum technology, SPIN obviously has a strong focus on quantum computing and on one specific qubit platform largely pioneered in Australia and already being followed up by Intel and various universities (e.g. Delft and Princeton) worldwide. This constitutes a risk and an opportunity at the same time: the opportunity to become a player in the development of spin qubits, and the risk of impairing some of the diversity of the preceding NCCRs.

Swiss quantum scientists also have a successful record in the acquisition of European funding. In the current EU Quantum Flagship programme, Switzerland is represented in 10 of the 14 application project consortia that comprise the first phase (130 mio Euro in total EU funding) of the, in total, 1 billion Euro programme. More significantly, Switzerland (both academia and industry, including start-ups) is represented in the larger (typically 10 mio Euro in EU funding) application-oriented projects across all pillars of the flagship. One of the quantum sensing consortia, macQsimal, is led by the CSEM where there is a strong focus on applications and commercial potential.[71] Participation in international programmes such as these serves to leverage the strong research and industrial positions of Swiss partners and, not least, further develop their capabilities and expertise through international collaboration.

	Number of Project Consortia in Total	Number of Consortia with Swiss Partners
Quantum Computing	2	2
Quantum Simulation	2	1
Quantum Communication	4	3
Quantum Sensing	4	3

A recent bibliometric study confirms the high competitiveness of Swiss quantum research. Although it cannot compete with larger nations like China, USA or Germany in absolute numbers of publications, Switzerland (together with Austria) is leading the field with a large margin in terms of the proportion of most cited papers in quantum technology (see Figure 1).

[69] See http://www.snf.ch/en/researchinFocus/nccr/spin/Pages/default.aspx#.

[70] See https://www.unibas.ch/en/Research/NCCR/Spin.html.

[71] See https://www.macqsimal.eu/.

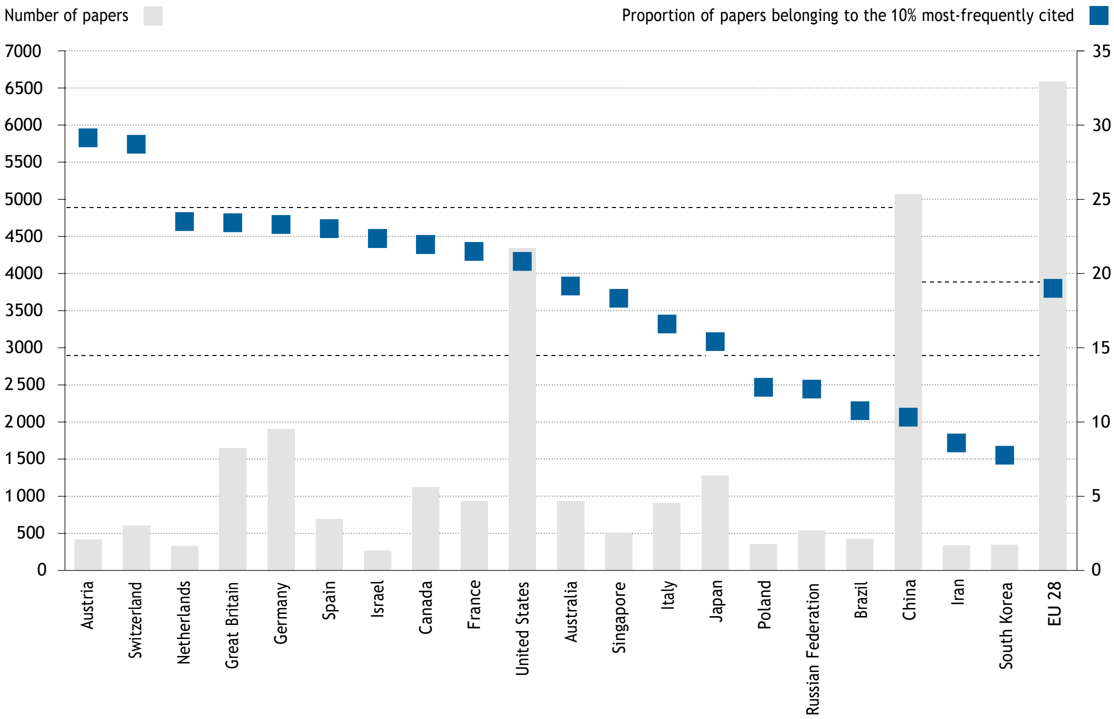


Figure 1: Countries with the most papers published in the field (between 2012 and 2016) and proportion of papers belonging to the 10% most frequently cited papers (including the EU 28). The countries are ordered by the proportion of papers belonging to the 10% most frequently cited papers. Figure reprinted from Bornmann, Haunschild, Scheidsteger, and Ettl (2019).

The continued and sustained financial engagement in world-class basic quantum research has led to successful and promising start-up companies in the domain of quantum technology, some of which already have or are on a good track to become world leading in their domain. The Geneva-based company ID Quantique has been pioneering the commercialisation of quantum encryption technologies. It has become a world-leading supplier of both QKD systems and QRNGs (Quantum Random Number Generators). This position has only been strengthened by ID Quantique's recent deal with South Korea Telekom and Deutsche Telekom under which South Korea Telekom transferred all its quantum technology activities to ID Quantique.[72] In close partnership with ID Quantique and IBM, the QSIT NCCR has helped spawn companies like Qnami, Q-Zabre, LiGenTec, IRSweep, MicroRsystem LLC, and BASPI that are active in quantum sensing and communication, and work hand in hand with companies such as Zurich Instruments and Basel Precision Instruments, who provide key enabling technologies in the form of advanced, non-cryogenic components, i.e. room temperature, high-speed control systems and ultra low-noise stable electronics for the measurement and control of quantum information systems.

To support and expand existing assets and to further exploit strategic advantages, it is crucial to take suitable measures to ensure a successful and swift transfer of knowledge and technology from academia to industry. Private-public research and development institutions like the CSEM play a crucial role in this regard. Networking and information platforms like the recently established Swiss Quantum Hub and events like the annual Quantum Industry Day in Zurich help to foster an exchange between academia, industry and investors and to accelerate the development of new quantum products.

Switzerland is in possession of all of the capabilities and resources required to foster and develop a viable quantum industry. The challenge is primarily one of coordination and communication: Coordination to ensure that a careful balance is struck between exploratory and mission-oriented research at this early stage, and communication to ensure that the interaction between academia and industry is mutually beneficial, furthering the goals of both.

[72] See https://www.idquantique.com/sk-telecom-continues-to-protect-its-5g-network-with-quantum-cryptography-technologies/; and https://www.idquantique.com/deutsche-telekom-invests-in-swiss-cryptography-company-id-quantique/.

3.2 Education and skills

It is generally recognised within the Swiss university system, quantum researchers in general and the fledgling quantum start-ups that there is an increasing need for augmenting education within quantum science and technology and thinking in terms of cross-disciplinary programmes.

ETH Zurich has provided a wide range of courses within this area for many years. The Department of Physics has been offering core courses in quantum information processing in its master programme for some years. In addition, since autumn 2019, ETH Zurich is offering a master programme in Quantum Engineering.[73] This course is a cross-disciplinary collaboration between the Department of Physics and the Department of Information Technology and Electrical Engineering at ETH. There is already a lot of interest from students at both departments, giving credence to the thesis that the combination of intellectual fascination and application potential within quantum science and technology is an attractive proposition to attract the best students.

In 2016, the Department of Physics at the University of Basel established the first PhD School in Quantum Computing and Quantum Technology in Switzerland with about 60 PhD students. In collaboration with the Albert-Ludwigs University in Freiburg (Germany), the University of Basel also created the Endress Postdoc Cluster in Quantum Science and Quantum Computing, a ten-year initiative funded by the G.H. Endress Foundation to foster and educate outstanding young scientists in areas like quantum information processing, quantum technologies, complex quantum systems, quantum materials, and other emerging topics in quantum science.

Quite apart from formalised education, there are also many advantages i.e. knowledge transfer and upgrading of skills for both academia and industry by supporting industrial PhDs or postdocs and by fostering collaboration on specific projects of mutual interest as exemplified by ID Quantique’s long-standing collaboration with the University of Geneva.

It is also worthwhile to mention the important role that the universities of applied sciences (UASs) could play in the growing Swiss quantum technology ecosystem. With their strongly application-oriented approach to research and teaching, their long-standing experience in the training of highly skilled specialists, as well as their proximity to Swiss industry, the UASs are ideally positioned to complement the efforts of universities in producing the highly specialised workforce needed to develop quantum technology. A diverse quantum industry needs many well-trained practitioners who are able to implement innovative technological ideas in usable and customer-friendly applications.

This notwithstanding, quantum technology development requires a level of multi-disciplinarity that goes far beyond physics, engineering and computer science. In light of the disruptive potential of quantum technologies, their implementation in society will pose a variety of challenges on different levels: economic, legal, and ethical. One obvious question concerns the consequences of decrypting all stored communications encrypted using pre-quantum algorithms, which can be more prosaically stated as “What happens when people can read all of your emails?”. Another concerns the exploitation of quantum communications by terrorist and other criminal syndicates. This means that the education of a workforce necessary for the development of a sustainable quantum technology ecosystem in Switzerland is likely to succeed only if the social sciences are included in this process. In a post-quantum society, economists, lawyers and social scientists need a robust understanding of both the technology and its implications if they are to successfully manage and regulate it. Technical competence should therefore be integrated into their curricula as well. For Switzerland, it might be worthwhile, for example, to consider a potential role for an institution like the University of St. Gallen in the training and education of social scientists that are fit to tackle challenges posed by quantum technology.[74]

[73] See https://master-qe.ethz.ch/.

[74] See as an example the University of St. Gallen's animated GIFt on quantum cryptography: https://imp-ccg.unisg.ch/en/wissen/animierte-forschung/academic-gifts.

3.3 The link to investors

Although it continues to develop and grow, the (tech) start-up environment in Switzerland is not as well-funded as those in the US, Israel, and the UK but comparable to most European countries, also in terms of its risk profile. The fact that this is not a conducive environment for "paradigm-shattering" tech companies cannot be solely attributed to a risk-adverse culture of VCs since this – paradoxically – does not seem to be the case for Swiss venture investments in the biotech sector.

In this context, it is interesting to note that all the VCs and telecommunication companies that have invested in ID Quantique, perhaps the best-known Swiss quantum start-up, are non-Swiss. In addition, given the strategic and commercial importance of secure communications, it would seem that government agencies, telecommunication companies, and financial institutions in Switzerland are less proactive than their counterparts in other countries despite the greater relative importance of secure communication in general, and in the financial sector in particular.

That said, the environment is becoming more conducive, not least because of various instruments such as Innosuisse and others, for less speculative start-ups that have a less risky path to market but a correspondingly smaller market potential. Recent reforms of the tax code have also been beneficial for cash-strapped tech start-ups. There is already a growing number of successful start-ups within the field of quantum sensing and metrology (such as Qnami and Q-Zabre) as well as companies such as Zurich Instruments that provide essential key enabling technology solutions for the nascent quantum industry.

Under the auspices of the NCCR QSIT, initiatives such as the annual Quantum Industry Day, bringing the Swiss quantum start-up community together along with a growing number of international companies and organisations, serve to strengthen the ecosystem. By the same token, the qstarter award initiative encourages students to think in terms of applications for their research and potentially identify business opportunities. Both these initiatives serve to improve the quality of the quantum start-up ecosystem, making it more attractive for both domestic and international investors.

3.4 The link to industry

3.4.1 Biomedicine & chemistry

The chemical and biomedical sectors are generally perceived as being among the first sectors to be impacted by the advent of quantum computing for two reasons: First, their businesses are already critically dependent on high performance computing, and second, there are a number of highly relevant computational problems e.g. the modelling of molecular interaction and properties that have substantial commercial potential and that are expected to be within the capabilities of the first generations of quantum computers.[75] It typically takes over 10 years and millions of dollars for pharmaceutical companies to both discover a new drug and bring it to market. Quantum computing, by radically improving the precision of the simulation of larger molecules, has the potential to substantially reduce both the costs and time to market by accelerating the drug discovery process in the early stages.[76]

The chemical industry is likewise affected by the current limitations of classical computational chemistry. For example, if it were possible to accurately determine the reaction mechanisms in the process by which certain bacteria convert nitrogen in the air to ammonia, a key component in fertilisers, then one would be significantly closer to a substantially more energy and resource efficient replacement for the industrial Haber-Bosch nitrogen fixation process by which fertilisers are manufactured today.[77]

[75] See "The next decade in quantum computing and how to play", P. Gerberg and F. Ruess, Boston Consulting Group, November 2018. Retrieved from: https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play.aspx and "A Quantum Computing Use Case Roadmap from IBM". Retrieved from: https://quantumcomputingreport.com/our-take/a-quantum-computing-application-roadmap-from-ibm/.

[76] See https://www.accenture.com/us-en/success-biogen-quantum-computing-advance-drug-discovery.

[77] See Reiher et al. (2016).

Opportunities at the horizon

"Quantum technologies, and quantum computing in particular, offer many interesting opportunities for the pharma industry," says Nicholas Kelley, Data Science and A.I. Advisor for the Chief Digital Office at Novartis in Basel. "A variety of data science business problems involving modelling and simulation are potentially affected by future developments in quantum computing – publications in quantum chemistry can already be seen for example. But it remains difficult to predetermine when a quantum computer will offer a significant advantage over a classical approach. We need to better understand the problem categories that would be significantly enabled as the technology reaches the different stages of maturity. Therefore, the initial challenge is to identify specific scientific and business use cases which have the possibility to be mapped to suitable quantum algorithms. We are closely following the developments and would value potential opportunities to collaborate in the domain of quantum computing."

3.4.2 Finance & insurance sector

For the banking and finance sector, both quantum computing and quantum communication technologies are expected to have a significant impact on the industry, also in the short term. Given a sufficiently powerful quantum computer, at some point it will be possible to hack current encryption protocols and lay bare the communication networks underpinning the entire sector. On the other hand, quantum computing could enable banks to improve their investment and risk mitigation strategies. There are already a number of published studies that strongly indicate that quantum computing is likely to outperform classical methods of automated portfolio optimisation.[78] Financial institutions that are able to adapt to and leverage the capabilities of emerging quantum computing technologies faster than their competitors are more likely to develop a competitive advantage. This will enable them to offer more attractive portfolios and sell improved financial products to their customers.

However, quantum cryptography, a sub-field of quantum communication, already provides a solution to the security problem posed by quantum computing, both for public key encryption and even post-quantum encryption should that become necessary. Commercially available quantum key distribution systems can already provide 100% secure communication channels for financial data over metropolitan distances (10's of kilometres). Over time, faster systems with longer reach will serve to accelerate the adoption of this technology.

It is therefore important that the Swiss financial industry, in particular Swiss banks with global operations, starts to acquire knowledge and develop competencies regarding these two quantum technologies. Robust technology assessments of the potential impact of quantum technologies on their businesses are crucial to avoid the negative disruptive effects that quantum technologies are likely to have.

The technology assessments should also encompass blockchain and similar technologies in a quantum context. While blockchain is also susceptible to public key encryption hacking by quantum computers, quantum key distribution technology also has the potential to increase the security of blockchain by greatly reducing the probability of double-spending[79] or greatly enhancing the secure storage of crypto assets in general.[80]

[78] Alcázar, Leyton-Ortega, and Perdomo-Ortiz (2019).

[79] See "First Quantum-Securing Blockchain Technology tested in Moscow", MIT Technology Review, 2017. Retrieved from: https://www.technologyreview.com/s/608041/first-quantum-secured-blockchain-technology-tested-in-moscow/.

[80] See "Mt. Pelerin and ID Quantique team up for Quantum Vault". Retrieved from: https://www.startupticker.ch/en/news/june-2019/mt-pelerin-and-id-quantique-team-up-for-quantum-vault?utm_source=newsletter408&utm_medium=email&utm_campaign=newsletter408#.XPqv54RkmYI.email.

In terms of network infrastructure, the benefits of quantum-secure data channels will only become fully exploitable for globally operating banks once quantum secure channels can be established intercontinentally. Given the current state of quantum communication technologies, this will initially be implemented through QKD via satellites. It is, however, highly unlikely that individual companies will be able to put the necessary infrastructure in place by themselves at this point in time. This highlights the need for a coordinated effort within the industry in establishing quantum secure data networks with true global reach.

Insurance companies will not only benefit from improved computational tools for risk optimisation; they will also benefit from improved code verification of the software applications used to assess the insurance risk of their customers. Errors in these systems could be both significant and wide-ranging if not detected and rectified.

3.4.3 Metrology & precision industry

Metrology, the science of measurement, and the precision industry are critically dependent on the ability to accurately determine the value of physical parameters like mass, size, time, etc. and commercial success can often be referred back to this capability.

Quantum sensing, with the ability to perform even more precise measurement of physical parameters, is therefore crucially important for metrology. This greater precision is expected to have a direct impact on our capacity to understand nature and manipulate the environment we live in.

Advances in metrology in the form of quantum sensing have played a role in the recent redefinition of the SI base units (The International System of Units that forms the basis of the metric system) whereby as of May, 2019, all seven base units are defined with respect to fundamental physical constants. The kilogramme, for example, is now defined in terms of Planck’s constant and no longer by reference to an artefact standard. Quantum sensors will therefore enable ever more precise and decentralised embodiments of these standards – essentially democratising metrology standards – to the benefit of both science and industry.

The METAS – world-class Swiss metrology

While not generally known, Switzerland is home to one of the world’s leading competence centres in metrology. The Federal Institute of Metrology METAS in Bern-Wabern provides resources and services that enable it to perform tests and measurements in Switzerland at the level of accuracy required to meet the stringent needs of Swiss research, business and society. The METAS is also home to one of the most accurate atomic clocks, the Fontaine Continue Suisse FoCS-2, which contributes to the realisation of the International Atomic Time (TAI), and the institute has played – and continues to play – an important role in the internationally coordinated efforts to redefine the International System of Units (SI).

“Quantum sensors are likely to have a huge impact in many fields of technology in the future,” says Beat Jeckelmann, Chief Scientific Officer at METAS. “Their great advantage is that they are intrinsically accurate, because they measure things at the most fundamental level possible.” Asked for his assessment of Switzerland’s role in the realm of quantum sensing, Jeckelmann’s answer is clear: “Switzerland has a longstanding tradition in excellent quantum physics research and it has the potential to play an important role at the forefront of the second quantum revolution. Switzerland is well equipped with infrastructure. We have the essential facilities and the technological know-how that are needed to build quantum sensors. However, in order for technology transfer to be successful it is of crucial importance that we bring the right people together. We have to create a cross-disciplinary framework. This is not an easy task. But Switzerland definitely has a great potential to play a leading role in quantum sensing.”

The redefinition of the SI system, however, is only one of many examples where quantum sensors have led to fundamental changes in applications for which precision is paramount. We are already witnessing first applications of quantum sensors in fields like medical imaging, where they will significantly increase the accuracy and resolution of imaging techniques. This is likely to have a considerable impact on the accuracy and reliability of medical diagnoses. Highly accurate time measurements are mandatory in domains that rely on synchronising both individual signals as well as networks. Satellite navigation technologies like GPS are only the most obvious examples because of their ubiquity. But the same thing applies to electricity grids or the banking sector, where the reliable exchange of digital signals (both data and control signals) at very high bitrates is required.

With its long-standing tradition and success with precision manufacturing and microtechnology in the region of the Arc Jurassien, Switzerland has an additional strong competitive advantage when it comes to the development of quantum sensing technology. The Centre Suisse d'Electronique et de Microtechnique in Neuchâtel, founded in 1984 with the goal of consolidating and augmenting the country's strong position in microtechnology, is today actively involved in quantum technology development. Quantum technology is one of the CSEM's focus areas and it is particularly strong in the development of proprietary atomic vapor microelectromechanical cells. The CSEM is also acting as the coordinating institution for the EU Horizon 2020 macQsimal project designed to conduct research and development of advanced quantum sensors for measuring magnetic fields, time, rotation, electro-magnetic radiation and gas concentration.

Of all the quantum technologies, quantum sensing is the one that is most often portrayed as an extrapolation and/or augmentation of existing technologies in well-established applications and markets. This means that it has a broader appeal in terms of the number and diversity of industries for which it is of relevance and, by the same token, is easier to introduce and/or integrate into these industries.

The CSEM – microtechnology for Swiss industry

"The mission of the CSEM is to transfer world-class microtechnologies to industry," says Steve Lecomte, Head of the Time & Frequency Systems Section at the CSEM. "This is mainly done by enabling collaboration between academic and industry partners within Switzerland. Despite the excellent products that the Swiss precision industry has produced in the past, there are still many capabilities that are currently underexploited, in particular also in the field of quantum technologies. The CSEM is proud to play a leading role in the European macQsimal project, which brings many benefits for Switzerland. It would be great to have a similar consortium for quantum technology development within Switzerland to better foster collaboration among Swiss stakeholders."

3.4.4 Energy & telecommunication infrastructure

The secure transmission of data in a wide variety of networks is becoming extremely important as our world becomes increasingly digitalised. At the same time, there is a growing awareness of the implications for society in general and national security in particular if this security is breached. The rise of IoT (Internet of Things) and the spectre of losing control of critical infrastructure and physical assets only serves to make these implications more vivid and tangible.

Quantum technology plays an ambivalent role in the context of data and network security. On the one hand, the prospect of a quantum computer puts current encryption technologies at risk, as has been described in Chapter 1.1, since a quantum algorithm that can hack classical encryption keys in minutes has already been developed (Shor's algorithm). On the other hand, commercially available quantum cryptography solutions, in the form of QKD systems, can provide secure communication channels that can counteract the security threat posed by quantum computing. In addition, it is expected that these QKD systems will become faster and have longer reach. In ID Quantique, one of the world-leading providers of quantum cryptographic systems and with strong ties to academia in this domain, Switzerland looks to be ideally positioned to play a pioneering role in quantum cryptography. It is commonly recognised that establishing quantum readiness, i.e. preparing for the advent of the quantum computer and the impact it could have on one's business or industry, is also particularly important for the security of critical infrastructures such as energy or telecommunication systems. The growing tendency for such systems to become more and more interconnected in an Internet of Things just increases the relevance of having secure data channels.[81] However, there appears to be a lack of awareness in Switzerland of the relevance of quantum technologies for the security of critical infrastructures. The National Strategy for the Protection of Critical Infrastructures published by the Federal Council in 2017 does not address quantum technology in this context, neither as a threat to security nor as an asset for enhanced security. [82]

Aside from the relevance for data network security, quantum computing technology will also play a key role in the generation, transmission, and storage of electrical energy in the form of more efficient windmill wing profiles for the generation of electricity, new battery technologies for improved energy storage, and improved materials. Looking further into the future and arguably even more important, the underlying physics suggests that quantum computing will be more energy-efficient than classical computing, thus reducing the impact on climate of a field – cloud computing – whose energy consumption is growing at an unsustainable rate.

Establishing quantum readiness for Swiss infrastructures

"IoT consumer goods are currently not produced to be secure, but to be cheap. This is a problem," says Ronny Kaufmann, CEO of Swisspower AG, a strategic alliance of Swiss utility companies and innovation think tank for the Swiss energy sector. "In the near future, our energy system will be fully integrated with the IoT. This includes so-called operational technologies, i.e. the hardware and software components that monitor and control industrial equipment. A higher degree of system integration and network convergence obviously creates new vulnerabilities. At this point, however, the relevance of quantum technology for network security is not yet fully recognised, even though the energy sector traditionally has a high sensitivity for security issues. There seems to be little awareness for the importance of establishing quantum readiness. We would definitely be interested and ready to run a Swiss pilot project on quantum security for energy systems in collaboration with suitable partners."

Grégoire Ribordy, CEO of ID Quantique, sees many opportunities for Switzerland: "If the universal quantum computer becomes a reality, the impacts will be systemic. This is why we have to start preparing for the threats of the future now. We call this establishing 'quantum readiness'. ID Quantique is currently working with a South Korean partner on a major telecommunication network security project. In Switzerland, there is little activity when it comes to establishing quantum-safe networks for critical infrastructures and services. In a first step, this would require to make a quantum risk assessment, i.e. to find out which data channels are at high risk. At a later stage, it means establishing quantum readiness and to start deploying quantum safety when needed."

[81] See Richdale (2019).

[82] See https://www.babs.admin.ch/de/aufgabenbabs/ski/nationalestrategie.html.

3.4.5 Military security

Within the domain of military security, there is an ongoing, continuous effort to improve one's capabilities with respect to potential foes, whether that be defensive or offensive capabilities. This is often referred to as the arms-race where the objective is to stay ahead at all times.

All quantum technologies – computing, communication, and sensing – are of great importance and relevance for military security precisely because price often does take a back seat to performance in this context. The potential of quantum computing to perform calculations that will never be feasible or possible with classical computers – including hacking public-key encryption – have long been known to fall into this category. One area of immediate relevance is the verification and validation of the complex software code that is used to control and operate high-performance military assets and systems. By the same token, the potential of 100% secure communication channels enabled by quantum cryptography for long-range, high-speed communication is also of great importance and relevance for military security. Quantum sensing-based applications such as quantum imaging (providing enhanced visibility in bad lighting conditions, including the ability to see around corners) and quantum timing (enabling the ability to navigate autonomously without an operational satellite-based GPS infrastructure) are just two examples for a wide variety of such applications that are of great interest to military security and the defence industry.

For a small country like Switzerland, an economically viable defence industry is not feasible due to the small size of the domestic market. It also does not make sense for the Swiss army to engage broadly in technology development, since it would literally be impossible to compete in an arms-race with much larger international competitors (such as China or the United States). It is nevertheless important that the Swiss defence community establishes and maintains deep technological competence with respect to emerging defence technologies. Quantum technologies fall squarely into this category.

In Switzerland, the task of monitoring future defence technologies falls to the Science and Technology Section of armasuisse. Armasuisse S&T builds up its technology competence through a network of national and international partners as well as initiatives such as the establishment of the Cyber-Defence campus.[83] The presence of even a handful of Swiss companies that are actively involved with any such technologies can therefore be quite beneficial. This also applies to quantum technologies. Consequently, supporting and fostering an emerging quantum industry also has implications for national security since being able to access and keep technological know-how within national boarders at an early stage of development greatly facilitates the acquisition of technological competence for an institution like armasuisse S&T.

However, because many quantum technologies have civilian applications, a security perspective on quantum technology cannot just focus on issues of military security. As seen above, quantum technologies also have clear implications for the security of civilian infrastructures and cybersecurity. For a country like Switzerland, tackling the security issues that could potentially arise from future developments in quantum technology is therefore only likely to succeed if aspects of military security, civil security, technology policy and basic research are properly coordinated.

Procurement programmes for quantum technology could play an important role in this regard. The strong involvement of military funding agencies in quantum technology development in other countries (e.g. DARPA and IARPA in the United States) clearly shows that quantum technology is generally treated as a matter of national security. Some of these agencies are also actively supporting and collaborating with Swiss quantum companies, even if that support is not always visible.[84] There is a risk that Switzerland becomes dependent on foreign partners when it comes to security relevant quantum technologies. Although procurement does not play a significant role in Swiss technology policy, it appears highly feasible in this case due to the strong dual-use character of quantum technology and its relevance for various aspects of national security.

[83] See https://www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

[84] The yearlong collaboration of foreign intelligence agencies with Crypto AG, a Swiss company specialising in communications and information security, may serve as a cautionary example for the effects of foreign influence on security-relevant companies.

3.4.6 Overview of potentially affected sectors

The following table provides examples of relevant Swiss industry sectors that could be affected by future developments in quantum technology. It is important to note, however, that the applications mentioned in the table are currently at very different stages of maturity. Some of them are already commercially available, while others (in particular those related to quantum computing) are still at an early stage and it remains unclear when, how and if at all they will be employed as indicated. It is nevertheless important to raise awareness for the possibility of such applications.

Industry sector	Relevant domains	Examples of possible applications	Technology readiness level (high/medium/low)
Telecommunication infrastructure	Communication; sensing	Secure transfer of network signalling information and data; network synchronisation	High
Energy infrastructure	Computing; communication	Secure control of energy grid infrastructure; technologies for improved energy storage	High for communication; low for computing
Precision industry and advanced manufacturing	Sensing	Increased accuracy and resolution of imaging and various sensor technologies; ultra-precise timing and synchronisation of communication networks across a wide variety of industries and applications	High
Military and civilian security services	Computing; communication; sensing	Intelligence gathering; secure communications; new sensors for operations	High for communication; low for computing; medium for sensing
Finance and insurance	Computing; communication	Portfolio optimisation; secure transfer of data	High for communication; low for computing
Pharma and chemistry	Computing	Improved modelling for drug design; improved chemical processes	Low
Logistics	Computing	Process optimisation; optimisation of fleet management	Low

Table 3: Overview of potentially affected industry sectors.

4 Annex

4.1 Abbreviations & glossary

AI **Artificial intelligence**

Atomic and quantum clocks Ultra-precise clocks based on the precision of selected transition frequencies of atoms and ions, respectively.

Black swan event An event that is rare, has a high impact and is difficult to predict.

CDTs **Centres for doctoral training**

CEO **Chief executive officer**

Cryogenics The science of the production and behaviour of materials at extremely low-temperatures i.e. just above absolute zero.

CSEM **Swiss Center for Electronics and Microtechnology**

DARPA **Defence Advanced Research Projects Agency**

Decoherence The process by which the phase relationship (the coherence) between quantum states is degraded by external perturbations (noise) thereby adversely impacting the degree of superposition and entanglement.

Deep Tech Refers to companies that are based on scientific discoveries and/or engineering innovation and that typically require at least five years additional research and/or development prior to market launch.

Entangled photon sources A device that generates entangled photons, a key component in the quantum internet of the future.

Entanglement A quantum phenomenon whereby two or more quantum objects i.e. qubits are correlated such that the quantum state of each object cannot be described independently of the quantum state of the other objects.

EPF **École polytechnique féderale**

ETH **Eidgenössische Technische Hochschule**

EU **European Union**

FET **Future Emerging Technologies**

GPS **Global Positioning System**
A satellite-based navigation infrastructure predicated on ultra-precise timing signals.

HPC **High-performance computing**
The use of supercomputers and parallel processing techniques to solve complex computational problems.

IARPA **Intelligence Advanced Research Projects Agency**

ICs **Integrated circuits**
A collection of electronic circuits on a single (monolithic) piece of semiconductor, typically Silicon.

IDC **International Data Corporation**

Ion trap qubit A qubit using ions (charged atomic particles) suspended in free space in a magnetic field.

IoT **Internet of Things**

KTT **Knowledge and technology transfer**

Laser An extremely precise (in terms of frequency) and powerful (bright) source of light that made it possible to build the high data-capacity, worldwide telecommunication networks of today.

LEDs **Light emitting diodes**
Semi-conductor devices that are rapidly becoming the energy-efficient lighting technology of choice for many applications.

LIGO **Laser Interferometer Gravitational-Wave Observatory**

Magnetometer (alkali vapour) A device based on alkali vapours in glass cells and used to measure very weak magnetic fields.

Magnetometers (NV - nitrogen vacancy) A device based on nitrogen vacancy centres in a diamond lattice and used to measure very weak magnetic fields.

METAS **Federal Institute of Metrology**

ML **Machine learning**

MRI scanner **Magnetic resonance imaging scanner**
A device that can non-invasively image the interior of the human body for medical diagnostic purposes.

MSK **Mobile broadband communications**

NCCR **National centre of competence in research**

NISQ **Noisy intermediate-scale quantum**

NIST **National Institute of Standards and Technology**

NMR **Nuclear magnetic resonance spectroscopy**

NPL **National Physical Laboratory**

NRP **National Research Program**

NTN **National thematic network**

NWO **Netherlands Organisation for Scientific Research**

Optical fibres Flexible and transparent fibres made by drawing glass to a diameter corresponding to the thickness of a human hair.

OTPs **One-time-pads**
An encryption technique that has been proved to provide 100% security provided both sender and receiver use the same one-time, pre-shared key that is at least as long as the message to be sent.

Photon A “packet” (or quantum) of light.

Public key encryption
A type of cryptography based on two types of keys: one private and one public. It is the most ubiquitous form of cryptography today. Also known as “asymmetric cryptography”.

QAs
Quantum annealers
Machines that run the quantum equivalent of simulated annealing from classical computing.

QCI
Quantum communication infrastructure

QEC
Quantum error correction
Error correction code to protect quantum information from errors due to decoherence and other sources of quantum noise.

QI
Quantum internet
A quantum version of the current (classical) internet but with 100%-secure communication between all points and entities, protected by the laws of quantum physics.

QKD
Quantum key distribution
A 100%-secure communication method whereby two parties can produce a shared random key known only to them and upon which a cryptographic protocol (private key encryption) can be implemented.

QRNG
Quantum random number generator

QSs
Quantum simulators
The quantum equivalent of the early (classical) analogue computers based on analogue circuit elements.

Quantum advantage
The ability of quantum computers to solve problems that classical computers cannot practically solve. Also referred to as quantum supremacy.

Quantum imaging
The use of quantum phenomena such as entanglement to achieve increased resolution or functionality not possible with classical imaging techniques.

Quantum repeater
A device that makes it possible to transmit quantum information over long distances (of the order of 1000s of kilometres) through optical fibres.

Quantum supremacy
The ability of quantum computers to solve problems that cannot be solved practically by classical computers. Also referred to as quantum advantage.

Qubit
A concatenation of quantum bit. Qubits are the fundamental building blocks of every quantum computer. Unlike classical bits, a qubit can represent both 0 and 1 and everything in between due to superposition.

R&D
Research & Development

SDVN
Secure data network

Semiconductor materials
Materials – such as Silicon and Germanium – that only partially conduct electricity: not as well as metals (which do conduct electricity), not as badly as insulators (which do not conduct electricity).

SERI
State Secretariat for Education, Research and Innovation

SHD
Shared technology development

SI units
International System of Units
The seven units of measure defined by the International System of Units that form the basis of the metric system.

Simulated annealing
A (probabilistic) optimisation technique that mimics the annealing process in metallurgy to find an approximate global optimum in very large search spaces.

SMEs
Small and medium enterprises

SNSF
Swiss National Science Foundation

SQUIDs
Superconducting quantum interference devices
A very sensitive magnetometer based on superconducting circuits and used to measure very weak magnetic fields.

SSC
Swiss Science Council

Superconducting qubit
A qubit realised using superconducting electronic circuits, a well-established microscale technology.

Superconductors
Materials that conduct electricity with zero electrical resistance i.e. zero energy loss.

Superposition
A quantum phenomenon whereby a quantum system can be in multiple states simultaneously i.e. both 0 and 1 for qubits.

TA-Swiss
Foundation for Technology Assessment

TAI
International Atomic Time

Thermodynamics
The study of the thermal properties of materials.

TKI
Top Sector Alliance for Knowledge and Innovation

TNO
Netherlands Organisation for Applied Scientific Research

Topological qubit
A qubit that is based on quasi-particles which are expected to be intrinsically significantly more immune to decoherence and quantum noise than other qubit realisations.

Transistor
A (semi-conductor) device used to switch electronic signals and is the key building-block in integrated circuits.

TRLs
Technology readiness levels

TUD
Technical University of Delft

UASs	**Universities of applied sciences**
UCL	**University College London**
UK	**United Kingdom**
Unicorns	Privately-held start-up companies with a valuation in excess of 1 billion USD.
UQCs	**Universal quantum computers** A programmable, multi-purpose computer – the quantum equivalent of today’s classical digital computer.
US	**United States**
VC	**Venture capital** Private equity funding provided by funds or firms, typically for early-stage firms that are considered to have (or have demonstrated) high growth potential.

4.2 Bibliography

Alcázar, J. R., Leyton-Ortega, V., & Perdomo-Ortiz, A. (2019). Classical versus Quantum Models in Machine Learning: Insights from a Finance Application. *arXiv:1908.10778v1*.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., … & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510.

Baggott, J. (2011). *The Quantum Story: A History in 40 Moments.* Oxford: Oxford University Press.

Bernstein, D. J. (2009). Introduction to Post-Quantum Cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-Quantum Cryptography* (pp. 1–14). Berlin, Heidelberg: Springer.

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature, 549*(7671), 195–202.

Bornmann, L., Haunschild, R., Scheidsteger, T., & Ettl, C. (2019). *Quantum technology – a bibliometric analysis of a maturing research field*. Retrieved from https://figshare.com/articles/Quantum_technology_a_bibliometric_analysis_of_a_maturing_research_field/9731327.

Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics, 21*(6), 467–488.

Finnila, A. B., Gomez, M. A., Sebenik, C., Stenson, C., & Doll, J. D. (1994). Quantum annealing: A new method for minimizing multidimensional functions. *Chemical Physics Letters, 219*(5), 343–348.

Gibney, E. (2019a). Hello quantum world! Google publishes landmark quantum supremacy claim. *Nature, 574,* 461–462.

Gibney, E. (2019b). Quantum gold rush: the private funding pouring into quantum start-ups. *Nature, 574*, 22–24.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Paper presented at the *Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing,* Philadelphia, Pennsylvania, USA.

Heim, B., Rønnow, T. F., Isakov, S. V., & Troyer, M. (2015). Quantum versus classical annealing of Ising spin glasses. *Science, 348*(6231), 215 –217. doi:10.1126/science.aaa4170.

Kadowaki, T., & Nishimori, H. (1998). Quantum annealing in the transverse Ising model. *Physical Review E, 58*(5), 5355–5363.

MacFarlane, A. G. J., Dowling, J. P., & Milburn, G. J. (2003). Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 361*(1809), 1655–1674.

Popkin, G. (2017). China's quantum satellite achieves "spooky action" at record distance. *Science*.

Raymer, M. G., & Monroe, C. (2019). The US National Quantum Initiative. *Quantum Science and Technology, 4*(2).

Reiher, M., Wiebe, N., Svore, K. M., Wecker, D., & Troyer, M. (2016). Elucidating Reaction Mechanisms on Quantum Computers. *arXiv:1605.03590v2*.

Richdale, K. (2019). Why Quantum Technologies Matter in Critical Infrastructure and IoT. In Q. Ladetto (Ed.), *Defence Future Technologies: What we see on the horizon* (pp. 65– 67). Thun: armasuisse Science and Technology.

Shor, P. W. (1994). *Algorithms for quantum computation: discrete logarithms and factoring.* Paper presented at the Proceedings 35th Annual Symposium on Foundations of Computer Science.

Touzalin, A. de, Marcus, C., Heijman, F., Cirac, I., Murray, R., & Calarco, T. (2016). *Quantum Manifesto*. Retrieved from http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf.

Wilhelm, F. K., Steinwandt, R., Langenberg, B., Liebermann, P. J., Messinger, A., & Schuhmacher, P. K. (2019). *Status of quantum computer development*. Bonn, Germany: Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_1.pdf?__blob=publicationFile&v=5.

Impressum

Schweizerischer Wissenschaftsrat SWR
Einsteinstrasse 2
CH-3003 Bern
T +41 (0)58 463 00 48
F +41 (0)58 463 95 47
swr@swr.admin.ch
www.wissenschaftsrat.ch

ISBN 978-3-906113-64-7
Bern 2020

Lektorat: Doris Tranter, Stéphane Gillioz
Konzept und Design: Modulator AG, Branding + Design

Schweizerischer Wissenschaftsrat SWR
Einsteinstrasse 2
CH-3003 Bern

T +41 (0)58 463 00 48
F +41 (0)58 463 95 47
swr@swr.admin.ch
www.wissenschaftsrat.ch

←

Code scannen und
die digitale Version
herunterladen.