WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

# Global Future Council on Quantum Computing Frequently Asked Questions

June 2020

## What makes quantum computers special?

In the 1920s and 1930s, great advancements were made in the development of quantum physics theories by such world-renowned physicists as Albert Einstein, Niels Bohr, Werner Heisenberg, Erwin Schrödinger and others. In particular, they discovered new phenomena in quantum physics, including superposition, entanglement and tunneling, which are all leveraged in quantum computing. It is important to note that the principles of superposition and entanglement are not used in any way in current classical computers. Tunneling is used in a limited way in flash memories, but that has been a relatively recent phenomenon.

Much of classical computing – certain portions of semiconductor theory are an exception – is based on basic mathematical and physics discoveries that were originally discovered in the 19th century, such as Boolean Logic, Ohm's law, Maxwell's equations, etc. The use of these new physical quantum phenomena has provided researchers with additional tools that can be leveraged to create new computer algorithms that can solve certain problems much more efficiently than the classical methods. Classical computing has been successful, but it uses digital ones and zeros to represent symbols in the physical world, which is inherently analog in nature. Quantum computers use quantum mechanical principles to model quantum processes. In 1982, physicist Richard Feynman made the following statement which perhaps says it best: "Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

## What is a qubit?

Quantum computers store information in something called a qubit, which stands for a quantum bit. These are physical structures that store information, like a classical computer bit, but utilize the phenomena of superposition and entanglement. Unlike a classical bit, which is either in the 0 or 1 state at any one time, a qubit can be in a superposition state, which can be in a linear combination of the 0 or 1 state simultaneously. In addition, qubits can be entangled, meaning that multiple qubits are linked together such that changing the state of one will instantaneously change the state of other qubits entangled with it, even if those other qubits are not physically near the original qubit. The basic purpose of a quantum algorithm is that it choreographs the manipulation of the qubits using a variety of techniques so that the quantum state of the qubits is shaped into the answer one is seeking with a very high probability. When the result of a calculation is finally measured, the qubit states will collapse into classical 0 or 1 states and will no longer exhibit superposition or entanglement. You will only obtain the same number of classical bits in your result as the number of qubits used in the calculation.

As anticipated by Feynman, quantum computers that make use of entanglement and superposition can make short work of problems from quantum chemistry and related fields that conventional computers could never tackle, no matter how much time, energy or resources were applied to them. But beyond the quantum science realm, Shor's factoring algorithm provides the example of a solution to a problem in abstract number theory, one that just so happens to underpin the internet security systems we rely on every day.

## Why is quantum computing so hard?

Qubits in a superposition state are very fragile. They easily collapse down to the simpler 0 or 1 state if there is any external interference. To minimize this, current quantum computers will try to isolate the qubits as much as possible by putting them into a vacuum, cooling them down to temperatures near absolute zero, utilizing vibration isolation platforms to minimize movements, and installing magnetic shielding to isolate them from stray magnetic and electromagnetic fields. Even with all these special measures, the lifetime for a qubit in the superposition state may only be a few microseconds or milliseconds for some of today's machines. For comparison,

as long as the power is continuous, a classical bit can stay in its chosen 0 or 1 state for millions of years without flipping over in error to a different state. Much of the research in quantum computing is going into finding ways to achieve better qubit quality so that computations can proceed longer with fewer errors. Fortunately, it is possible to make an effectively noiseless or logical qubit from many noisy physical ones. At present, the best protocols for doing so require many thousands of physical qubits for every logical one created.

## What applications are quantum computing good for?

The most obvious application will be to use quantum computing for quantum chemistry, including material design, drug discovery and chemical reactions. The reason for this is simple: chemical reactions are regulated by the principles of quantum mechanics and the best way to simulate them is to use a quantum computer to model them. Although a classical computer can approximately model very small molecules, the problem is that as the number and size of the atoms in the molecule grows, the number of different forces that need to be included and tracked grows exponentially. So for any reasonably sized molecule, the number of calculations becomes intractable to complete in a reasonable period of time; you will be "bumping" into numbers that exceed the energy output of a star, the number of atoms in the universe, or the number of seconds since the big bang. So it is not just a matter of waiting until conventional technology improves, these solutions require defying convention. Classical computing has developed a few algorithms to approximate these effects, but the predictions from these approximate models are not as good as the scientists' desire.

Other important applications include optimization, financial modelling and quantum machine learning. However, classical computing is continuing to make strides in improving its capability for these problems. Although a lot of work is also being put into developing solutions for these types of problems, there is always a chance that a clever graduate student may develop a new classical technique to solve the same problem.

## What technologies are being used to build quantum computers?

A fascinating aspect of quantum computing is the fact that there are a multitude of technologies being researched to create the qubits and quantum computers. These include technologies such as superconducting, annealing, ion traps, photonics, quantum dots, topological qubits, cold atoms and others. No one really knows yet which of these technologies will win out and become dominant. In fact, a few different technologies may become common depending upon the specific application requirements. Several of these technologies leverage semiconductor manufacturing technologies to take advantage of existing vendor tools and fabrication facilities. Others are leveraging technology from the photonics industry to develop their computers. Although we expect the recent rapid progress that we have seen to continue, we do not expect the development to follow a linear path as different technologies come on stream and show advantages and overcome limitations experienced by others.

## Will quantum computers ever completely replace today's classical computers?

No. Quantum computers will always be used more as co-processors to a classical computer rather than something that replaces the classical computer. Although quantum computers may eventually displace some high-performance classical computers, there are a great many tasks that a quantum computer is not well suited for, such as reading email, using an running a website, maintaining a financial transaction data base, browsing the internet, calculating bank balances, and most of the other tasks we currently perform on computers today. In addition, there is no quantum equivalent for many of the things we take for granted in the classical world, such as disk drives for long-term storage. Also, the probabilistic nature of quantum computers may be a problem in some applications because quantum computers are not, by their physical nature, deterministic.

## Will I ever be able to purchase a quantum computer and install it in my office or home, or even carry it in my pocket like a smartphone?

We do not seeing this happening for a very long time. If this ever does happen, it will take decades or even centuries for the technology to advance far enough to make this economical or reliable. With the possible exception of certain organizations that deal with highly confidential data and require on-premise capabilities, we expect that most access to quantum computing will be through a cloud offering. This is due to the large costs needed to build a quantum computer, preference by the manufacturers to keep the machines in their facilities due to maintenance, calibration, spare parts, and other logistical concerns, and the desire to have the quantum computers physically close to large classical computing installations to support hybrid classical/quantum algorithms that require processing different portions of the algorithm on both types of computers.

## What needs to happen for us to see a useful quantum computer?

Those seeking to build quantum computers have historically had to make a choice between focusing on building a large, fault tolerant, universal quantum computer, or devoting resources towards building a much smaller, noisy quantum computer. There has been some success building NISQ (noisy intermediate scale quantum) machines, however there are no known NISQ applications yet that are superior to those run on classical computers. A functional fault tolerant machine on the other hand could tackle real-world problems by enabling billions of gate operations without being overwhelmed by noise and errors.

## If quantum computers will be so powerful, won't they be power hogs and require an immense amount of electrical power with the associated environmental impacts?

No. When you look at the power utilization in total, it is the opposite. Because of the fundamental principles of quantum computing make it scale exponentially, they will be able to solve large problems with just a fraction of the power that today's supercomputers use. The superconducting, photonic and other technologies that are used to build them take much less power than the transistors used in today's classical computers. In addition, quantum computers will help provide solutions for many other things that provide a negative impact to the environment. These include finding an efficient method for carbon sequestration, minimizing energy use in nitrogen-based fertilizer production and optimizing traffic flows in a city to minimize traffic jams and wasted fuel for automobiles.

## What timeline do you forecast for quantum computers and when will we see them in common use?

Experimental quantum computers are available now and some are publicly available. The primary purpose of these quantum computers is to help end users learn and familiarize themselves with using the machines and the quantum algorithms. Programming a quantum computer is much different than programming a classical computer and one cannot just simply port an algorithm currently running on a classical computer to a quantum computer. A number of organizations have started to study how a quantum computer can be applied to use cases currently facing their organizations. They are starting to develop POC (proof-of-concept) cases to show how they can use such a computer. We expect that a number of the POCs to grow over the next few years with some entering production usage within the next 2-5 years. After that, more production uses will come online on a gradual basis until we will see what might be called common usage in the 5-10 year timeframe.

## Can a quantum computer be used to help find solutions to the current coronavirus situation?

Although a quantum computer will become useful in the future to help us find new vaccines and medications much faster than before, it is unlikely that we will be able to use a quantum computer to solve today's situation. Quantum computing technology is still at an early stage and many scientists are still learning how to best utilize it. We expect the coronavirus situation to be resolved with classical technologies within the next 1-2 years and we think that is just a little too short for quantum computing to make a meaningful contribution. However, we do believe that the coronavirus situation can be used as a case study in the coming years to help us develop techniques where quantum computing could be leveraged to help solve the next pandemic whenever that might happen.

## I read recently that Google has developed a quantum computer that has achieved quantum supremacy. Can you explain what that means?

Google has demonstrated successful completion of an experiment to find a solution with their quantum computer to a very specific crafted problem much faster than the solution can be derived on a classical supercomputer. It is important to note that the problem chosen, called a random quantum circuit benchmark, was specifically chosen for this experiment but has minimal applicability to problems we are likely to see in the real world. Some might call the term "quantum supremacy" a misnomer because achieving this milestone does not imply that a quantum computer is better than a classical computer for all other problems. Nonetheless, it is a significant achievement and helped drive Google's engineering team to create a better quantum chip.

## I heard that quantum computers will be able to break the encryption we use on the internet. Will all of my internet security be at risk?

In 1995, a researcher named Peter Shor developed a theoretical algorithm that would be able to factor a large semi-prime number. This algorithm could potentially be used to find the keys that are used in public key encryption algorithms used on the internet, like RSA or Diffie-Hellman. Fortunately, this would require very large quantum computers that contain millions of qubits. Currently, gate-level computers are available with 53 qubits while quantum annealing computers are available with 2,048 qubits and these are too small and too unreliable to implement the Shor or other factoring algorithms. However, the capabilities of the quantum computers are growing rapidly and industry experts expect that it will take at least another 10 years before quantum computers with very large numbers of qubits are available that could run this algorithm and break the public key encryption we have today.

## Ten years' time is not all that far away. Is anyone doing anything about this?

Yes. There are two different approaches that people are taking to develop a solution. The first is to use quantum mechanical principles to create a quantum internet that communicates between two points using photons, the elementary quantum particles that light is comprised of. By leveraging a basic consequence of quantum mechanics to information theory called the "No-Cloning Theorem", one can guarantee that someone cannot eavesdrop on a quantum internet link without detection. These networks are called QKD (Quantum Key Distribution) networks and there are a number of these networks already in place in the US, China and Europe that operate on this principle. A second approach is a software approach being investigated by the US National Institute of Standards and Technology agency and others. It would use different software algorithms to encrypt data that are not dependent upon factoring a large semi-prime number. There are currently several dozen different algorithms under consideration to replace the current set of algorithms, and researchers are performing intensive research to select ones that cannot be broken by either a classical or a quantum computer, yet are still efficient for everyday use. Although several strong candidate algorithms are available now, we expect to see announcements of the final recommended algorithms in the next 2-3 years.

## So I have nothing to worry about because we will have replacement technology available soon, right?

Not exactly. First, we estimate that over 20 billion digital devices will need to be either upgraded or replaced in the next 10-20 years to use the new forms of quantum resistant encrypted communication. This will require a massive effort, similar to the Y2K effort that occurred in the computing industry 20 years ago. We do recommend that organizations start planning for this now because this conversion of our digital communications infrastructure will take years to complete. In addition, for certain types of data that have both high data value and high shelf life characteristics, there is an attack known as "Harvest now, Decrypt later". Certain attackers may be currently intercepting encrypted data transmissions and storing them on a hard disk drive for later use. Although the encrypted data may not be of any value today, it might still be of interest 10 or 20 years from now when the attacker has access to a powerful quantum computer. We will discuss this in more detail in a future blog article.

## If we do manage to keep Moore's law going for the next 20 years then there is no need for quantum computers, is there?

There are problems which a quantum computer will be able to solve that are completely out of reach, even if all the silicon in the galaxy were turned into a regular classical computer tomorrow. Quantum computers are able to do computation differently and with exponentially greater power. They are not just accelerated versions of classical computers; they are fundamentally different.

## Will blockchain and cryptocurrencies be affected by this?

Yes, the problem is very similar to the data transmissions described above. Some new blockchain and cryptocurrency protocols have already been developed that are believed to be quantum-resistant. And updates will need to be made to Bitcoin, Ethereum and others so that the currencies do not fall into the wrong hands when the encrypted tokens are transmitted from one party to another.

## What is the bottom line? How should we think about the ways that quantum computing will affect society?

We believe that the development of quantum computing technology will follow Amara's Law, which states: "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run." So although there is a lot of discussion in the popular press about how quantum computing will change everything, we caution people not to form unrealistic expectations. Although quantum computing will help provide very significant advances in computing capabilities, it is still at an early stage and will take several decades before it reaches full fruition. But in the end, it will have a significant impact on improving the state of the world.