The Quantum What? Advantage, Utopia or Threat?

Michel Barbeau[1], Erwan Beurier[2], Joaquin Garcia-Alfaro[3], Randy Kuang[4], Marc-Oliver Pahl[5] and Dominique Pastor[6]
[1]Carleton University, [2,5,6]IMT Atlantique, [3]Institut Mines-Telecom, [4]Quantropi Inc.

Introduction

Quantum computing is at the top of the agenda for several countries. They acknowledge its strategic importance. They invest significant public funds in the development of this technology. While some show unconditional enthusiasm, others are more moderate and even very critical with respect to the promises of quantum computing. It is not easy to navigate for a non-expert in the field. Does quantum computing have a real advantage or is it rather a utopia? Is quantum computing a threat to cybersecurity? With a non-expert point of view, this article sheds light on these questions. We consider quantum computing as an advantage, a utopia, or a security threat. We look at applications that we think are promising. We review the efforts made by participants engaged in the race for the quantum computer. Finally, we project ourselves into the future.

An Advantage?

In the 1980s, Richard Feynman suggested using the properties of quantum physics to compute chemical interactions at the molecular scales. In the 1990s, the interest in quantum computing increased significantly thanks to Shor's algorithm (Shor 1994). With this algorithm, a quantum computer can rapidly solve a large class of cryptology problems. Standard asymmetric encryption methods used to protect communications can potentially become highly vulnerable. The so-called quantum advantage or quantum supremacy refer to the ability of quantum computers to solve complex problems much faster than classical computers (Preskill 2012). Shor's algorithm is the best-known example Another contribution of importance is Grover's algorithm. In an unsorted list of items, it speeds up the search for a specific element. It is an elementary operation that can accelerate several programs. Furthermore, the quantum advantage may refer to conducting operations that have no analogue in classical computing, e.g., merging multiple quantum states into one of higher quality (Leone et al. 2021).

Some believe that a genuine quantum computer with 50 qubits would achieve quantum supremacy. Some estimations increase that number to, at least, hundreds of qubits (Choi 2020, Dalzell et al. 2020). Computers with such a high number of qubits could achieve computations requiring several thousands of years on today's fastest supercomputer.

Quantum computing is a complex technology. Quantum computers of intermediate size, composed of only a few physical qubits have already been developed by IBM, Google, and Rigetti. They are limited. The realization of a universal quantum computer that can achieve any type of quantum calculation and outperforming any current supercomputer is not expected before 2030.

A Utopia?

Not everyone shares the optimism about quantum computing. It is making extraordinary claims. Extraordinary claims require extraordinary evidence. According to (Dyakonov 2018, 2020), a useful quantum computer requires between 1,000 to 100,000 qubits. Current quantum computers are extremely vulnerable to errors that happen due to noise or manufacturing imperfections. This challenge is not clearly tackled. The quantum threshold theorem states that physical error rates below a certain level can logically be solved using error-correction algorithms. As often in mathematics, this theorem relies on several assumptions that seem unrealistic because they need to be exactly verified. Entanglement – the inherent connection of different qubits - makes the effect of errors even worse than in traditional computing today. An error in a qubit implies a cascade of other errors in related qubits. To counter the noise effects, error-correcting codes are required at the lowest level of the computer. The issue is then that achieving efficient error-correcting codes becomes more difficult as the number of qubits increases.

Shor's algorithm is one of the reasons why there is interest in quantum computing. The initial integer factorization algorithm requires a tremendous number of quantum gates, around 72n3 to factorize an n-bit number. And yet, most of the companies that claim to have realized a quantum computer use it as a test of their computing capabilities. Actually, they use a compiled version of the algorithm that drastically reduces the number of gates by knowing the factorization to compute. One could see this as plain cheating. Thus, even if quantum computing is a promising technology, it seems mainly driven by optimism. Dyakonov argues that, albeit solid technological attempts, the quantum computing fervor is nearing its end; much energy and money were put into it for little results so far. But there is hope: recent research dramatically improved the number of qubits required for integer factorization (Gidney and Ekerå 2021).

The development of a quantum computer is extremely challenging. It requires overcoming several technical issues. The realization of two qubits with the same nominal behavior requires a high level of reproducibility of several physicochemical parameters because we want those multiple runs of the same program output the same results. The current mass production technologies are insufficient to guarantee such a reproducibility for a high qubit volume.

Qubits interact with their environment. Superposition of qubit states eventually disappears. This unavoidable phenomenon is called decoherence. The decoherence time is crucial to control. It represents the time during which we can benefit from the superposition of the two possible states of a qubit to achieve several computations at the same time.

The efficiency of quantum computers relies on their ability to use few qubits to deal with large amounts of data. Unfortunately, there is currently no known method to efficiently transcribe a large set of data into a single quantum state. For problems involving large amounts of data, the initialization of a quantum computer becomes dominating in time over the computation. This significantly reduces the quantum advantage.

Clearly, these challenges are of different nature. Overcoming them will require cooperation between various fields of expertise, such as computer science, complexity theory, quantum physics, mathematics, systems engineering, process engineering, and materials. Such a cross-fertilization may be difficult to setup. On the one hand, we have physicists who are motivated by scientific knowledge, discovery, and experimentation. On the other hand, we find computer scientists and electronic engineers who reckon that technical achievements are possible without full knowledge of the underlying physics and who, therefore, may underestimate and even neglect fundamental issues of importance.

A Security Threat?

Shor recently raised awareness about complacency over Internet security (Castelvecchi 2020). The strength of Diffie-Hellman and Elliptic Curve Cryptography relies on the discrete-logarithm problem. The security of Rivest, Shamir and Adleman (RSA) depends on the problem of factoring large numbers. Due to recent advances in quantum computing, the security of classical Public Key Infrastructure (PKI) is at risk. Shor‘s algorithm provides an exponential speedup in breaking it. In 2019, Google declared quantum supremacy with their Sycamore 54-qubit quantum computer (Arute 2019). In 2020, Wang et al. made a milestone on prime factorization with the D-Wave annealing quantum computer (Wang et al. 2020). They successfully factorized into prime numbers all numbers up to 10 000. D-Wave paves the way to a new cracking strategy for PKI. It may be closer to cracking practical RSA than a general-purpose quantum computer running Shor's algorithm. The commercial availability of quantum computers, especially the quantum annealers, shakes the foundations of contemporary information security.

Applications

One of the first applications of the quantum technology is its use to secure classical data. Leveraging the laws of quantum physics, Bennett and Brassard proposed the Quantum Key Distribution (QKD) protocol (Benn 84). QKD has been widely explored resulting in a variety of implementations and improvements (Giampouris 2017). Despite its name, QKD is in fact a key expansion protocol. Its operation relies on a companion authenticated classical channel. It is not a complete solution, a barrier to its adoption. Other barriers include the need for special hardware. It cannot run over the classical Internet. Furthermore, although theoretically secure, QKD is vulnerable to several practical attacks (National Security Agency 2020).

Machine learning is another application of quantum computing whose interest is growing (Biamonte et al. 2017). Phenomena unique to the quantum level, such as entanglement, could make quantum computers learn things that classical computer cannot. Another potential advantage is to make the time complexity of classification independent of the number of data points. Quantum machine learning is a situation where large amounts of data are involved. The setup and initialization of quantum machine learning are preponderant in time over the computation, thus reducing the quantum advantage. Quantum machine learning is promising but requires further research.

Quantum-resistant routing is another positive outcome of the quantum challenge. It has inspired researchers into modeling new threats against the quantum Internet (Kimble 2008, Wehner et al. 2018). The main goal is to achieve secure and sustainable quantum repeaters (Satoh et al. 2020). Classical information-oriented attacks, such as those compromising confidentiality, seem to have less of a hold over quantum information. The non-cloning theorem of quantum mechanics reframes secrecy related issues.

The Quantum Race

We make a world tour of initiatives and investments in quantum computing. The Quantum Manifesto prompted European states to establish a strategy to maintain Europe at the forefront (Collective 2016). This was deemed crucial to avoid dependence on a single technological path that could result from a concentration of expertise in China and USA. Quantum computing became a priority for the European Union (EU) with an advanced strategy and funding scheme. The EU invested 550 M€ in quantum computing research from 1997 to 2017. The EU started a Future and Emerging Technologies action on quantum communication, sensing, computers, and simulators.

The roadmap is having QKD in systems for inter and intra-city communication in 2023. The goal is to achieve by 2027 quantum Internet links across distances longer than 1000 kms. By 2023, they aim to achieve quantum computers with error correction outperforming physical qubits, and in 2027 quantum algorithms outperforming classical computers. For quantum simulation, the objective is to achieve by 2027 a quantum advantage in solving important problems in science, demonstrate quantum optimization, and realize prototype solving problems beyond supercomputer capability, for application domains such as quantum chemistry, new material design. The roadmap for quantum sensing and metrology is, for 2023, integrated quantum sensors, imaging systems and metrology standards at the prototype level; and in 2027 transition from prototypes to commercially available devices. In October 2018, the European Commission launched the Quantum Technologies Flagship with a 1 B€ budget for ten years to support the transformation of research into commercial applications exploiting the potential of quantum technologies.

In parallel, EU countries set up their own initiatives. France aims to acquire a general-purpose quantum computer. In 2021, France launched the Quantum Plan and announced a public-private investment of 1.8 B€ in quantum technology, over five years (Frésillon 2021, Gouvernement Français 2021), with public investments of 200 M€ per year leading to the creation of three interdisciplinary quantum information institutes (Le Monde 2021). The strategy builds upon public-private sector partnerships, flagship research regions, and training with new graduate programs. Startups are supported, which is another strategy to increase technological advance. There are seven focus areas. Their monetary attributions in parenthesis give an idea of the prioritization: i) developing and disseminating the use of Noisy Intermediate Scale Quantum (NISQ) simulators and accelerators (352 M€), ii) developing the Large Scale Quantum computer (432 M€), iii) developing quantum sensor technologies and applications (258 M€), iv) developing the post-quantum cryptography offer (156 M€), v) developing quantum communication systems (325 M€), vi) developing a competitive enabling technology offering (292 M€), and vii) structuring the ecosystem across the board.

As emphasized in (Forteza et al. 2020), to anticipate the advent of quantum computing and benefit completely from this technology once it is mature, a challenge is to disseminate its use and practice and, more generally, to teach quantum computing in priority sectors, such as chemistry, logistics, artificial intelligence, pharmacology, materials, fertilizers, catalysts, and logistics finance. Several French companies are investing in the field. For instance, Électricité de France (EDF) and Total set up programs dedicated to quantum computing in collaboration with the startup Pasqal, specialized in programmable quantum simulators and quantum computers composed of 2D and 3D atomic arrays.

The Atos company program reflects the strategies of involved companies. Launched in 2016, it aims to make available the benefits of the already existing NISQ technology. In particular, the Atos Quantum Learning Machine provides a simulation environment for developers, training, build use cases and assess quantum implementation benefits. Atos collaborates with national players such as Grand Equipement National de Calcul, the Commissariat à l'Energie Atomique and Pasqal. It is desirable that other private stakeholders emerge to help anticipate the possible breakthrough and advent of quantum technologies in an open and highly competitive economy.

In the vein of recommendations in (Forteza et al. 2020), the emergence of other European competitors will help avoid too much dependence of Europe on a single private partner. In addition, in a market economy, companies face challenges and adopt strategies that do not always align with the governmental ones. They may fluctuate according to market developments. This challenges the ability of countries to protect their scientific and technological heritage as well their advances achieved through public financial support.

Germany invests 100 M€ per year in quantum computing, with an overall funding of 650 M€ between 2018 and 2022 (Bundesministeriums für Bildung und Forschung 2018, 2021). In 2021, a further investment of 1.1 M€ had been announced. Germany favors four directions: quantum computers, quantum communication, quantum-based measurement technology, and enabling technologies for quantum systems. The focus is on developing the quantum technology research landscape, creating research networks for new applications, flagship projects with the industry, sovereignty, international collaboration, and getting the commitment of the population. Showing the importance of the strategy, the research organizations involved in the enacting of the plan include all major German actors such as German Research Foundation, Max Planck society, Fraunhofer society, Helmholtz Association, Leibniz Association, National Meterology Institute, Federal Office for Information Security, and Agency for Innovation in Cybersecurity.

In 2013, the United Kingdom (UK) was the first European country to announce a quantum strategy, investing 370 M€ over five years and creating in 2018, a national center aimed at developing a quantum computer. In June 2019, UK announced an additional £153 M investment on quantum, together with a £205 M commitment from industry. In early 2020, the Netherlands announced that about 23.5 M€ will be invested in quantum technologies over the next five years. Quantum technologies in Spain are being promoted by public-private partnerships, including large multinational companies such as Telefónica (telecommunications) and Hispasat (satellites), research centers such as Institute of Photonic Sciences and Spanish National Research Council, and start-up initiatives such as Quside, Multiverse Computing, and Qilimanjaro Quantum Tech. Investment plans are expected to grow from 20 M€, for the period 2015-

2017, to 400 M€, for the period 2021-2027. An aim is to promote quantum solutions in financial, pharmaceutical, automotive, and aeronautical sectors (Ametic 2019).

In the USA, coordination of quantum research started in October 2014. Since 2018, research and development in this area is a national priority by the National Quantum Initiative Act. The plan is to inject $1.2M in development of quantum information systems over the next decade (INRIA 2020). Over five years, $625M will be invested in five research centers across the country. Furthermore, the USA private sector and academia are contributing an additional $340M to these research centers.

The Big Tech are at the forefront in the soaring of quantum computing in the USA, with especially Google, IBM and Microsoft leading the way by striving to make the technology emerge via tremendous investments in it. Ultimately, big-data, artificial intelligence and quantum computing are to meet for such companies to maintain their leadership in the digital world. Google has been developing its own quantum computer and announced in August 2020 that its computer Sycamore had performed the first-ever quantum simulation of a chemical reaction. At the same time, IBM claimed that its quantum computer handled 64 qubits. Microsoft is developing technology on topological quantum computing and has developed its own open-source quantum programming language Q#. Behind the Big Tech, it is worth mentioning the existence of companies such as the Canadian D-Wave with a new generation of quantum computer and the American startup Rigetti, which announced in August 2020 that it had raised $79M to support the development of a 128-qubit computer.

While it has invested over $1B over the last decade (National Research Council Canada 2017), Canada has announced a $360M budget over seven years, starting in 2021, to support its National Quantum Strategy (Department of Finance Canada 2021). It emphasizes training of qualified personnel and development of job opportunities in the area. Historic strengths of Canada are cryptography, Information and Communications Technology (ICT) and photonics.

China is quickly catching up with the construction of a $10B national laboratory dedicated to quantum information science. China‘s leading quantum research group announced in December 2020 that their computer Jiuzhang attained the quantum supremacy (Conover 2020, Zhong et al. 2020), with a computation that took 200 seconds whereas the world fastest non-quantum computer would have needed 600 million years to achieve the same result. China is thus the second country achieving quantum supremacy, after the USA with Google’s Sycamore (Conover 2019). This achievement is of prime importance. The technology is based on photons, a technology that seemingly received less attention than others, whereas Sycamore relies on superconducting materials conducting energy without resistance and not light.

The private Chinese company Alibaba launched in 2015 its Quantum Computing Laboratory aimed at producing a prototype of a general-purpose quantum computer involving 50 to 100 qubits by 2030. The company has also invested $15B in artificial intelligence and quantum research. In 2018, the search engine Baidu announced the creation of the Institute of Quantum Computing. Tencent set up a lab dedicated to scientific research in quantum computing.

An Obstacle Race

From a very general point of view, two main issues could slow down the successful realization of private and public plans. A first issue is the lack of skills in the quantum computing job market. This may affect the dissemination, use and practice of quantum practice. In contrast to machine learning, the number of computer engineers and scientists familiar with quantum computation is very limited. It is necessary to significantly increase the skills of engineers and scientits in quantum computing to speed up its diffusion.

A second issue for Western countries is their dependence on the most advanced producers of semiconductors. Specifically, qubits out of silicon are among the most robust available (Gonzalez-Zalba et al. 2019, Petit et al. 2020). This allows for maintaining a sufficiently long decoherence time to benefit from superposition and thus parallelization. The development of silicon-based quantum computers could furthermore leverage the previous infrastructure investments in microchip technology to maintain low-level production costs. The ambition of many countries is to explore the silicon path by relying on their strong research and industrial experience in microelectronics, as well as the pertaining industrial facilities. Semiconductors have thus become the new oil in a global economy dominated by the tensions between China and the USA. For several months now, we have been aware of a shortage of semiconductors already affecting the video game, automotive, communication industries, among others. Since the European semiconductors industry has dropped significantly over the last ten years to end up with merely 10% of the market share, we easily understand why the EU aims to boost Europe‘s position in the semiconductor market. If the chip war continues and intensifies, it may jeopardize programs and schedules established by governments and industries.

Conclusion

Countries invest in quantum computing to maintain their technological advance. One may not expect the race to result into a definite winner, but rather to maintain a technological advancement equilibrium across leading countries. We are facing a very risky technology that opens many uses, some possibly yet unthinkable because new algorithms will emerge from current and future research. Nobody can reasonably predict how quantum technology will evolve.

Various aspects of the quantum technology have already proved to be feasible. For more than twenty years, researchers and industrialists have come up with realistic methodological plans, achieved findings with potential high impacts, and succeeded in elaborating the very first generations of quantum computers and sensors. The literature on the topic shows that researchers and industrialists are capable of continuously adapting to deal with unforeseen issues. On the other hand, the same literature puts forward that the technology is ambitious, with the potential to have a high scientific, technological, economical, and even societal impact. For sure, quantum technology entails much uncertainty and unpredictability. Quantum technology is a high-risk high-gain technology. The issue is thus not whether researchers and industry will be able to provide various technological bricks or not. They will! Even in case of failures, the amount of work achieved will provide --- and has already opened --- new research paths that contribute to the classical technology of computers communications and cybersecurity.

Quantum computing is an incentive to classical computer science. As mentioned by Chao-Yang Lu who co-authored (Zhong et al. 2020) “It’s a continuous competition between constantly improved quantum hardware and constantly improved classical simulation” (IQT News 2020). For example, very rapidly after Google announced that its quantum computer Sycamore had reached quantum supremacy, IBM claimed to have developed a supercomputer capable of simulating the 54-qubit Sycamore circuits and performing the same tasks.

Above all the technical advances in quantum computing, the main issue remains political. There is a short list of stakeholders that are strong enough to support a sufficiently long-term investment in this high-risk, high-gain technology. As in martingale pricing, such will probably get the expected significant return on their investment. In this respect, we currently have two types of major stakeholders. On the one hand, two countries are noticeably key players, namely, China and the USA. These countries keep on funding research and application of quantum computing, simply because it is well accepted that the country that will lose the race for innovation will fall. On the other hand, we have industrial stakeholders, that include Google and Microsoft, two of the GAFAM, as well as Alibaba, Baidu and Tencent, three of the BATX. Among the major stakeholders in quantum computing, we find data rich countries and leaders in artificial intelligence. Otherwise said, big data, artificial intelligence and quantum technologies are poised to meet each other and merge. Major players in artificial intelligence invest tremendous amounts of money in quantum technology, positioning them ipso facto as leaders of the digital world. For instance, Microsoft is fully playing the game of the high-risk high-gain technology. It is one of the few players addressing topological quantum technology. This technology is in its infancy. The feasibility of topological qubits is not demonstrated yet. However, Microsoft Station Q is a research group fully dedicated to this field. Topological quantum computing is expected to be more stable and robust to noise than standard quantum computing.

Where do we go from here?

For countries, research institutions and industrials other than the unrivalled few, what can be done to avoid becoming digital colonies of two main leaders of the digital world? There is probably no other choice than continuing research on the topic for mainly political reasons. Indeed, it is crucial for countries to keep some independence, at least on niches that may provide prominent advantage on some aspects and trigger further cooperation.

The sanitary crisis put forward the importance of supporting research in pharmacology, biology, and personalized therapy. A - perhaps too simple - point of view could be that research in such areas should prevail at the expense of quantum computing. However, quantum computing is expected to help model chemical reactions at the molecular scale, thus making possible the study of interactions between proteins and medicine. So, instead of choosing between pharmacology, biology and quantum computing, a possible way involves combining them. If we cannot win the race and become leaders on quantum computing, we can still become key stakeholders on topics requiring hybridization of two or more research areas including some specific aspects of quantum computing. Hybridization and interdisciplinary research seem unavoidable, simply because quantum computers are not aimed at replacing standard computers or supercomputers. The quantum computer is akin to a co-processor, tailored to speed up specified computations such as simulations in meteorology or the prediction of a protein folding. Albeit highly desirable, hybridization and interdisciplinary advancement will depend on our research and industrial tissues and organizations. International cooperation is beneficial to attain the critical mass required to play this high-risk, high-gain game. International cooperation is strongly conditioned by our ability to smooth out respective ways to handle and support research, development, and innovations.

It is worth emphasizing that sustainability and ecological issues are poorly addressed in the literature on the topic. What is the carbon footprint of research in quantum computing? Can we expect that this technology, once it is mature, render our world more sustainable thanks to its capacity to carry out computations that would otherwise consume our planet? For Pan Jianwei, one of Jiuzhang’s designers, the answer is clear since he deems that Jiuzhang discovery means a gain in computing capacity without an increase in energy consumption, in contrast to supercomputers, which are very energy intensive.

If the quantum technology holds its promises, we can expect decisive advantages in chemical and physical simulations that should induce applications with high impact in agriculture, drug discovery and battery design. It could contribute significantly to environmental preservation by reducing the energy footprint of fertilizer production, leading to substantial savings and helping reduce the ecological impact of the food industry.

This technology may also allow speed-ups in optimization and machine learning applications, including finance, energy, automotive, traffic improvement, environmental sciences, actions against global warming, with possibly new processes for efficient CO2 recycling, or even the identification of early warning signs of natural disasters with quantum sensors embedded in satellites.

Several researchers, engineers and scientists highly involved in this technology reckon that it could potentially affect every aspect of our everyday life. Great! But current quantum computers are devoted to very specific tasks of relatively poor practical interest with respect to the expectations. The general-purpose quantum computer is not for tomorrow.

What will be the environmental price integrated over all these years before the technology is mature, deployed and meets all the expectations? Once the technology reaches maturity, will we not be tempted to carry out even more calculations to the point where the possible gain in sustainability brought by quantum computing could finally be cancelled out? The way is long, but the camel is patient and watchful. What is your opinion? Is Quantum Computing a utopia, an advantage, or a threat?