



Quantum Internet

Description

[Also available as [audio](#) delivered by a soft American voice.]

Quantum computers exist in labs and theoretical models at present, but promise to outperform current, everyday supercomputers by many orders of magnitude. As I'm looking into [cryptography](#) and the built environment I thought I should find out more about quantum computing.

Quantum computers can potentially remove the need to iterate through the huge numbers of combinations required to crack a code, reconstruct an original source document from a hash string or derive the key used to encrypt a file. I've read articles that suggest quantum computers could thereby break the [blockchain](#) underlying bitcoin and other cryptocurrencies. Without some remedial action, the wealth tied up in cryptocurrencies would disappear.

These threats have spawned an industry of *postquantum* encryption algorithms designed to thwart the capabilities of these computers of the future. Cryptographers are also developing encryption methods based on quantum computing that will be even more robust than current methods. Keith Martin's book *Cryptography: The Key to Digital Security, How It Works, and Why It Matters* provides a helpful summary of some of the issues in a section ominously titled "Weapons of mass decryption."

Quantum researchers and the companies and universities that employ them have produced numerous YouTube videos explaining how quantum computing works and what it offers. The most helpful [video](#) I've found so far in explaining the process is by Robert Smith of Rigetti Computing. I draw on some of his explanations of the maths here, though any errors are my own.

Qubits 101

Here's the state of my current understanding. The basic unit of arithmetic in a computer is the bit, an electronic component in a microchip that can be in one of two states. It is either on or off, i.e. 1 or 0.

Microchips contain circuitry that stores and manipulates strings of bits at billions of times per second. Unlike a binary computer, the basic unit in a quantum computer is the *qubit*, a cute name that indicates

a unit that stores a value of either 1 or 0 or both 1 and 0.

Spinning

The condition of being in two states at once is the nub of the quantum mechanics conundrum. Subatomic particles such as electrons and protons spin in two directions, usually described as up or down. I tend to think of a ball spinning rapidly, stopping and changing direction, oscillating from one to the other or rotating about two axes. Were you to freeze a few frames in a video of the spinning ball you would catch it in one direction or the other, or catch it between states. This is the wrong model.

Spinning electrons do so in two directions simultaneously and with no intermediate states. This is the middle state of a qubit. In the case of a spinning electron it stays in that dual state until someone interferes to measure it. Then the spin is either up or down according to some probability.

A quantum computing microchip has circuits that exploit arrays of supercooled subatomic particles spinning in this controlled quantum state, but without extraneous electromagnetic interference or measurement, until monitored to record its state at that moment. â??Recordâ?• doesnâ??t do justice to the mechanism here, which under quantum logic is to both to measure and to create.

The state of an array of qubits is computationally interesting. 50 or so qubits connected each to the other provides an instantaneous parallel processing unit. The size of the array doesnâ??t impede the quantum calculation, and the computational power increases exponentially with the addition of extra qubit processing capability.

There are parallels here with chemical processes in which molecules interact without iteration as required in normal computer simulations. So biotech is one of the key areas motivating the development of quantum computing. That and security, fintec and the possibilities of a â??quantum internet.â?•

References

- Hossenfelder, Sabine. 2021. Donâ??t fall for quantum hype. *YouTube*, 6 February. Available online: <https://www.youtube.com/watch?v=b-aGlvUomTA&t=4s> (accessed 27 March 2021).
- Martin, Keith. 2020. *Cryptography: The Key to Digital Security, How It Works, and Why It Matters*. New York, NY: Norton
- Smith, Robert. 2018. Quantum Instruction Set â?? Computerphile. *Computerphile on Youtube*. Available online: <https://www.youtube.com/watch?v=ZN0lhYU1f5Q> (accessed 27 March 2021).

Note

- The image is an orrery on display in the Mus  e des Arts et M  tiers in Paris, September 2009.

Category

1. Architecture

Tags

1. cryptography
2. quantum computing

Date Created

March 27, 2021

Author

rcoyne99

default watermark