



## Quantum Leaps

During the Christmas break, I had a mundane problem to solve. Most PCs today no longer come with disk drives. This was problematic for me since, like for many of you, my family videos are stored on CDs and DVDs. I needed to upgrade to a more “modern” storage system. I use quotation marks because the modern solution I select today will likely become obsolete very quickly. Why is this the case?

Let us pause for a while and consider this: Are you keeping pace with the technological advances that are speeding by? For example, in a matter of three decades, mobile phones went from the bulky, heavy, and expensive devices available from Motorola in 1984 to the flashy, light, and powerful smartphone devices of 2018. During this same period of time, we went from using the 5.25-in floppy disks in our PCs (the younger generation may not know what those are) to using CDs, DVDs, USBs, and cloud storage. Even computer terminals went from having voluminous screens that occupied large portions of our desks to having flat compact screens and, from there, to having touchscreens that respond to our fingers. All of these transformations in personal technology have happened since my college years. And we view the devices of today as superbly advanced and life changing. I wonder what technology my daughters will have

at their fingertips two or three decades into the future. They will likely look back at the fancy smartphones, smooth touchscreens, and cloud computing of today and view them in ways similar to the way we view the old, bulky cell phones, large floppy disks, and cumbersome desktop terminals of the past.

We should not underestimate human ingenuity and the pace at which technology, the sciences, and engineering are changing the world. The history of these domains teaches us one fact: discovery and technological development are difficult, but they march forward continually and steadily. Sometimes, these developments take a drastic turn and alter the world around us in fundamental ways. The Internet is one notable example with the huge impact it has made on how we communicate, conduct business, or seek information. Imagine living today without the Internet! Wireless communication is another example; it has enabled almost everyone to be constantly connected to others around the globe (and 5G is coming). Many traditional industries have been displaced as a result of these developments. We can now stream videos directly into our living rooms, causing many famous video rental chains to disappear. We can also order products directly online, lead-

ing many well-known business stores and even chains to close.

Businesses, and even civilizations, fall and rise based on the state of their technology. This is no trivial matter. For this reason, scientists and engineers, like you and I, have the solemn responsibility to be forward-looking and to explore the unknown and the impossible continually, even if immediate or short-term rewards are difficult to visualize. For us, what looks challenging today should be the driver for what we aspire to achieve tomorrow. The famous Lebanese author Khalil Gibran (1883–1931) put it

**We should not underestimate human ingenuity and the pace at which technology, the sciences, and engineering are changing the world.**

best by stating that “yesterday is but today’s memory, and tomorrow is today’s dream.” And, to paraphrase the famous American astronaut Neil Armstrong (1930–2012), small steps by men can turn into giant leaps for mankind. From that initial step on the moon in July 1969, space exploration has gone much farther, including the recent landing in January 2019 (almost half a century later) of a Chinese rover on the dark side of the moon and NASA’s recent images of the most distant world ever explored.

Technological progress never stops. We sense it around us. We are living in transformative times, with potential for quantum leaps driven in part by the expansive interest in intelligent

systems, data sciences, the biosciences, and physical sciences. Some leaps will be questionable or unethical and should be regulated. The recent story of the Chinese researcher who announced in November 2018 that he used the genetic altering tool CRISPR to alter the genome of twin babies reverberated across the world. What I find alarming about this story is not that it happened. What is worrisome to me is that the incident adds to a trend that we have been witnessing at an increasing pace. We are perfecting our tools to such a degree and developing interfaces that are so smart

**It is rewarding to be witnessing evolutions in technology that can be transformative.**

and easy to deploy that we are making it easier for rogue players to spread havoc at a disturbing rate. The spread of misinformation over the Internet is one example. The possibility of cybersecurity attacks on key national infrastructure is another example. Critical data breaches in major industry and government agencies is yet another example, including the recent leaks of sensitive personal information for hundreds of German politicians in January 2019. And the list goes on. Just as one talks about espionage and counterespionage, I believe we should have a similar concept in the sciences where we also need to develop understanding and tools to counter the malefic use of whatever advanced technologies we are putting out, especially in this day and age.

This interplay between the great potential offered by new technologies and the threat that they can pose if used for ulterior purposes is applicable to two other prominent research directions in quantum computing and blockchain technology. If successful and fully developed, these technologies can have far-reaching consequences on our way of life. And many government agencies and leading research institutions have taken notice.

For example, in December 2018, the U.S. National Academies of Sciences, Engineering, and Medicine issued the report “Quantum Computing: Progress and Prospects.” The report recognizes the strategic importance of quantum science and engineering while

acknowledging that many technological challenges remain that make the development of practical quantum machines less likely to occur in the near future. In the same month, U.S. president Trump signed the National Quantum Initiative Act to provide US\$1.25 billion over five years for research on quantum information processing. The European Union is also investing US\$1.1 billion over the course of 10 years. These investments pale in comparison to China’s more robust initiative with funding of US\$11.4 billion over 10 years [1]. In August 2016, China even launched

a quantum satellite into space [2]. There have also been multiple initiatives and centers launched in 2018 in the domain of quantum science and engineering at prominent universities and research labs in the United States, Europe, and China. These steps by governments and research institutions point in one common direction. Namely, they highlight the fact that research on quantum science and engineering is highly strategic and potentially transformative. To appreciate the opportunities and challenges that lie ahead, let us consider a brief (but shallow) technical overview.

We all know that our traditional digital computers, like my laptop or your iPad, store information in the form of zeros and ones. Each location in the computer’s memory is called a *bit*, and its value can be zero or one. The size of the memory determines the amount of information that can be stored in the machine. For example, the text of this editorial is saved into my computer. Each word is represented by a string of zeros and ones put together; different words will have different string representations. Therefore, on a higher, macroscopic level, we can view the computer memory as a collection of boxes, with each box storing one of the words. If we were to ask the computer to search for a particular word in the document, it would need to look into each box, check the word stored in it, and move on to the next box until it found the desired target.

One of the attractions of quantum computing is the ability to process multiple states (or *boxes*) simultaneously. Quantum computers use qubits instead of bits. A qubit can be zero or one or in several other simultaneous states at once. Imagine a needle pointer in a device measuring values between zero and one. The needle can be pointing at the endpoints zero or one. It can also be pointing at any value in between, with some locations being closer to zero and other locations being closer to one. For example, if it is closer to one than it is to zero, we may say that the state of the needle is 60% at one and 40% at zero. It is like being in two places at the same time with part of you in one place and another part in a different place. This analogy is imperfect but helpful. Imagine how much more you could do if you were able to be present at two meetings (or *states*) at the same time. If this were possible, you could solve two problems simultaneously rather than have to go to one meeting to solve one problem and then move to the second meeting to solve the other problem. If you could be at both meetings concurrently, such as 40% of you present in one meeting and 60% present at the other meeting, you would be able to solve both problems at the same time. We can extrapolate and assume that one could be present at a thousand or million such locations simultaneously, with a small probability of being present in each location. Then, one would be able to solve many problems simultaneously, such as searching for the target word in our previous example by looking into all boxes in the computer’s memory in parallel.

There are key challenges that need to be overcome before quantum computing can become a reality. For example, qubits are sensitive to noise from their environment, including the perturbations caused by the act of probing the state of a qubit. For this reason, many experts argue that one may need to run a quantum computation multiple times on the data and average the results to smooth out the effect of noise. The quantum computer models of today built by companies like Google, Intel, D-Wave, or IBM still appear to have a

high error rate and the machines use a small number of qubits close to 100. In the report by the U.S. National Academies of Sciences, Engineering, and Medicine, it is stated that the error rate will need to be decreased by at least a factor of 100 or 1,000 down to  $10^{-3}$  or  $10^{-4}$  and the number of qubits increased to hundreds of thousands or millions for quantum machines to become practical. That is a long way to go! But at least the target is clear.

In my view, there are ample opportunities for signal and information processing scientists to contribute to the development of reliable quantum machines. There are connections to many concepts that we are familiar with. For instance, in our discipline, we regularly deal with variables that can belong to a multitude of states in a probabilistic manner. We know how to quantify the amount of information in such variables through their entropy. We also know how to perform inference and processing tasks to extract information from randomness and how to address the effects of measurement noise and define regions for reliable detection and inference. We also understand that when a random variable is measured under noise, we are actually observing a particular realization for it. For this reason, it is common practice to resort to ensemble averaging (the practice of averaging many results and realizations) to assess performance. Our discipline can be a player in this domain and help smooth the transition to practical implementations.

If the ongoing efforts on quantum computing succeed and these machines become available one day, they will have the potential to revolutionize science and technology due to the sheer computing power that they will provide. We will be able to explore new design concepts that are far more complex than those before. We will also be able to simulate intricate biological and chemical processes, discover new pharmaceutical drugs, explore the complexities of the human brain, run realistic simulations of physical and logistical systems, and even design more intelligent machines. The huge leap in computing power will move our exploration space to a far higher dimension.

There are also negative ramifications that we need to prepare for. In particular, much of our communication infrastructure today is secured by encryption keys. These will likely be compromised by the power of quantum machines, with serious risks posed to national security agencies and financial institutions worldwide. The digital world as we know it, as well as all the cybertrust associated with it, can crumble. For this reason, some governments have already started taking precautionary measures. In 2015, the U.S. National Security Agency announced that it was moving to quantum-resistant cryptographic codes.

Quantum computing will also be in a position to make or break another emerging technology known as *blockchain* [3]. This technology provides a trusted way to validate transactions or contracts. Each time a new transaction takes place, it is added to a ledger listing all previous transactions. The new block of information is encrypted based on the history of prior transactions, and the ledger is shared in a distributed manner across a network of computers. Once added, a block of information cannot be altered without altering all subsequent blocks and destroying consensus across the network. One of the main weaknesses of the blockchain technology is that it requires large amounts of energy to perform the required computations to validate transactions. Quantum computing, with its magnified computing power, can help reduce the energy requirement (which is positive). At the same time, this same computing power enables quantum machines to compromise the encrypted channels that form the very fabric of the blockchain (a negative). Some blockchain teams have already recognized this threat and are working on developing ledgers that are resistant to quantum-computing attacks [3], [4]. It is interesting to observe how the blockchain and quantum computing technologies are influencing each other even at these early stages of their development. Talk about an interconnected world!

**In my view, there are ample opportunities for signal and information processing scientists to contribute to the development of reliable quantum machines.**

Whether these technologies blossom is still an open question. Nevertheless, it is rewarding to be witnessing evolutions in technology that can be transformative. Even if these technologies prove to be too challenging to become effective or useful, many other important scientific (and unintended) discoveries

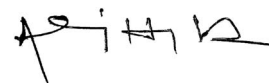
will emerge along the way as has often happened time and again in the history of science.

I used to love to watch *The Jetsons* cartoon in my younger years. It was a futuristic cartoon with

a family living in space and traveling around in tiny flying cars. That cartoon was amazingly forward-looking, and it predicted many technologies, such as communicating with others through video screens (we use Skype and FaceTime today), delivering objects and giving rides in small flying machines (we are witnessing the emergence of drones), using watches that keep you connected to your friends and family (we have Apple Watches today), and relying on robotic assistants (we are even moving toward autonomous vehicles). That was fiction then. It is reality today, and the march toward progress never stops, even in our imagination.

## References

- [1] J. Hsu, "Is the U.S. lagging in the quest for quantum computing," *Sci. Amer.*, Dec. 6, 2018. Accessed on: Dec., 2018. [Online]. Available: <https://www.scientificamerican.com/article/is-the-u-s-lagging-in-the-quest-for-quantum-computing/>
- [2] A. Katwala, "Why China is perfectly placed to be quantum computing's superpower," *Wired*, Nov. 14, 2018. Accessed: Dec. 2018. [Online]. Available: <https://www.wired.co.uk/article/quantum-computing-china-us>
- [3] Emerging Technology, "If quantum computers threaten blockchains, quantum blockchains could be the defense," *MIT Tech. Rev.*, May 1, 2018. Accessed on: Dec. 2018. [Online]. Available: <https://www.technologyreview.com/s/611022/if-quantum-computers-threaten-blockchains-quantum-blockchains-could-be-the-defense/>
- [4] P. Waterland, "Quantum resistant ledgers," GitHub, Nov. 2016. [Online]. Available: [https://github.com/theQRL/Whitepaper/blob/master/QRL\\_whitepaper.pdf](https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf)



SP