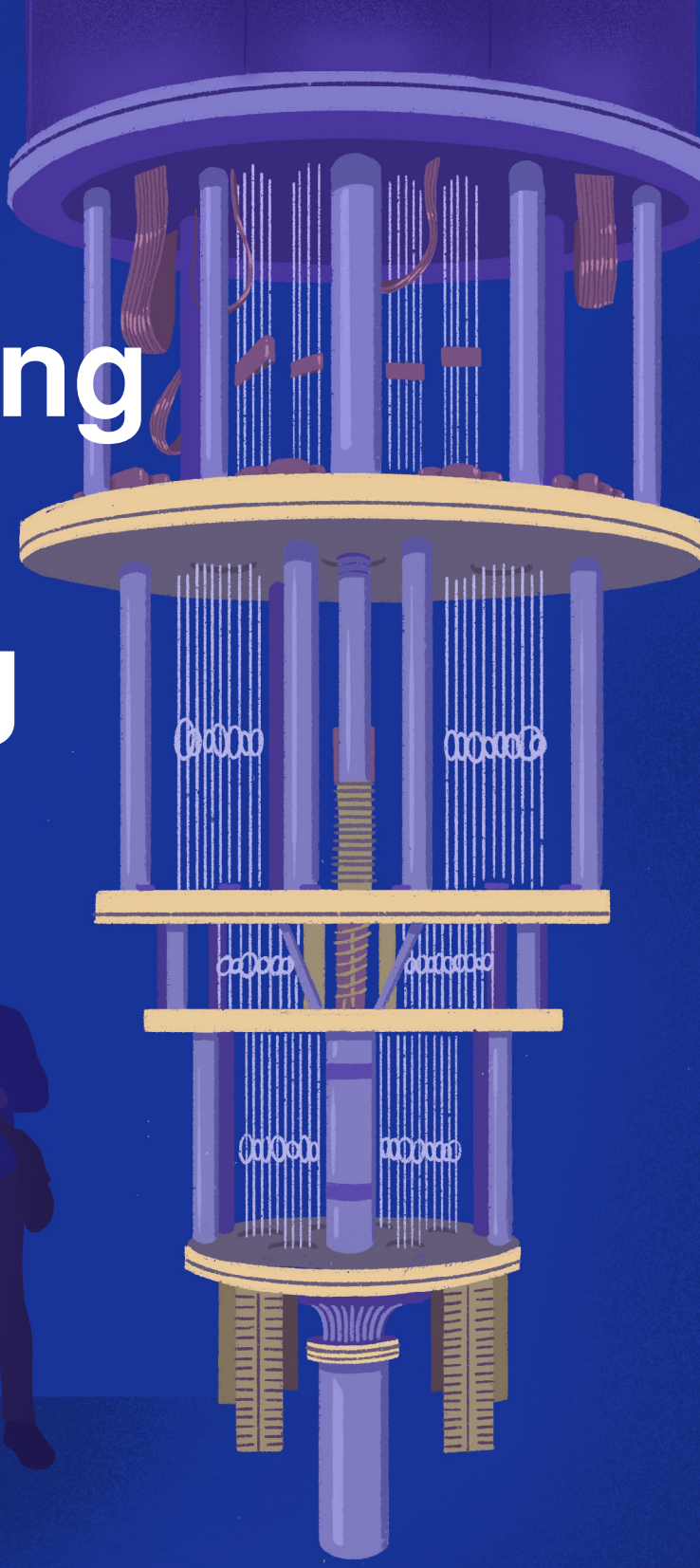
Demystifying Quantum Computing

for the Humanitarian Sector



DH Network
Digital Humanitarian Network

Dec 2019

Licensing Information

Demystifying Quantum Computing

For the Humanitarian Sector

by

Stephanie Tran (stephanie.tran@mail.utoronto.ca | stephanietran.ca)
Munk School of Global Affairs and Public Policy, University of Toronto

Andrej Verity (verity@un.org I @andrejverity)
Office for the Coordination of Humanitarian Affairs (OCHA)
United Nations

Design

Ignacio G. Rebollo (gimenez-rebollo@un.org I igrebollo.com)
Office for the Coordination of Humanitarian Affairs (OCHA), United Nations
M.Des. Ontario College of Arts and Design University (OCAD U)

This document was made possible
with the support of

OCHA

Table of Contents

Key Messages

- It is best to avoid the hype surrounding quantum computers as there remains much uncertainty of when a practical, large-scale, error-corrected quantum computer will be developed - or if such a feat will ever be achieved.

- Quantum computers are fundamentally different from the computers that are widely used today. Quantum computers process information differently as they operate using quantum mechanics.

- Although basic quantum computers have been built, there has reportedly been only one specific calculation that a quantum computer has completed better than a classical computer.

- There is no guarantee of when, or if we will ever, achieve a practical quantum computer as they are incredibly difficult to build and interact with. There are significant technical barriers that still need to be overcome before practical quantum computers become a reality.

- There are only a few tasks that large scale quantum computers are expected to perform significantly better than a classical computer. This includes the ability to break today's most widely implemented encryption schemes; solving optimization/large search problems; and simulating chemical systems.

- Humanitarian organizations should make efforts now to ensure that confidential data with long-term security obligations is secure against adversaries with access to a large-scale quantum computer.

- The arrival of large-scale quantum computers have the potential to exacerbate several issues that exist today. As STEM teams continues to demonstrate a lack of diversity across gender and other measures, there is concern over the implications of shared unconscious biases within homogeneous research and development teams.

- Since quantum computer development requires massive investment, there are questions regarding how much more of an advantage giant companies will have over smaller companies.

- National security may become implicated once an entity gains access to a large-scale quantum computer that can break today's widely-used cryptosystems.

Interviewees

This report is informed by a review of publicly available resources as well as interviews with professionals and researchers in the field of quantum computing and technology.

Thank you very much to all who generously provided their time and expertise.

Meredith Broussard	Arthur L. Carter Institute at New York University
Dr. Shohini Ghose	Department of Physics & Computer Science at Wilfrid Laurier University
Ronald de Wolf	Institute for Logic, Language and Computation at the University of Amsterdam

Special thanks to the team at IBM research including Jurij Paraszczak, Michael Jacobs, Chris Nay, Alexis Harrison, and David Raper.

Introduction

There is much excitement around the emergence of quantum computers. The field of quantum computing has seen significant private sector investment while countries have invested billions of dollars into quantum research and development programs.[1] Despite great investment efforts, today's quantum computers are still very far from the level of development that is needed to perform any groundbreaking operations. This document is intended to demystify quantum computing so that humanitarian workers and beyond can realistically understand and plan for its potential emergence. Since the technology is still early in its development, this publication is meant as a primer to quantum computing in today's context as opposed to a purely speculative investigation on its potential implications to humanitarian work.

What becomes clear when evaluating the potential implications of a world with large-scale, practical quantum computers is that our socioeconomic and geopolitical climate are not separate, but rather entwined, in both the development and potential use of quantum computers

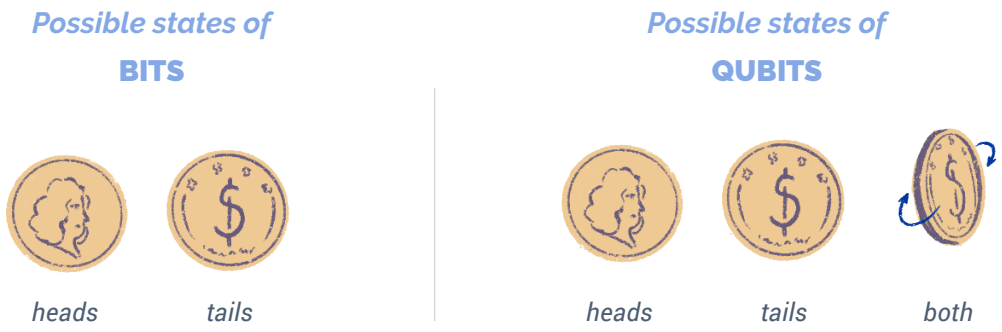
1 *Lardinois, Frederic. "UK Government Invests $194M to Commercialize Quantum Computing." TechCrunch. TechCrunch, June 13, 2019. https://techcrunch.com/2019/06/13/uk-government-invests-194m-to-commercialize-quantum-computing/.*

Avoiding the Hype

Emerging digital technologies have the capacity to dramatically alter the way that we work. What is efficient, effective, and impossible today may not be so tomorrow. It is in the interest of organizations across all sectors to evaluate future threats and opportunities and to strategize accordingly. However, when it comes to speculating on an uncertain future, especially with regards to emerging technologies, it is important that we maintain a reasonable perspective informed by evidence and full awareness of the limitations of technologies.[2]

According to interviews and reviewed literature, quantum computing is in an early development phase. Because a practical quantum computer has yet to be built, the discussions in this paper on the possible applications and impacts are speculative. It is important for decision makers to avoid the hype when it comes to emerging technologies including quantum computing.

Figure 1:



2 For a complete discussion on the downfalls of overly optimistic views on technology, refer to Meredith Broussard's book, Artificial Unintelligence (2018).

Demystifying Quantum Computers

01. They are different

A quantum computer is a new type of computer that works differently from the computers that we use today. Today's conventional computers are considered to be classical computers.[3] In classical computers, the basic unit of information processing is the bit. A bit can only be one of two states: 0 or 1. Classical computers process information using bits.

Quantum computers are different as they process information differently by using quantum physics. Instead of bits, quantum computers use **qubits** (short for quantum bits) as their basic unit of information. While bits can only be one of two states (0 or 1), qubits are able to represent states in a nonbinary way. Qubits can be in the state of 0, 1, or even both zero and one at the same time "with some probability of being zero and some probability of being one".[4] This combination of being both 0 and 1 at the same time is an instance of **superposition**: a quantum property that refers to a combination of states that we would normally describe independently from one another.[5] You can think about it like two piano keys being pressed at the same time: the resulting sound that you hear is a superposition of two musical notes.[6]

Another way to understand the difference between bits and qubits is to imagine them as coins (see figure 1). Bits can be only one of two states, similar to how a flipped coin can be either heads or tails. Qubits can also be found as one of either state, but they can also be both basis states at the same

3 Preskill, John. "Quantum Computing in the NISQ era and beyond". Quantum. 2: 79. (2018) doi:10.22331/q-2018-08-06-79, 2.

4 Ghose, Shohini, "A beginner's guide to quantum computing," 2018, TED video, 10:05, https://www.ted.com/talks/shohini_ghose_quantum_computing_explained_in_10_minutes.

5 IBM Q, "What is quantum computing?" Accessed July 22, 2019. https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/.

6 It is important to note that a "quantum computer (despite a qubit being '0 and 1 at the same time') is not equivalent to a classical exponentially-parallel computer" (de Wolf, 2019)

time through superposition.[7] Imagining qubits as coins, they can be found as either heads, tails, or both at the same time as represented by a spinning coin.

By harnessing superposition along with other quantum mechanical properties, quantum computers fundamentally process data differently from classical computers. Scientists have demonstrated that in theory this new way of information processing can lead to much faster performance compared to that of classical computers today.[8]

02. There is no guarantee when we'll see practical quantum computers - or if we ever will

"Because quantum computing technology is so different from the information technology we use now, we have only a very limited ability to glimpse its future applications, or to project when these applications will come to fruition. While this uncertainty fuels optimism, our optimism should be tempered with caution."

- Theoretical physicist John Preskill ("Quantum Computing in the NISQ era and beyond", 2018)

Building and working with quantum computers is very difficult as quantum systems are very sensitive.[9] Qubits are incredibly fragile, with some requiring temperatures that are 250 times colder than deep space in order to remain stable.[10] Vibrations, electromagnetic waves, temperature changes and other interactions with the outside environment can cause qubits to lose their quantum state, or to decohere.[11] As of today, scientists have built "very simple" quantum computers that can perform a

---

7 Alber, Gernot, et al. Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments (Berlin, Heidelberg: Springer Berlin Heidelberg, 2001), 60.

8 McMahon, D. Quantum Computing Explained. John Wiley & Sons. 2018.

9 Preskill, John. "Quantum Computing in the NISQ era and beyond". 4.

10 Greenemeier, Larry. "How Close Are We-Really-to Building a Quantum Computer?" Scientific American. Scientific American, May 30, 2018. https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/

11 Alber, Gernot, Thomas Beth, Michał Horodecki, Paweł Horodecki, Ryszard Horodecki, Martin Rötteler, Harald Weinfurter, Reinhard Werner, Anton Zeilinger. Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments (Berlin, Heidelberg: Springer Berlin Heidelberg, 2001), 31; Institute for Quantum Computing . "Quantum Computing 101." Institute for Quantum Computing. University of Waterloo, June 14, 2019. https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101.

few operations, but there remains a significant amount of work to be done in order to achieve the goal of building a practical, scalable quantum computer capable of logical computation.[12]

Last year, the US National Academies of Science, Engineering and Medicine assembled a committee to produce a report exploring the current state of quantum computing. Consisting of 13 quantum computing experts including the head of Google's quantum-hardware efforts, the committee decided not to commit themselves to any estimates of when practical quantum computers will emerge because "significant technical barriers remain before a practical quantum computer can be achieved, and there is no guarantee that they will be overcome."[13]

03. Only one quantum computer has reportedly performed a computational task better than a classical one

We are said to be approaching the era of quantum supremacy (also known as quantum superiority) when a quantum computer can perform tasks that ordinary digital computers are unable to.[14] At the time of this publication, Google has reported that their Sycamore quantum processor is able to execute a specific algorithm that would take a state-of-the-art classical supercomputer approximately 10,000 years to perform.[15] However, this achievement is a contentious one as IBM has refuted Google's claim. IBM contends that the threshold for quantum supremacy has not been met, arguing that "an ideal simulation of the same task can be performed on a classical system in 2.5 days".[16]

---

12 National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. xii, 15.

13 National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects, 5. Schneider, David. "Full Page Reload." IEEE Spectrum: Technology, Engineering, and Science News. December 05, 2018. Accessed August 1, 2019. https://spectrum.ieee.org/tech-talk/computing/hardware/the-us-national-academies-reports-on-the-prospects-for-quantum-computing.

14 Preskill, John. "Quantum computing and the entanglement frontier." arXiv preprint arXiv:1203.5813 (2012), 1.

15 Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019) doi:10.1038/s41586-019-1666-5.

16 Pednault, Edwin, John Gunnels, Dmitri Maslov, and Jay Gambetta. "On 'Quantum Supremacy.'" IBM Research Blog. IBM , November 7, 2019. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/.

04. Quantum computers won't be better at everything

Scientists have proven that there are many instances where a quantum computer would be no better in performance than classical computers.[17] The list of computational problems that a quantum computer can solve significantly faster than a classical computer is actually quite small. Here are some key areas where scientists see large-scale quantum computers making a big impact:

A / **Cryptography**

To ensure that unauthorized people do not see our confidential information online, most of our online communications, e-commerce activities, and more are disguised using **cryptographic algorithms**: sets of rules that are used to obfuscate or reveal messages.[18] Doing this means anyone who tries to intercept such communications will be unable to see the actual contents of the communication. If an interceptor were to try to reveal the message's contents (also known as decrypting), they would have to solve a large mathematical problem that today's computers cannot solve.[19]

One of the well-known possible applications of a large scale quantum computer is factoring large numbers and solving other hard-to-compute questions. This is significant as our most widely-used methods of encryption rely on the fact that problems such as factoring very large numbers is too difficult a problem for classical computers to solve. A large quantum computer will greatly reduce the amount of work needed to decrypt "almost all internet traffic and stored encrypted data".[20] A

---

17 de Wolf, Ronald. "The potential impact of quantum computers on society." Ethics and Information Technology 19, no. 4 (2017): 272.

18 Piper, Fred and Sean Murphy, 'Understanding cryptography' in Cryptography: A Very Short Introduction (Oxford, 2002; online edn, Very Short Introductions online, Sept. 2013), doi: 10.1093/actrade/9780192803153.001.0001, accessed 08 Aug. 2019, 8.

19 Ghose, Shohini (Professor of Physics and Computer Science, Wilfrid Laurier University), interview with author. New York, 11 June 2019.

20 National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196. (2019). 8.

sufficiently powerful quantum computer can force us to change our approaches in securing our digital communications and data.[21]

B / **Optimization**

Another set of problems that scientists view quantum computers being potentially useful for is optimization or large search problems. Optimization problems typically require finding the best solution among a set of solutions.[22] For example, questions like finding the shortest route between two points on a map or searching through large data files are optimization problems. Searching through big data efficiently, especially unsorted data, is a huge challenge across industries including finance, environment, healthcare and more. Scientists believe that quantum computers would be able to solve large search or optimization problems at significantly faster speeds than classical computers.[23]

There are quantum algorithms that scientists know can search through unsorted data better than any known classical computer algorithms.[24] Moreover, quantum computers can speed up machine learning in some cases. After being given some data, machine learning algorithms work to find a well-fitting or optimally fitting model based on the patterns found in the data. This is an optimization problem that quantum computers may be able to solve better or faster than classical computers.[25] However, such a process is technologically very demanding and will likely not be realized soon.

C / **Analyzing and designing drugs**

Quantum computers are likely to make an impact in drug design and analysis in two ways:

Creating simulations of atoms_ Essentially, drug development involves designing or finding molecules with specific desirable properties.[26] One approach for curing diseases would be to look at

---

21 Chen, Lily, et al. Report on Post-Quantum Cryptography. Gaithersburg: National Institute of Standards and Technology, 2016. Accessed 1 August, 2019. http://dx.doi.org/10.6028/NIST.IR.8105.

22 Ghose, Shohini, interview with the author. June 2019

23 de Wolf, 273.

24 Ghose, Shohini, June 2019.

25 de Wolf, 273.

26 Ibid, 274; Ghose, June 2019.

diseases on the quantum level and then to create or find a molecule that could target it. Figuring out the properties of such molecules is very challenging from a computational perspective. Accurately simulating individual atoms requires a lot of computing time and memory on classical computers. In contrast, scientists say that quantum computers can, in principle, simulate the behavior of quantum systems much more efficiently. This could be advantageous in the field of drug development and health care as quantum computers could help chemists more quickly identify the properties of specific molecules, in turn supporting their work in discovering drugs for treating diseases.

Search optimization_ When looking for drugs to treat specific diseases, chemists basically search through massive databases of possible molecules that have a desired behavior.[27] As large-scale quantum computers are likely to solve large search problems faster, this process may become more efficient in the future.

05. Quantum computers won't replace traditional computers

Quantum computers are currently being designed as special-purpose devices that operate alongside classical computers.[28] Considering this, it is unlikely that quantum computers will replace classical computers entirely, especially in the consumer market.

Besides practicality, there are enormous financial and practical barriers to building and possessing a quantum computer. It is certain that it will initially be exceedingly expensive to build even one medium-sized quantum computer.[29]

27 Ibid.

28 The National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. Grumbling, Emily; Horowitz, Mark (eds.). Washington, DC: National Academies Press. (2019) doi:10.17226/25196, 5.

29 de Wolf, 275.

How might quantum computers impact humanitarian work?

"To me it seems very safe to say that [quantum computing] won't be relevant for humanitarian applications for at least the next 5-10 years."[30]

- Ronald de Wolf, theoretical computer scientist

Although quantum computers are expected to be applied in areas like drug design, optimization, and cryptography, such applications (especially optimization and cryptography) will require very large quantum computers. Thus it may be too early to speculate about the ways that applications such as improved drug design processes and searches can benefit humanitarian work.

However, organizations with data that they hope to remain secret for the next two decades and beyond should already start addressing the potential security threats that large-scale quantum computers can potentially present.[31]

30 de Wolf, Ronald, email to author, 10 June 2019.

31 Emerging Technology from the ArXiv. "How a Quantum Computer Could Break 2048-bit RSA Encryption in 8 Hours." MIT Technology Review. May 30, 2019. Accessed August 1, 2019. https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.

Communications and Data Protection

"Companies and governments cannot afford to have their now-private communications decrypted in the future, even if that future is 30 years away. For this reason, there is a need to begin the transition to post-quantum cryptography as soon as possible, especially since it takes over a decade to make existing Web standards obsolete"

- National Academies of Sciences, Engineering, and Medicine, Quantum Computing: Progress and Prospects (2018)

It is recommended that, even before large quantum computers are finally developed, efforts should be made to ensure that confidential data with long-term security obligations are **quantum secure**: secure against adversaries with access to a large-scale quantum computer.[32] Governments, militaries, health care organizations and other organizations tend to handle **sensitive data**: "data that is likely to lead to harm when exposed".[33] This data may still be considered sensitive in 20 years time. As data remains a critical component of humanitarian response, it is important for the humanitarian community to prepare their information security systems for a possible quantum future. At the same time, it is important to note that a committee of quantum experts have shared their doubts that a quantum computer will be built within the next decade that is capable of compromising our widely used cryptosystems.[34]

Active research is being undertaken around the world to address the information security issues in a

32 The National Academies of Sciences, Engineering, and Medicine, 97; Stewart, Duncan. "Quantum Computers: The next Supercomputers, but Not the next Laptops." Deloitte Insights. December 11, 2018. Accessed August 1, 2019. https://www2.deloitte.com/insights/us/en/industry/technology/technology-media-and-telecom-predictions/quantum-computing-supremacy.html.

33 The Centre for Humanitarian Data. "Working Draft of the OCHA Data Responsibility Guidelines." OCHA. March 2019. Accessed August 1, 2019. https://centre.humdata.org/introducing-the-working-draft-of-the-ocha-data-responsibility-guidelines/.

34 The National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. Grumbling, (2019). 9.

quantum future, including efforts to develop and test quantum-resistant technologies.[35] Since 2016, the US National Institute of Standards and Technology (NIST) has been in the process to select and standardize replacement cryptography methods that are expected to be quantum secure. There already exists cryptographic algorithms (such as lattice-based cryptography) that are believed to be quantum secure and are currently being evaluated by NIST.[36]

What humanitarian organizations can do now

NIST advises that, "As the replacements for currently standardized public key algorithms are not yet ready, a focus on maintaining crypto agility is imperative."[37] **Crypto agility** is the capacity to quickly replace cryptographic algorithms for more secure ones as they gain approval by NIST.[38] It is recommended that organizations remain up to date on these developments and to have roadmaps to follow these recommendations prepared.

35 *Chen, Lily, et al. Report on Post-Quantum Cryptography. 2.*

36 *For more on lattice-based cryptography refer to: https://www.research.ibm.com/5-in-5/lattice-cryptography/*

37 *Chen, Lily, et al. Report on Post-Quantum Cryptography. 7.*

38 *Stewart, Duncan. "Quantum Computers: The next Supercomputers, but Not the next Laptops."*

Wider Concerns: Beyond the scope of humanitarianism

Just like all other technologies, quantum computers are not being developed in a vacuum. The technology has the potential to both impart influence, and be influenced by, the wider sociopolitical context that it operates in. As such, large-scale quantum computers aren't going to just introduce new issues, but may exacerbate problems that already exist today. The following are questions shared by several quantum physicists and technology ethicists on the speculative implications of a world with large-scale, fault-tolerant quantum computers.

Implications of a lack of diversity

> ***"Maximizing the catalytic role of STEM requires drawing on the widest pool of talent to promote excellence and leaving out women is a loss for all."***
>
> - UNESCO, Cracking the code: girls' and women's education in science, technology, engineering and mathematics (STEM). United Nations Educational, Scientific and Cultural Organization, 2017. 15.

Quantum computing theory and devices requires contributions of many fields including chemistry, physics, computer science, mathematics and more.[39] As men have widely outnumbered women in science and engineering employment and training historically, some concerns arise on how the lack of diversity may impact things like decisionmaking around quantum computing and development of its technologies.

A 2017 publication by UNESCO found that only 28% of the world's researchers in STEM were women.[40] Globally, female students represent only 35% of students enrolled in STEM-related fields within higher education. Gender diversity (as well as demographic diversity including

39 The National Academies of Sciences, Engineering, and Medicine, 182; Ghose, Shohini, June 2019.

40 UNESCO, Cracking the code: girls' and women's education in science, technology, engineering and mathematics (STEM). United Nations Educational, Scientific and Cultural Organization, 2017.

ethnicity, age, class, sexuality and more) in research teams "has the potential to drive scientific discovery and innovation".[41] For example, American researchers paid more focus on women's health issues as more American women entered medical research in the 1980s and 1990s.[42]

Several concerns thus arise regarding the implications of having largely homogenous teams producing research and work regarding quantum computing. What kinds of questions and possibilities are not being considered due to shared unconscious biases? Social groups tend to share collective blind spots.[43] These blind spots are evident in cases where, for instance, HP programmers' unconscious bias resulted in their face-tracking webcams being unable to recognize dark-skinned faces.[44] If the fields contributing to quantum computing research continues to represent a select few demographics, the breadth of perspectives driving knowledge production subsequently remains lacking. As stated by UNESCO (2017), "From a scientific perspective, the inclusion of women promotes scientific excellence and boosts the quality of STEM outcomes, as diverse perspectives aggregate creativity, reduce potential biases, and promote more robust knowledge and solutions".[45]

Ensuring women and girls attain equal access to STEM education and careers is not only imperative from a scientific perspective, but also from a development one.[46] According to UNESCO, "gender inequalities in STEM education and employment perpetuate existing gender inequalities in status and income."[47] In the case of the future of quantum computing, gender equality (as well as equality among races, classes, nationalities, etc.) in STEM education and employment could help ensure that

---

41 Nielsen, Mathias Wullum, Carter Walter Bloch & Londa Schiebinger, Making gender diversity work for scientific discovery and innovation. Nature Human Behaviour 2, 726–734 (2018) doi: https://doi.org/10.1038/s41562-018-0433-1. 732.

42 Gewin, Virginia. "Why Diversity Helps to Produce Stronger Research." Nature News. November 13, 2018. Accessed August 4, 2019. https://www.nature.com/articles/d41586-018-07415-9.

43 Broussard, Meredith. Artificial Unintelligence: How Computers Misunderstand the World. Cambridge, MA: MIT Press, 2018, 28; Broussard, Meredith (Professor of Data Journalism, New York University), interview with author. New York, 11 June 2019.

44 Broussard, Meredith. Artificial Unintelligence: How Computers Misunderstand the World. 157.

45 UNESCO, Cracking the code: girls' and women's education in science, technology, engineering and mathematics (STEM). 15.

46 Ibid.

47 Ibid.

men and women are able to gain the skills and opportunities to contribute to and benefit equally from advances in quantum computing.

Who will benefit? Efficiency gains for big companies

Publicly available information indicates that the current big players in quantum computing development are major companies including IBM, Microsoft and Google.[48] As quantum computing development requires massive investment, currently entrenched giant companies are not as likely to face disruption by competition from small companies like we have seen in classical computing.[49] Consequently, if quantum computers bring efficiency gains, it may be possible that only a handful of big companies get to enjoy such gains, possibly contributing to more unequal power and wealth distribution between the few large corporations and the rest of society, but as well as between America and the rest of the world.

This concern is exacerbated by these companies patenting ideas and subsequently reducing the open flow of information.[50] This could lead to already large businesses dominating or monopolizing commercial quantum computing. Aside from market inequalities, the hoarding of knowledge can also impact the rate of overall development of quantum computing. As there is increased global competition for leadership in quantum computing between nation-states and private sector entities, there is some worry that this competition "could drive the field to be less open in publishing and sharing research results".[51] Progress in the field of quantum computing may occur more slowly if research results are kept proprietary or secret.

48 *Ghose, Shohini, June 2019.*

49 *de Wolf, 275.*

50 *Ibid.*

51 *The National Academies of Sciences, Engineering, and Medicine, 186-7.*

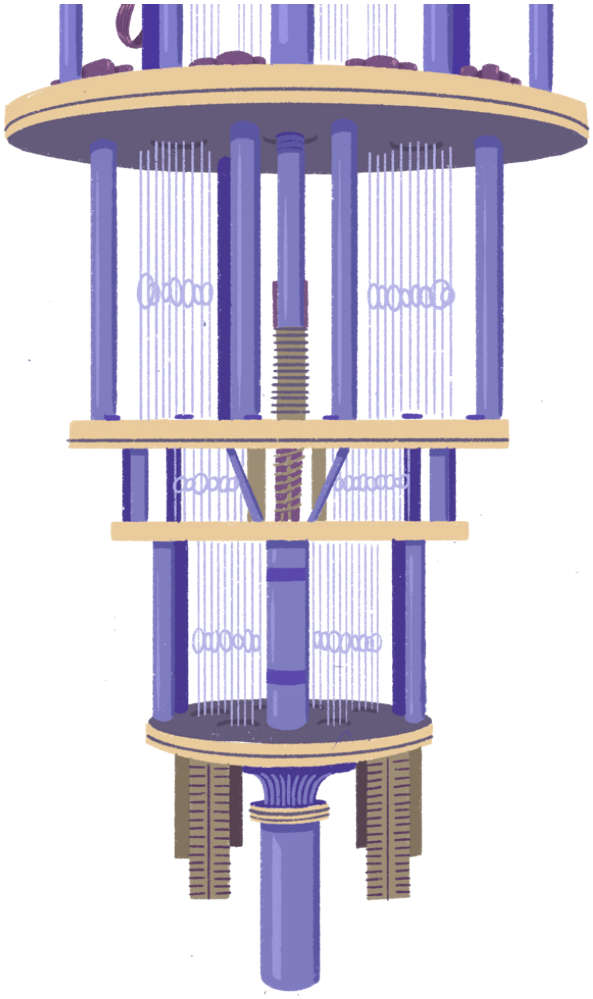
National Security and civilians

Quantum computing has clear implications for national security since an entity could gain significant intelligence advantage once they have a large-scale, practical computer that could break today's asymmetric cryptosystems. Indeed, a state's pre-quantum encrypted data could be significantly beneficial to foriegn intelligence operations.

Moreover, since quantum computers likely won't be as accessible as today's digital computers, a great imbalance may arise in terms of whose information gets to remain private and whose privacy will be breached. One scenario could be a large nation-state obtaining access to the data of activists or other actors who are targeted politically. This could include sensitive medical data or past messages sent through communication channels such as email or instant messages.

Conclusion

Quantum computers are fundamentally different from the digital computers that we know of today. Although their potential applications bear substantial implications across sectors, quantum computers have yet to reach the size and capability needed to perform such tasks. In essence, quantum computers are incredibly difficult to make and use. Around the world, researchers from the fields of chemistry, physics, computer science and more continue to search for answers to a wide array of questions that surround quantum systems and the adjustments that will need to be made in a post-quantum world. As for now, humanitarian organizations and beyond should be prepared to adopt new, standardized and quantum-secure cryptographic methods once they arise.



Annex I: Works Cited

Arute, F., Arya, K., Babbush, R. et al. *Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019) doi:10.1038/s41586-019-1666-5.* **Bernhardt, Chris.** *Quantum Computing for Everyone. Cambridge: MIT Press, 2019.*

Broussard, Meredith. *Artificial Unintelligence: How Computers Misunderstand the World. Cambridge, MA: MIT Press, 2018, 47.*

Broussard, Meredith *(Professor of Data Journalism, New York University), interview with author. New York, 11 June 2019.*

Chen, Lily, et al. *Report on Post-Quantum Cryptography. Gaithersburg: National Institute of Standards and Technology, 2016. Accessed 1 August, 2019. http://dx.doi.org/10.6028/NIST.IR.8105.*

de Wolf, Ronald. *2017. The potential impact of quantum computers on society. Ethics and Information Technology 19, (4) (12): 272.*

de Wolf, Ronald, *email message to author, 6 June 2019.*

de Wolf, Ronald, *email message to author, 14 August 2019.*

Emerging Technology from the ArXiv. *"How a Quantum Computer Could Break 2048-bit RSA Encryption in 8 Hours." MIT Technology Review. May 30, 2019. Accessed August 1, 2019. https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/.*

Alber, Gernot, Thomas Beth, Michał Horodecki, Paweł Horodecki, Ryszard Horodecki, Martin Rötteler, Harald Weinfurter, Reinhard Werner, Anton Zeilinger. *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments (Berlin, Heidelberg: Springer Berlin Heidelberg, 2001).*

Gewin, Virginia. *"Why Diversity Helps to Produce Stronger Research." Nature News. November 13, 2018. Accessed August 4, 2019. https://www.nature.com/articles/d41586-018-07415-9.*

Ghose, Shohini, *"A beginner's guide to quantum computing," 2018, TED video, 10:05, https://www.ted.com/talks/shohini_ghose_quantum_computing_explained_in_10_minutes.*

Ghose, Shohini. *(Professor of Physics and Computer Science, Wilfrid Laurier University), interview with author. New York, 11 June 2019.*

Greenemeier, Larry. *"How Close Are We-Really-to Building a Quantum Computer?" Scientific American. Scientific American, May 30, 2018. https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/.*

IBM Q, *"What is quantum computing?" Accessed July 22, 2019. https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/.*

Institute for Quantum Computing. *"Quantum Computing 101." Institute for Quantum Computing. University of Waterloo, June 14, 2019. https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101.*

Lardinois, Frederic. *"UK Government Invests $194M to Commercialize Quantum Computing." TechCrunch. TechCrunch, June 13, 2019. https://techcrunch.com/2019/06/13/uk-government-invests-194m-to-commercialize-quantum-computing/.*

McMahon, D. *(2008). Quantum Computing Explained. John Wiley & Sons.*

National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196. (2019).*

Nielsen, Mathias Wullum, Carter Walter Bloch & Londa Schiebinger, *Making gender diversity work for scientific discovery and innovation. Nature Human Behaviour 2, 726–734 (2018) doi: https://doi.org/10.1038/s41562-018-0433-1*

Park, Chris, and Michael Allaby. *"optimization." In A Dictionary of Environment and Conservation. : Oxford University Press, https://www-oxfordreference-com.acces-distant.sciencespo.fr/view/10.1093/acref/9780191826320.001.0001/acref-9780191826320-e-5677.*

Pednault, Edwin, John Gunnels, Dmitri Maslov, and Jay Gambetta. *"On 'Quantum Supremacy.'" IBM Research Blog. IBM , November 7, 2019. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/.*

Piper, Fred and Sean Murphy, *'Understanding cryptography' in Cryptography: A Very Short Introduction (Oxford, 2002; online edn, Very Short Introductions online, Sept. 2013), doi: 10.1093/actrade/9780192803153.001.0001, accessed 08 Aug. 2019, 8.*

Preskill, John. *"Quantum computing and the entanglement frontier." arXiv preprint arXiv:1203.5813 (2012), 1.*

Preskill, John. *"Quantum Computing in the NISQ era and beyond". Quantum. 2: 79. (2018) doi:10.22331/q-2018-08-06-79, 2.*

"Quantum Mechanics." In A Dictionary of Chemistry, edited by **Rennie, Richard, and Jonathan Law.** *: Oxford University Press, 2016. https://www-oxfordreference-com.acces-distant.sciencespo.fr/view/10.1093/acref/9780198722823.001.0001/acref-9780198722823-e-3461.*

Schneider, David. *"Full Page Reload." IEEE Spectrum: Technology, Engineering, and Science News. December 05, 2018. Accessed August 1, 2019. https://spectrum.ieee.org/tech-talk/computing/hardware/the-us-national-academies-reports-on-the-prospects-for-quantum-computing.*

Stewart, Duncan. *"Quantum Computers: The next Supercomputers, but Not the next Laptops." Deloitte Insights. December 11, 2018. Accessed August 1, 2019. https://www2.deloitte.com/insights/us/en/industry/technology/technology-media-and-telecom-predictions/quantum-computing-supremacy.html.*

The Centre for Humanitarian Data. *"Working Draft of the OCHA Data Responsibility Guidelines." OCHA. March 2019. Accessed August 1, 2019. https://centre.humdata.org/introducing-the-working-draft-of-the-ocha-data-responsibility-guidelines/.*

The National Academies of Sciences, Engineering, and Medicine *(2019). Grumbling, Emily; Horowitz, Mark (eds.). Quantum Computing : Progress and Prospects (2018). Washington, DC: National Academies Press. p. I-5. doi:10.17226/25196.*