Quantum Computing: What should we know?

Leandro Maglianella, Leen Salah, Maram Abdallah, Rahma Ellisy and Shahnoor Dara
Kingston University

1. Introduction

Within the past decade, the world has been experiencing massive technological developments and breakthroughs especially within the quantum realm. This has allowed us to conduct more research and learn more about the world around us. It also raises a lot of ethical, social, legal and economic concerns. However, it caused undeniable scientific and technical changes. This report will be exploring the field of quantum computing, how it came about and the future it holds.

2. What is quantum computing?

Circuit chips in computers are made of several components, each with their own unique function. One of the deep components of circuits are transistors which nowadays can be the size of 14nm which is 500 times smaller than a red blood cell (Kurzgesagt – In a Nutshell, 2015, 0:54). A transistor is an electric switch that allows electrons information called bits to come through. Bits are identified as either 0 or 1. Combinations of bits allow to create larger and more complex information.

In classical computers, bits are the smallest units of information. Quantum computers use another set of bits called qubits which carry superposition of 0, 1 and all what is in between at the same time (*How Do Quantum Computers Work?*, no date). This difference allows quantum computers to process significantly more data and information. It is found in many field such as medicine, financial strategies and algorithms.

3. The history and origin of quantum computing

Quantum computing can be traced as far back as 1980, when Paul Benioff outlined a "Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines", it explained that the logic behind quantum computing lies in various complex demanding tasks in today's world that normal computers cannot handle. Richard Feynman thought about using quantum computing to show and simulate quantum physics. Feynman states that a complex simulation of nature must be made through quantum mechanics, since the problem is complex and requires deep thinking (Montanaro, 2015).

One of the precursors to quantum computing was conjugate coding, which is a pre-requisite cryptographic tool, invented by Columbia University professor Stephen Wiesner in the late 1960 (Wiesner, 1983). David Deutsch proposed a quantum Turing machine to model quantum computing in 1985 (Montanaro, 2015). In 1992, Deutsch and Richard Josza explained that the problem in question is solved with guarantee in much less time by quantum computation than with normal classical methods of computation. This would later be proven in 1993 when Ethan Bernstein and Umesh Vazirani demonstrate quantum computers are more rapid in processing and efficient than classical computers.

4. Advantages and disadvantages of quantum computing

There are various advantages to why quantum computing could be chosen over a normal computing system. It has the power to solve many more problems that a normal computer system is not capable of doing because quantum computers are more efficient. Google claimed that it was able to solve a problem that would have taken them 10,000 years in just seconds (CNBC, 2019). In the medical sector, it is used in the learning of the specific activities of proteins and the search for new drugs by algorithms (Parsons, D F. 2011). This will help the development of drugs which will help improve the healthcare industry. Researchers are also exploring its uses to help combat climate change. For example, they are developing systems to route taxis in Beijing. It will basically be able to "send a command to a particular taxicab to take an alternate route with the goal of sort of smoothing out the traffic" (Mcleod, J. 2018). This will help reduce carbon dioxide emissions as cars are going to be taking shorter and easier routes that will help them stay off the roads. Quantum computing will also be used for encryption purposes which means more protection from hackers and secure their systems.

Quantum computing is still at its development period so it's hard to predict the full extent of its drawbacks however, that means many problems will still arise as it is a very new concept. Quantum computers will be very expensive to get hold of meaning not everyone will be able to get them especially small companies which can affect the growth of their businesses. One of the main issues is that once people get hold of quantum computing, normal computers will become very vulnerable (Sohail, H. 2019), which means protection on private files kept on normal computers won't be as secure anymore. Quantum computers will not be able to reach their full potential and may still be very similar to normal computers until there is enough algorithms written to solve a wide range of problems when used.

5. Internet security work

One of the concerns that came about with the rise of technology has been security and it is still important today as it was decades ago. The security of encryption is quantified in terms of "bits of security". This gives an easier method of algorithm comparison when looking at algorithms with differing characteristics. 2,128 computational iterations are required for an attacker to decode a 3,072-bit RSA key, a 128-bit AES key, and a 256-bit elliptic curve key. Every one of these methods of encryption provides 128 bits of security (considering that a classical computer was being used) (Martin, no date). The easiest way in which an attacker would be able to break a code is by trying all possible variations till one of them works. Conventional computers have reached a point where they can do this, but it is not as easy as it sounds. An example would be the collective effort of 300,000 people for more than four and a half years to break through key known as 64-bit AES in 2002 (Martin, no date). Even the world's fastest supercomputer would need up to a trillion years to find the right key. Having an AES-256 algorithm would mean that you have a sufficient level of security against any threats of quantum computers.

6. Present and Future of quantum computing

Nowadays many companies, Google and IBM among the most known, are investing huge amounts of money (billions of pounds) in development teams that work and research with the aim of designing a functioning quantum computer with higher capacity than a classic supercomputer. The existence

of a quantum computer with this characteristic implies that we can possibly reach the so-called “quantum supremacy". Currently, IBM has succeeded in producing a computer with a 50-qubit design called “IBM Q” while Google has created a 54-qubit one called “Sycamore” and a 72-qubit quantum processor called “Bristlecone” (Hossenfelder, 2019). Google recently announced in an article published in the scientific journal “Nature” that they have achieved quantum supremacy thanks to “Sycamore”, a statement not verified with total support by the scientific community (Porter, 2019).

Furthermore, these technologies produced so far do not still appear to be sufficient, they are able to carry out some tasks with a very high efficiency but are not yet completely error-free (Fan, 2019). Quantum computers are very delicate and currently need to operate at a temperature close to zero degrees Kelvin as well as being isolated from noises and electromagnetic interference. The process of the creation of Qubit need to occur at very low temperatures, close to zero but colder than the temperature of a vacuumed space. Quantum computers have dilution refrigerators (IBM, no date) which preserved the temperature for the qubits by creating a very cold environment out of more than 2,000 components. The complexity and the rate of errors increase exponentially to a corresponding linear increase in the number of qubits of the computer architecture. It makes sense that these constraints make quantum computers very expensive and not suitable for large-scale retail trade.

It is still not clear whether the quantum computers will ever be able to completely replace the classic computers, in fact they are not able to work as a standalone device but need a programmed and monitored computer to function (Hossenfelder, 2019). For the foreseeable future, we imagine that we will continue to use classic computers that will interact with quantum computers only to complete particularly complex tasks.

7. Conclusion

With regards to the advantages and disadvantages of quantum computing, it seems to have a significant impact on our society and our everyday lives. It will not be a surprise if it develops even further especially as technological progresses through time. This technological sensation has allowed more opportunities in several research areas and will not be stopping anytime soon. It is and will continue to be one of the major and prominent ways to develop our understating of the world in the upcoming years.

References

- Benioff, P. (1980) *Journal of Statistical Physics*, pp. 563-564 Available at: https://doi.org/10.1007/BF01011339 (Accessed: 14 November 2019).

- Bonsor, K. and Strickland, J. (no date) *How Quantum Computers Work.* Available at: https://computer.howstuffworks.com/quantum-computer1.htm (Accessed: 11 November 2019).

- Childs, A. (2009) *Universal Computation by Quantum Walk*. doi: 10.1103/PhysRevLett.102.180501 (Accessed: 14 November 2019).

- CNBC (2019) *Google claims its quantum computer solved a 10,000-year problem in seconds*. Available at: https://www.cnbc.com/2019/10/23/google-claims-successful-test-of-its-quantum-computer.html (Accessed: 21 November 2019).

- Fan, S. (2019) *Quantum Computing, Now and in the (Not Too Distant) Future.* Available at: https://singularityhub.com/2019/02/26/quantum-computing-now-and-in-the-not-too-distant-future/ (Accessed: 11 November 2019).

- Hossenfelder, S. (2019) *Quantum supremacy is coming. It won't change the world.* Available at: https://www.theguardian.com/technology/2019/aug/02/quantum-supremacy-computers (Accessed: 11 November 2019).

- *How Do Quantum Computers Work?* (no date). Available at: https://www.sciencealert.com/quantum-computers (Accessed: 11 November 2019).

- IBM (no date) *What is quantum computing?* Available at: https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/ (Accessed: 11 November 2019).

- Kurzgesagt – In a Nutshell (2015) *Quantum Computers Explained – Limits of Human Technology*. Available at: https://www.youtube.com/watch?v=JhHMJCUmq28 (Accessed: 11 November 2019).

- Martin, L. (no date) *Is quantum computing the end of security as we know it?* Available at: https://techbeacon.com/security/quantum-computing-end-security-we-know-it (Accessed: 24 October 2019).

- Mcleod, J. (2018) *D-Wave's quantum computers 'can save energy, solve climate change*. Available at: https://business.financialpost.com/technology/d-waves-quantum-computers-can-save-energy-solve-climate-change (Accessed: 21 November 2019).

- Montanaro, A. (2015*) The past, present, and future history of quantum computing.* Available at: https://people.maths.bris.ac.uk/~csxam/teaching/history.pdf (Accessed: 14 November 2019).

- Parsons, D F. (2011) *Possible Medical and Biomedical Uses of Quantum Computing*, Medical Sciences--Psychiatry And Neurology, 9(3), p599. Available at: https://search-proquest-com.ezproxy.kingston.ac.uk/docview/1724505003?accountid=14557 (Accessed: 21 November 2019).

- Porter, J. (2019) *Google confirms 'quantum supremacy' breakthrough.* Available at: https://www.theverge.com/2019/10/23/20928294/google-quantum-supremacy-sycamore-computer-qubit-milestone (Accessed: 11 November 2019).

- Sohail, H. (2019) *Quantum Computing: Pros and cons of quantum computing*. Available at: https://techmazia.com/quantum-computing-latest-pros-and-cons/ (Accessed: 21 November 2019).

- Wiesner, S. (1983) *Conjugate Coding*. Available at: http://delivery.acm.org/10.1145/1010000/1008920/p78-wiesner.pdf?ip=141.241.26.20&id=1008920&acc=ACTIVE%20SERVICE&key=BF07A2EE685417C5%2EF2F1A3FD390199EA%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1574330610_1233ba4838d801d3d04bea346936fad5 (Accessed: 14 November 2019).