Károly Kiss

Quantum Computers are Near

SNDL and post quantum cryptography[1]

According to experts, quantum computers will be operational by 2030, which means that from then on, these machines will be able to decipher any code. Criminals and data thieves in cyberspace systematically prepare for this: they collect and steal data in order to decipher it with quantum computers. This is called SNDL: store now, decrypt later.

The official side is prepared for this by developing quantum-resistant cryptographic methods: PQC, post quantum cryptography.

The task is incredibly big. By 2030, the protection of more than 20 billion devices must be solved: all mobile phones, laptops, iPads, servers, websites, and mobile applications. Plus, all the systems built into cars, ships, planes, and operating infrastructure will need to be updated.

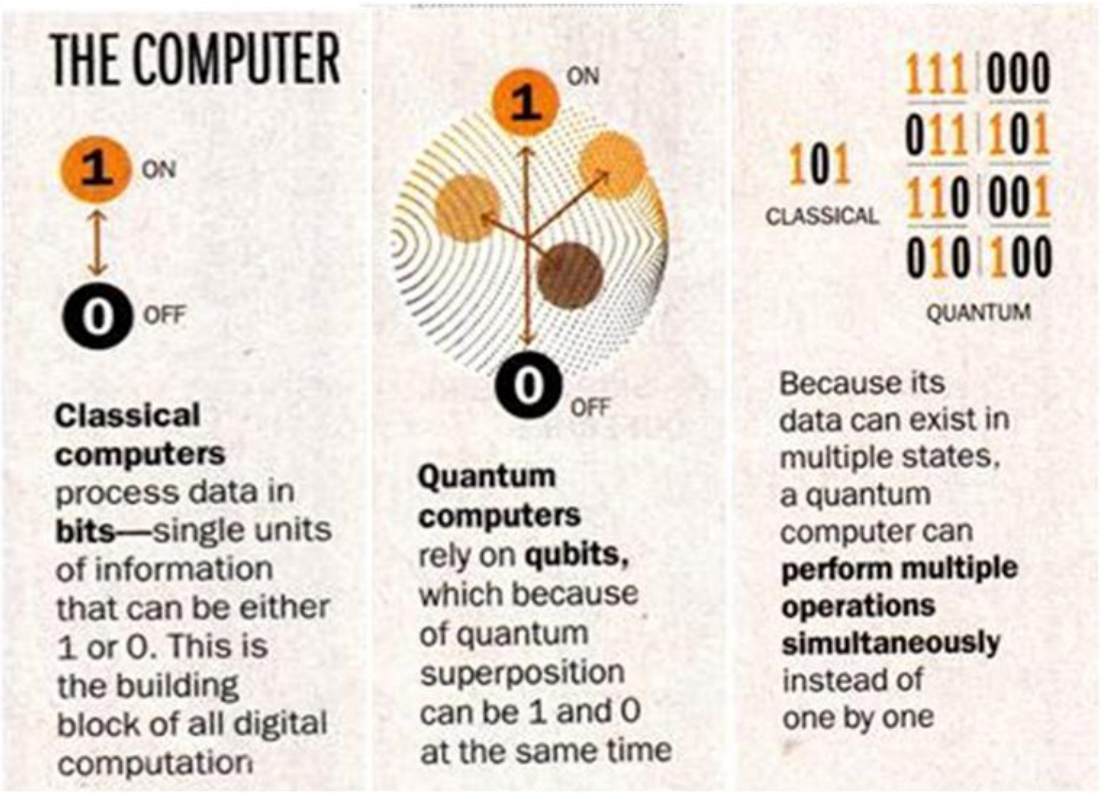
The principle of functioning

This is something that mere mortals cannot understand (including the author of these lines, who is an amateur on the subject). Quantum physics is based on superposition and quantum entanglement. These concepts refer to the position and relationship of electrons, which are almost opaque during complex chemical reactions. The innumerable number and variation of these positions gives the possibility of the placement of the bits and the operations with them.[2] „Quantum computers turn some of the probabilistic, simultaneously here-and there weirdness of quantum physics into numberr-crunching elegance.”[3]

The operation of traditional computers is based on binary bits, which can exist in either a 1 or a 0 state, and are used for information processing. Qubits, the basis of quantum computing, are tiny subatomic particles that can exist in both states at the same time. "The jump from dual data processing to multivariate exponentially increases computational capacity." [4] A quantum computer better reflects and corresponds to the processes taking place in nature. Molecules are made up of atoms held together by electrons, and these electrons are part of every atom. The way electrons are part of two atoms at the same time represents the working principle of a quantum computer. The idea is traced back to Richard Feynman saying in 1981 that “Nature

[1] The Economist: The World Ahead 2023**.**
[2] A comparatively less complicated way of storing information and computing is when the genes of DNA are used for the same purpose. (But as a theoretical possibility, the use of electron spin for information storage was also discussed.)
[3] The Economist July 16th 2022.
[4] Time February 13d 2023. 2030 / Technology.

isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical".[5]



The IBM – back on the cutting edge

IBM has more than 60 quantum computers in operation, more than all other such devices in the world combined. In recent years, IBM has lagged behind Apple and Microsoft in cloud technology and has not grasped the opportunities inherent in the development of artificial intelligence. But with quantum computing, it is now back on the cutting edge. Its latest development is the 433-qubit Osprey chip, the world's most powerful quantum processor, the speed of which – if expressed in traditional bits – would far exceed the number of all atoms in the known Universe.[6] (IBM plans to build a 1,121-qubit chip this year, and then surpass the 4,000-qubit speed in 2025 by creating "modular quantum circuits".

Uses and implementation

What we have known for a long time; that after the appearance of quantum computers, there will be no security code that they cannot crack. But what else can they be used for? In the

[5] The Economist September 26th 2020.
[6] Time February 13d, 2030 / Technology. (Honestly, I have no idea how the computational speed can be expressed in terms of numbers of atoms. KK)

strict sense of the word for everything that needs to be optimized based on large data sets. To optimize the route of tankers crossing the seas of the world, to decide which of the patients in an intensive care unit it needs the most urgent maintenance, the creation of new materials using the knowledge of chemical processes at the atomic level, the control of artificial intelligence, the improvement of the algorithm of self-driving cars and flying drones, the operation of asset management companies, currency speculation, the development of a new kind of "deep learning" of AI, for data processing, shortening the lengthy design process of vehicles, anticipating the results of industrial experiments, etc. etc. “This technology is the next industrial revolution.” [7]

At first glance, it seems that quantum computers will be able to perform similar tasks as artificial intelligence: solving complex intellectual tasks.

Development costs

In 2020, $412 million was available to the industry globally. In 2027, according to estimates, the sector will have 8.6 billion dollars. Today, 17 countries have quantum strategies and four more are under development. Since the mid-1980s, China has spent an estimated $25 billion (!) on quantum computing research. (In 2021, the Chinese were still in the lead with their 56-qubit computer.) These developments are a priority in their five-year plan.

The US government considers this area to be a serious threat to the economy and national security and treats it as a priority at all government levels. According to estimates, America should spend an amount on the order of 1 trillion (thousand billion) dollars to prevent the future "quantum threat". The program is reminiscent of the Manhattan Plan.

According to the World Economic Forum, in 2022 the world will spend more than 30 billion dollars on quantum development; roughly half of this is from the Chinese, a quarter from the EU, and America 1.2 billion (compared to the thousand billion considered necessary)

I have been studying China's economic situation for years, I try to keep up with the developments there. Contrary to the general professional perception – that China is approaching America in terms of economy and science, but it will take a long time to overcome its disadvantage – my opinion is that catching up and Amerrica’s falling behind will occur much sooner than expected. The topic under discussion is eloquent proof of this.

Cyber security

Today, in practice, the cyber security used by large international platforms and smartphone service providers is based on the RSA system (Asymmetric Cryptography Algorithm). An average computer today would need billions of years to crack these codes. A fast quantum computer would only need a few hours to do this. At the end of last year, Chinese computer

[7] I.e.

scientists announced that they had managed to crack the RSA system with a 372-qubit quantum computer.

The new technology also brings a new element to the world of computerization: it requires trust! We can still track the results produced by our traditional computers with manual calculations. In the age of quantum computers, this will no longer be possible, you have to believe in the result.

Bp, May 2023

Source:

Time, February 13d, 2023, 2030 / Technology: The Quantum Leap (Leslie Dickstein)
The Economist: The World Ahead 2023
The Economist July 16th 2022: Cryptography. Post-quantum solace.
The Economist September 26th 2020. Quantum computing. From cloisters to the cloud.
Asbóth János: Szuper a pozíció. Magyar Nemzet 2023 már. 25. (Eötvös Z.)