Quantum computing: from the qubit to a commercial reality

26 February 2019

Quantum computers have been a dream for over 40 years, which comes from harnessing the laws of quantum physics to process information. Although one might hear of this concept often, the general public do not realise the importance of quantum computers and understand how it would affect our society.

Quantum computers promise a technology which is orders of magnitude more powerful than current systems, capable of disrupting entire industries. In the face of an ideal quantum computer, our current network security would be as fragile as a house of cards. It is also believed that quantum computers would bring AI into the next stage, bringing supercomputers from fiction to reality. Having such a technology is just like holding a gun in the world of swords.

Carrying a high expectation, quantum computing is driving significant investment worldwide (currently estimated at $4 billion/year), mostly due to its potential value for economic and information security. Governments are the key investors in quantum computing, both directly and via defence contractors. It is estimated that the total revenue generated from potential quantum computing markets could exceed $15 billion by 2028.

Quantum computing is now more than a scientific curiosity and is rapidly transitioning into a technical reality. But how far away we are from real quantum computing?

Development of the quantum computer

To better understand the current stage of quantum computer, it is worth to have a look at the history of the digital computer. The ENIAC was the first electronic computer built for general purposes in 1945. It occupied large rooms, containing more than 20000 vacuum tubes and was operated with switches that needed to be rewired for every new calculation. Vacuum tubes were later replaced with transistors that today power every electronic design. Progressive miniaturisation of microprocessors has taken us in less than a century from vacuum tubes to pocket-sized digital computers, following Moore's law .

A similar revolution is taking place today with the advent of quantum computation. Many current prototypes of quantum computer are still hybrid ones (leveraging both quantum and classical computation), which occupy a few garages and have less processive power than the most basic PC. However, the development of quantum computers is moving fast.

IBM showcased a quantum computer at the Consumer Electronics Show (CES) in Las Vegas earlier this year. The prototype, which IBM claims is the first integrated, general-purpose quantum computer, has been named the 'Q System One', and is enclosed in a 3-meter sealed cube made of borosilicate glass. IBM claims that Q System One is, with 20 qubits, more reliable than its previous experimental prototypes, bringing the company a step closer to the commercialization of this technology.

As expected, large IT players are at the forefront of quantum computing. Just like the early players in classical computers ended up dominating the market, the same might be true for the emerging quantum computing market. This is why larger blue-chip companies are moving into the quantum computing race. For example, Intel is working on a 49-qubit chip, Google designing a 72-qubit quantum processor called Bristlecone, and Microsoft is working on a scalable quantum computer. The image below shows some important players and investors in quantum computing.

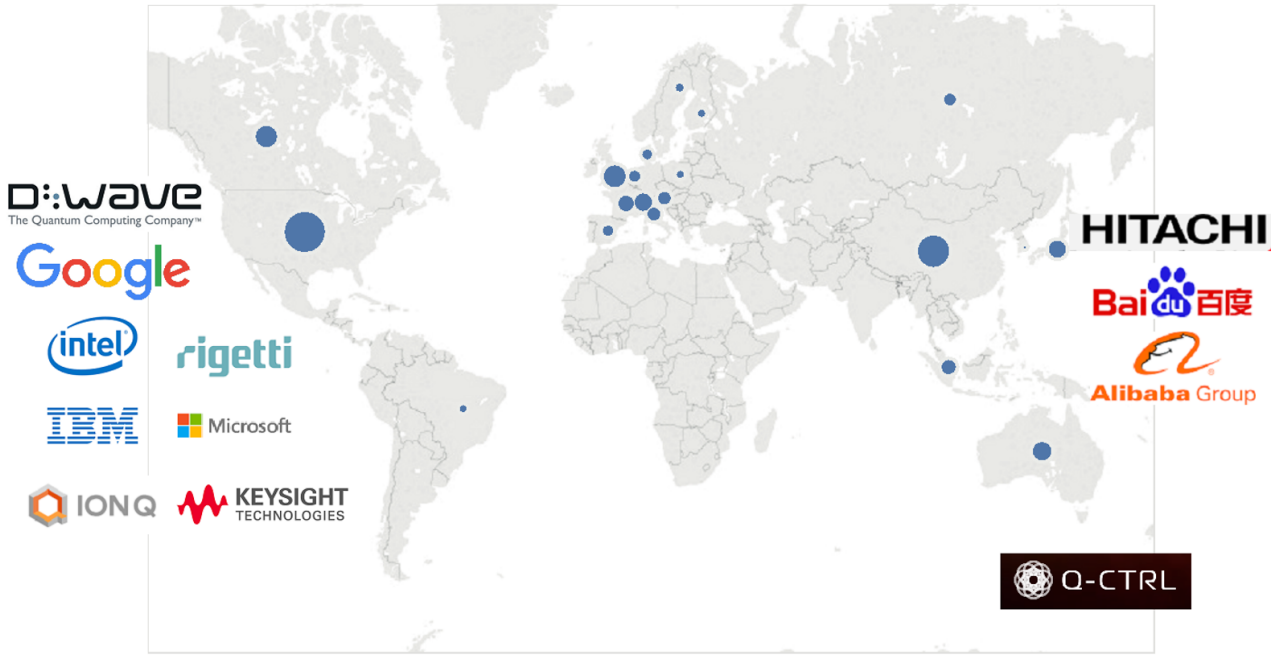

Figure 1 worldwide investment and key players in quantum computing. The size of circles shows the investment.

From bit to quantum bit

But what is a quantum computer and how is it different than a classical computer? The word quantum suggests some exotic property closely linked with quantum physics, which is the branch of physics that describes the world of atoms and its subatomic particles. Despite the name, quantum computers only differ from classical computers in the way they represent and process information. Classical computers process information with the limitations of classical physics. Information is represented by bits (either 0 or 1). Quantum computers, however, make use of an important quantum phenomenon, known as superposition, by which the state can be in both 0 and 1. This coherent superposition of 0 and 1 is a quantum bit (qubit). A quantum bit when represented on a sphere, the angles the radius forms is related to the probabilities of the state being in either 0 or 1 ((shown in Figure 2) Source: Nielsen, M. A. & Chuang, I. (AAPT, 2002)) . This strange quantum property allows for a quantum bit to encode more information than a regular classical bit. For example, a pair of qubits can represent four states, three qubits eight states, and N qubits can represent 2N bits.

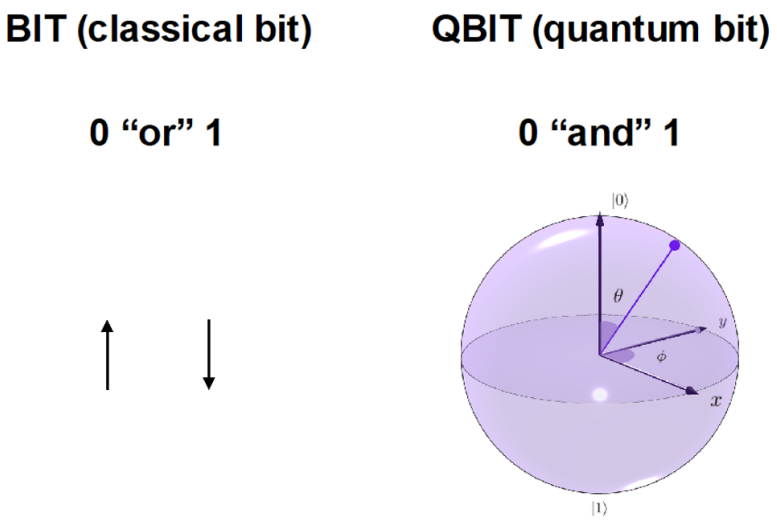

Figure 2 A classical bit in its two possible states (0 or 1) and geometrical representation of a quantum bit (so-called Bloch sphere), as a superposition of 0 and 1. The angles on the sphere are related to the odds of being either in 0 or 1

How to build a quantum computer?

Quantum computing is no longer a mere scientific curiosity, only discussed in some theoretical physics textbook. In the past years, engineers have realised several qubit platforms experimentally. Two promising technologies stand out as physical implementations of quantum computers, namely ion traps and superconducting qubits. The most natural approach is to use single atoms as qubits, trap them in a confined space and manipulate them with lasers. In ion traps, each atom can represent the binary code values of 0 or 1 (or a super¬position of the two), as illustrated in (Figure 3 right). In superconducting qubits, however, the strategy is based on building superconducting circuits that can take on the value of 0 or 1 or a superposition, by the presence or absence of a microwave photon (Figure 3 left).

We are used to desktop computers (and phones) with billions of classical bits. Quantum engineers have managed to create quantum computers beyond 20 qubits. Why is this so challenging? An essential requirement is to generate and maintain isolation of individual quantum particles and retain their "quantumness". Qubits lose their quantum properties easily and become mere classical bits (a process known as decoherence). This is why the physical implementations of quantum computers often require extreme conditions to avoid any sources of noise, such as ultralow temperatures and ultrahigh vacuum. The fragility of qubits makes large-scale quantum computation practically impossible, unless a form of error correction is used. Quantum error correction is a crucial aspect of quantum computation and helps preserve the fragile quantum states making quantum computation feasible. Sceptics point out that the high sensitivity to noise is a significant roadblock for successfully implementing quantum computers that are better than classical ones. However, experimental efforts to reduce the noise, increase the lifetime of the qubits and reduce the time required for single operations are on their way.

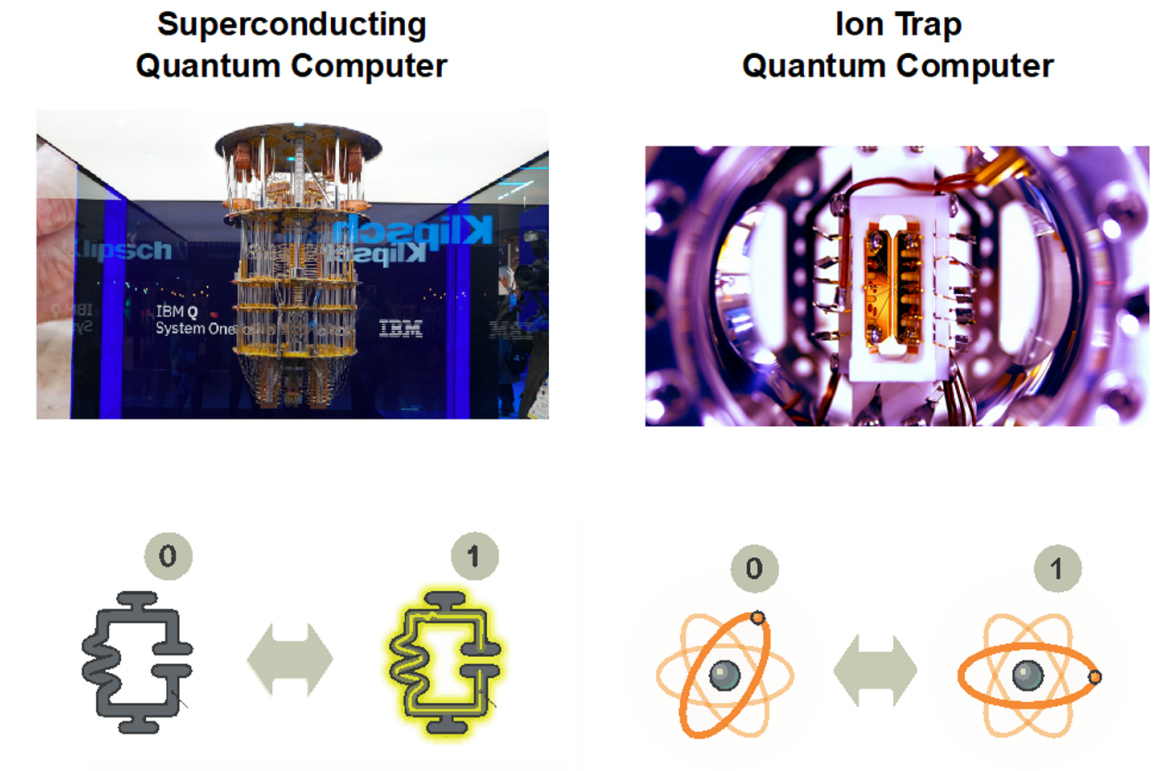

Figure 3 The IBM Q System One is a superconducting quantum computer of 20 qubits (left, from CES 2019). This technology is, made of superconducting circuits. Qubits can take the value of 0 or 1 or a superposition based on the absence or presence of a microwave photon. The Ion Trap (right) consists of trapping atoms in a confined space and storing information in their electronic state. (Image from Christopher Monroe Laboratory)

What can quantum computers do and why should we care?

Early on, physicists realised the immense computational potential of qubits. For example, cryptography is one important future application of quantum computing. Decryption of messages could become trivial with quantum computers as they will solve complex calculations in mere seconds. Multiplying two large numbers to get a larger one is easy, but the opposite problem (integer factorisation) is at the foundation of modern communication security cryptosystems. The ability to factor a large number into its prime integers, known as the RSA-problem, is intractable with modern classical computers. Peter Shor's algorithm shows that an ideal quantum computer could factor integers efficiently and therefore break RSA-codes in reasonable times. Figure 4 shows how the time it takes to find the RSA-key scales exponentially for classical computers, reaching the age of the universe for problems that quantum computers could solve in a matter of hours.

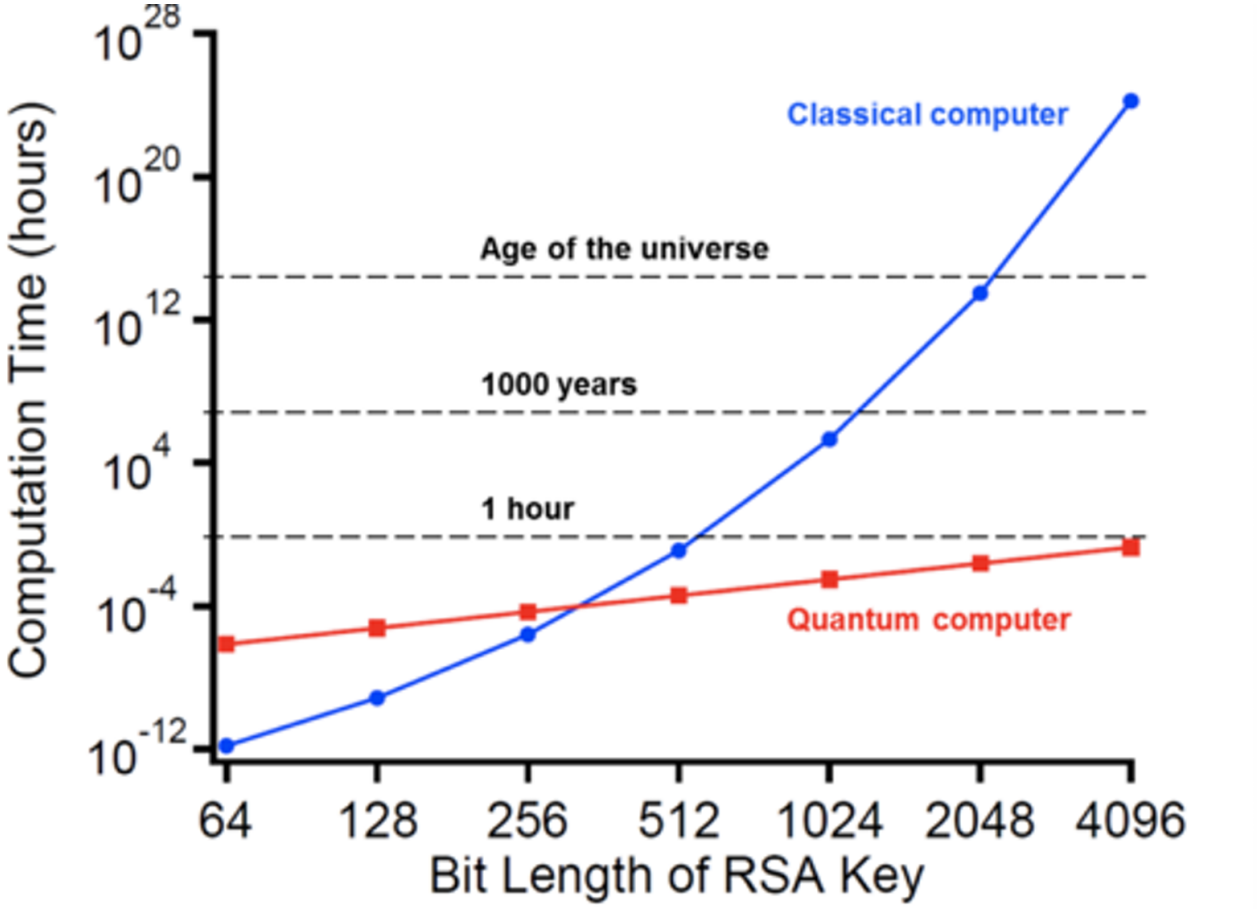

Figure 4 The computational time needed for classical and quantum computers depending on the number of bits in a key used by a cryptographic algorithm.

In addition to breaking cryptocodes, ideal quantum computers can search unsorted databases and solve optimisation problems more efficiently. More importantly quantum computers can serve as "quantum simulators" for more complex systems, with applications in drug development and material science.
The perspective of combining machine learning algorithms with the computational power of quantum computers has opened up a new field of Quantum Machine Learning. Quantum computers will help solve complex AI problems more efficiently. Finding patterns in a sea of data, using these to predict future outcomes will open the door to many possibilities, ranging from traffic control to supply chains. With the vast amount of data that we generate today, it is in this area that quantum computers can be disruptive.
Quantum supremacy is the moment when quantum computers are able to solve problems that classical computers cannot. There is a long road ahead to reach that goal. There are a number of technical obstacles and thus far quantum computers are not faster than a classical computer. While the software and hardware challenges are still considerable, large-scale realisations of quantum computers are on their way.

The journey for the classical computer took a century, from the vacuum tubes to the smartphone. The race for the quantum computer is on, and it moves fast. Whether big or small, we will soon find out what kind of impact quantum computers will bring.

If you wish to learn more about quantum computing please contact us at: research@IDTechex.com

Authors:
Dr. Ibon Santiago is a physicist at the Technical University of Munich.
Dr. Luyun Jiang is a technology analyst from IDTechEx.

Sources:
1 The Economist (2017).
2 Nielsen, M. A. & Chuang, I. (AAPT, 2002).
3 Debnath, S. et al. Demonstration of a small programmable quantum computer with atomic qubits. 536, 63 (2016).