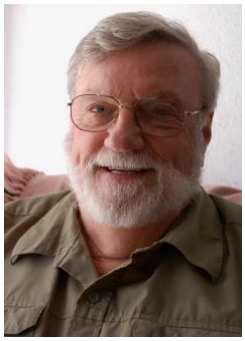
Quantum Computing vs. Encryption

By Gerald Trites, FCPA, FCA, CISA
Editor in Chief



Jerry is a retired partner of KPMG, and a retired, tenured Professor of Accounting and Information Systems at a Canadian university. He also served for 12 years as Director of XBRL Canada and has published 12 books and numerous articles and papers.

He is Editor in Chief of ThinkTWENTY20 and has recently published a book on Corporate Financial Reporting on the Internet.

Quantum computing is at the gates and is likely to disrupt our information systems. It is much faster than conventional computing and can handle tasks that are impractical or impossible for conventional computers. While quantum computers have not reached the mainstream yet, the overall consensus is that they will in time. How much time depends on who you talk to, but generally estimates range from five to twenty years. Given the rate of change in the past few years, there is a growing realization that the shorter time span is more likely. Google, IBM, Microsoft and Honeywell already have quantum computers. For an extensive discussion of the quantum computers in place in various industries, see this article from *ISACA Magazine*.[1]

As is common knowledge, conventional computers (which include all the desktops, notebooks, laptops and smart phones we currently use along with more traditional computers) are based on a binary numeric system. The smallest of the components are bits, which can reflect one of two states, such as on or off, positive or negative.

Given their speed and power, quantum computers could have a major impact on encryption, which is the backbone of modern IT systems security.

How Does Quantum Computing Work?

Quantum Computing is based on quantum physics, which posits that some things can exist in several different states, even at the same time. It's a field that is counterintuitive for most of us and difficult to understand, yet it has been mathematically demonstrated to be sound. In a technological sense, quantum computing is accomplished through the use of qubits, superposition and entanglement.

[1] Ahmet Efe, PhD, CISA, "Anticipating the Disruptive and Incremental Innovations Brought by Quantum Computing" (COBIT 5 Foundation: *ISACA Magazine*, January 1, 2020). *https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-1/anticipating-the-disruptive-and-incremental-innovations-brought-by-quantum-computing_joa_eng_0120.pdf*.

Qubits are the smallest of the components in quantum computing, rather like a bit in conventional computing. One suggestion is to "think of a qubit as an electron in a magnetic field. The electron's spin may be either in alignment with the field or opposite to the field. External influences, like a laser beam, can change the electron's spin from one state to another, but if the strength of the charge is sufficient only to stop the spin but not change it then according to quantum law, the particle then enters a superposition of states, in which it behaves as if it were in both states simultaneously. Due to the phenomenon of superposition, the measured particle has no single spin direction before being measured, but is simultaneously in both a spin-up and spin-down state."[2]

Enter entanglement, which is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated. This leads to correlations between observable physical properties of the systems. In a computer, they need to be close together in order to avoid outside influences on their stability.

The state of the particle being measured is decided at the time of measurement and communicated to a correlated particle, which simultaneously takes on the opposite spin direction to that of the measured particle. This is accomplished in an engineering sense by inserting two charged slivers into a silicon slab, all at a micro level, to represent the two correlated particles. To keep them in superposition and entangled, it is necessary to maintain them in an environment free of all external influences, by freezing them to a very low temperature.

It follows that each qubit utilized, consisting of two correlated particles, could take a superposition of both 0 and 1. Thus, the number of computations that a quantum computer could undertake is 2^n, where n is the number of qubits used. A quantum computer comprising 500 qubits would have a potential to do 2^500 calculations in a single step; 2^500 is a huge number – more than all the atoms that exist in the known universe.

To illustrate the speed, "In 200 seconds, the (Google) machine performed a mathematically designed calculation so complex that it would take the world's most powerful supercomputer, IBM's Summit, 10,000 years to do. This makes Google's quantum computer about 158 million times faster than the world's fastest supercomputer."[3]

---

[2] https://whatis.techtarget.com/definition/qubit.

[3] https://medium.com/predict/googles-quantum-computer-is-about-158-million-times-faster-than-the-world-s-fastest-supercomputer-36df56747f7f.

"Goldman Sachs recently announced that they could introduce quantum algorithms to price financial instruments in as soon as five years. Honeywell anticipates that quantum will form a $1 trillion industry in the decades ahead."[4]

Given their speed and power, quantum computers could have a major impact on encryption, which is the backbone of modern IT systems security.

The threat of quantum computing to encryption is widely known. But it has not been acted on with much alacrity because of the widespread feeling that quantum computing is far away in the future

Encryption is in Danger

Modern encryption is based on the fact that conventional computers are limited in their ability to solve problems other than in a linear way. They have always had an issue dealing with permutations and combinations, because they need to identify and solve every possible outcome and then compare the result to the desired outcome.

"A particular problem they struggle with is a category of calculation called combinatorics. These calculations involve finding an arrangement of items that optimizes some goal. As the number of items grows, the number of possible arrangements grows exponentially. To find the best arrangement, today's digital computers basically have to iterate through each permutation to find an outcome and then identify which does best at achieving the goal. In many cases this can require an enormous number of calculations (think about breaking encrypted passwords)."[5]

"Researchers have identified combinatorics problems in banking and finance that might benefit from quantum computing, including portfolio optimization, foreign exchange arbitrage, and credit scoring."[6]

Encryption is a standard technique to protect most systems, particularly mission-critical ones. It's the norm with banking and other financial systems. In its most basic form, encryption works through the use of encryption keys that, when applied to plain text, yield, through an algorithm, the cipher text, which can't be read without the key for decrypting it. So, the recipient is sent a decryption key, which is the only key that can decrypt the cipher text. A hacker would need to obtain the decryption key or intercept it when it is sent to the authorized recipient. Interception of keys is an important risk and much effort has been expended to make key transmission secure. Encryption is part of blockchain for its role in public/private keys, and that's an important role.

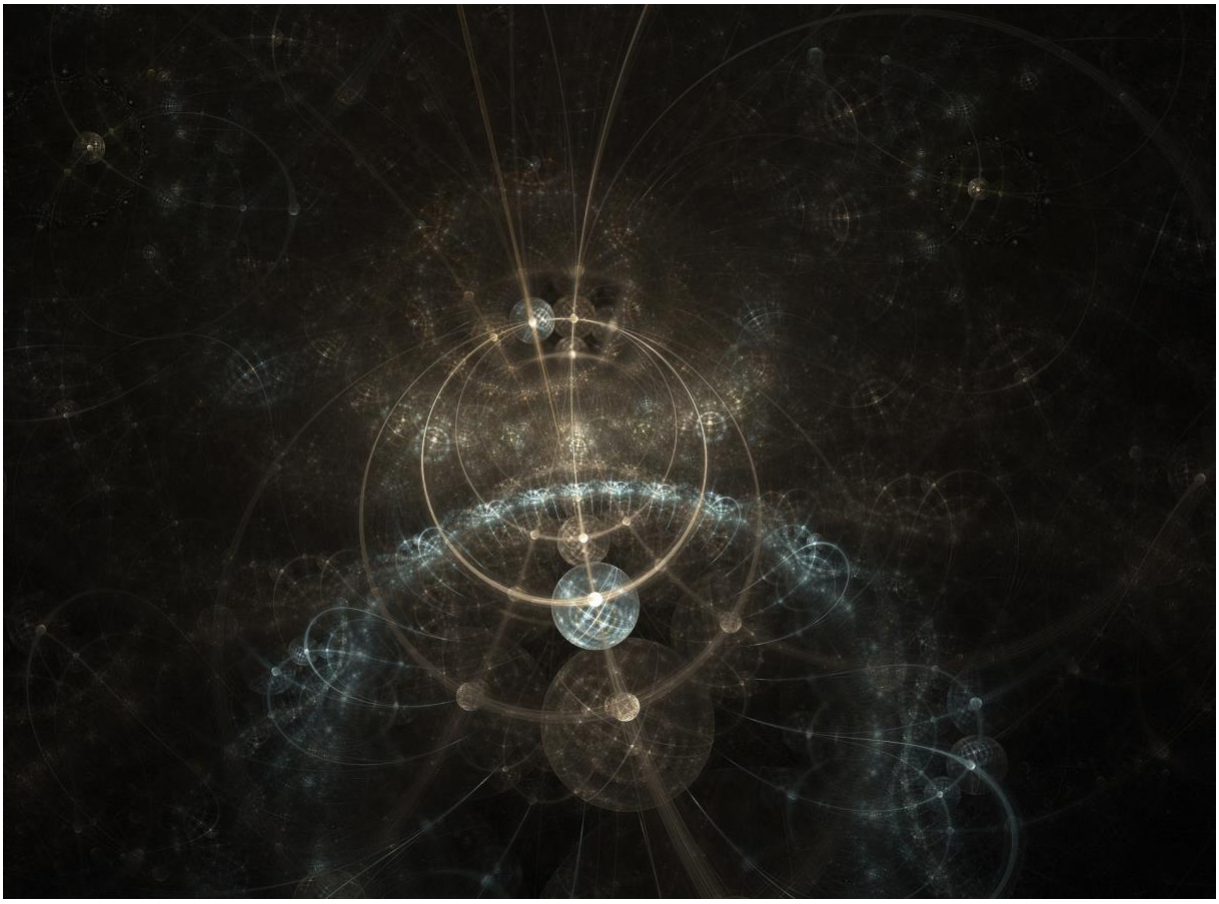
---

[4] Francesco Bova, Avi Goldfarb and Roger Melko, "Quantum Computing Is Coming. What Can It Do?" (*Harvard Business Review*, July 16, 2021).

[5] *Op. cit., HBR*.

[6] Francesco Bova, Avi Goldfarb1 and Roger G. Melko, "Commercial applications of Quantum Computing" (*EPJ Quantum Technology*).

Much of the encryption used today can be easily broken with quantum computers. This poses a real challenge for all kinds of computer systems. The World Economic Forum has said that quantum computing could make today's cybersecurity obsolete.



Meeting the Challenges

The threat of quantum computing to encryption is widely known. But it has not been acted on with much alacrity because of the widespread feeling that quantum computing is far away in the future – but the future is coming quickly these days. Given the likely timeframes of events, it is advisable that IT systems managers consider what action they might take today to protect their systems in the future.

"If a fully functioning sufficiently coherent quantum computer becomes available, many files encrypted using current standards would be more easily decipherable. Therefore, if something needs to remain encrypted for many years, the threat that a quantum computer may be available in a decade or two means that it is worthwhile investing in quantum-safe encryption today."[7]

[7] *Ibid*.

There are several ways to invest in quantum-safe technology already. Commercial applications are available that are not dependent on having quantum computers available but, rather, make use of some of the quantum computing concepts. Increasing key sizes is an obvious starting point. Use of different algorithms is another tactic. Various white papers and directives are available.[8]

Another tactic for addressing the problems with key transmission is QKD (Quantum Key Distribution) which is based on the quantum idea that any observation of data fundamentally alters those data. The state of the data after exposure cannot be predicted. Therefore, if a key transmission is intercepted and observed, even briefly, then it will change and become useless for purposes of decoding the cipher for which it was intended. QKD is used in the banking and finance industries now, not using quantum computers, but rather using a process inspired by quantum physics to detect the presence of a third party and developing a new key known only to the parties to a transaction.

This is only the beginning. As quantum computers become more widely available, and to the extent that current encryption models are not updated, there will almost certainly be significant cases of system intrusion and data loss.

OIO

[8] For example, https://pqshield.com/quantum-threat/?gclid=Cj0KCQiAnuGNBhCPARIsACbnLzqlL6IwhXYLPkMocdwg7EHZDHC8Vp1cM4RH4WpqOWrNo-r5-v6qJHYaAp7pEALw_wcB and https://www.etsi.org/technologies/quantum-safe-cryptography