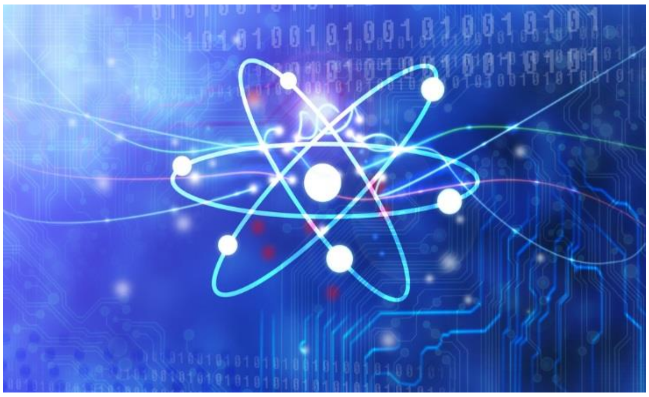
At a glance
Scientific Foresight: What if …?

What if computers were trillions of times faster?

Could the theory of quantum mechanics one day revolutionise commonplace technical devices such as sensors, communication devices and computers?


©Shutterstock/Winiu

Quantum mechanics is a scientific theory that has revolutionised our understanding of the Universe. In the world of classical physics, a system is always in one particular state (e.g. at rest or in motion) while in the quantum world, a system can be in a superposition of two or more states. Performing a measurement on such a superposition causes it to collapse into a single state. Furthermore, in contrast to the classical world, where a system can be measured without changing it, in the quantum world a measurement can have an impact on the state of the system.

As counterintuitive as quantum theory might sound to the layperson, it is already the basis for many common technologies, such as the transistor (the building block of modern computers) and the laser (a device used to produce well-controlled and powerful beams of light). However, scientists are now able to control the states of individual quantum systems with high precision. This ability could result in the development of new technologies, which can be divided into three areas: sensing, cryptography and computing.

Quantum sensors encompass a wide range of devices which use quantum effects to make high-precision measurements of quantities such as time, gravity and magnetic field. Many of these devices could be commercialised within the next few years, with quantum clocks in particular already substantially surpassing their traditional counterparts. Cryptography is usually performed by the prospective recipient of a message distributing a public key for a potential sender to encrypt a message, which can only be decrypted with the private key held by the recipient. This method depends upon it being computationally difficult to determine the private key from the public key, as it is possible that a hacker could find out the public key by intercepting communications between the two parties. The alternative of quantum cryptography is (at least in theory) impossible to defeat, as it relies on the fundamental law that measuring a quantum system changes that system – when using such a system to transmit information, two communicating parties can find out whether someone is listening to their messages. Finally, quantum computing is the technology with perhaps the greatest potential, whilst also being the least developed. Ordinary computers use 'bits' to store and process information, which are represented by electronic components that have two possible states: one representing '0' and the other representing '1'. A quantum computer would also allow a 'quantum superposition' of these two states, which can be thought of as being both '0' and '1' at the same time. These superpositions would vastly speed up the computation of certain problems, some of which would take billions of years on an ordinary computer, but only take a matter of hours on a quantum computer.

Potential impacts and developments

There is considerable public and private interest in developing quantum technologies. The Netherlands and the United Kingdom have programmes in this area that have attracted hundreds of millions of euros both from public bodies and from industry. Also, the European Commission recently announced a plan to invest €1 billion in a quantum technologies flagship initiative within its investment in Future and Emerging Technologies. Among those technologies, a quantum computer is perhaps the one that would be most disruptive.

EPRS | European Parliamentary Research Service
Authors: Lieve Van Woensel with James Tarlton
Scientific Foresight Unit (STOA)

There are several known applications of a quantum computer. One of these applications is calculating how other quantum systems behave, which could be very useful in the development of new chemicals, medicines and materials. Another possible application is in artificial intelligence, although it remains unclear what improvements a quantum computer would offer in this area. One other application is in breaking our existing cryptography protocols. The most commonly used protocol, the Rivest-Shamir-Adleman (RSA) protocol, has been shown to be vulnerable to attack from a hacker with a quantum computer. This vulnerability could encourage improvements in quantum cryptography, which would be protected from such an attack. The link between quantum computing and quantum cryptography means that if the progress in developing a quantum computer were to be faster or slower than expected, then there might be a corresponding increase or decrease in the amount of investment in quantum cryptography. However, a quantum computer could be used not only to decrypt existing transmissions, but also data that were intercepted and recorded in the past. Therefore, unless quantum computing is shown to be completely unfeasible, organisations wanting to keep their current information secure in future decades will likely maintain an interest in quantum cryptographic systems.

Anticipatory policy-making

As with many new technologies, it is important to consider how to bridge scientific research and commercial application. The science behind quantum technologies is believed to be well understood, and research is now moving beyond demonstration experiments towards building useful devices. However, as commercial application of many of these technologies is still some way off, investment from private companies remains at a fraction of what is put into their conventional counterparts. Public investment programmes will be important for bringing quantum technologies closer to commercial viability, and the effectiveness of current programmes should be monitored in this regard.

One particular aspect of quantum technologies that may need large public investment is the infrastructure required for quantum cryptography. This technology would be likely to require special optical fibres to transmit single photons (particles of light) in such a way that their quantum state is maintained. There are already initiatives to develop this infrastructure in China, Japan and the USA, as well as in some Member States of the EU, notably the Netherlands and the United Kingdom. In order to allow for quantum communication across the EU, as well as around the world, there would need to be an uninterrupted network. However, companies and other organisations may instead prefer to use existing infrastructure, but with new 'post-quantum' protocols, which have no known quantum algorithm that could be used to break the encryption (but such algorithms may be developed in the future). This may mean that investing in the infrastructure for large-scale quantum cryptography would not make economic sense.

For quantum computers, the question of what they would be able to do is still an active area of research. They could be used to simulate quantum systems, leading to possible applications in medical and materials research, and they would vastly speed up certain common computational tasks, such as searching large databases. The ability to break existing cryptography protocols is one application that could have negative consequences, and it is possible that other harmful applications will be developed in the future. Possibilities include the ability to hack other security protocols that are currently considered to be secure against a quantum attack. In addition, there may be no advance warning of new threats posed by quantum computers – once an algorithm or software package is created, it could immediately be applied by anyone with a quantum computer. Therefore, it may be prudent to regulate access to such machines. However, a likely business model for this emerging industry would be to allow users to submit problems online to be solved by a central computer (as already demonstrated by IBM and the University of Bristol), which may result in such regulation being unfeasible. A delicate balance has to be struck, as excessive regulation may stifle the potential for a huge acceleration in technological progress, reducing the corresponding benefits for society.

Quantum technologies offer fascinating possibilities which have yet to be fully explored, and progress in this area could be accelerated by boosting public investment and attracting an increasing amount of private investment. However, policy-makers need to devote a considerable amount of attention to the field as progress unfolds, in order to minimise the possible negative consequences resulting from these technologies.

This 'What if ...?' publication is a product of the Scientific Foresight Unit (STOA) of EPRS. More information on the unit's activities can be found at http://www.europarl.europa.eu/stoa/ and http://epthinktank.eu/author/stoablogger/