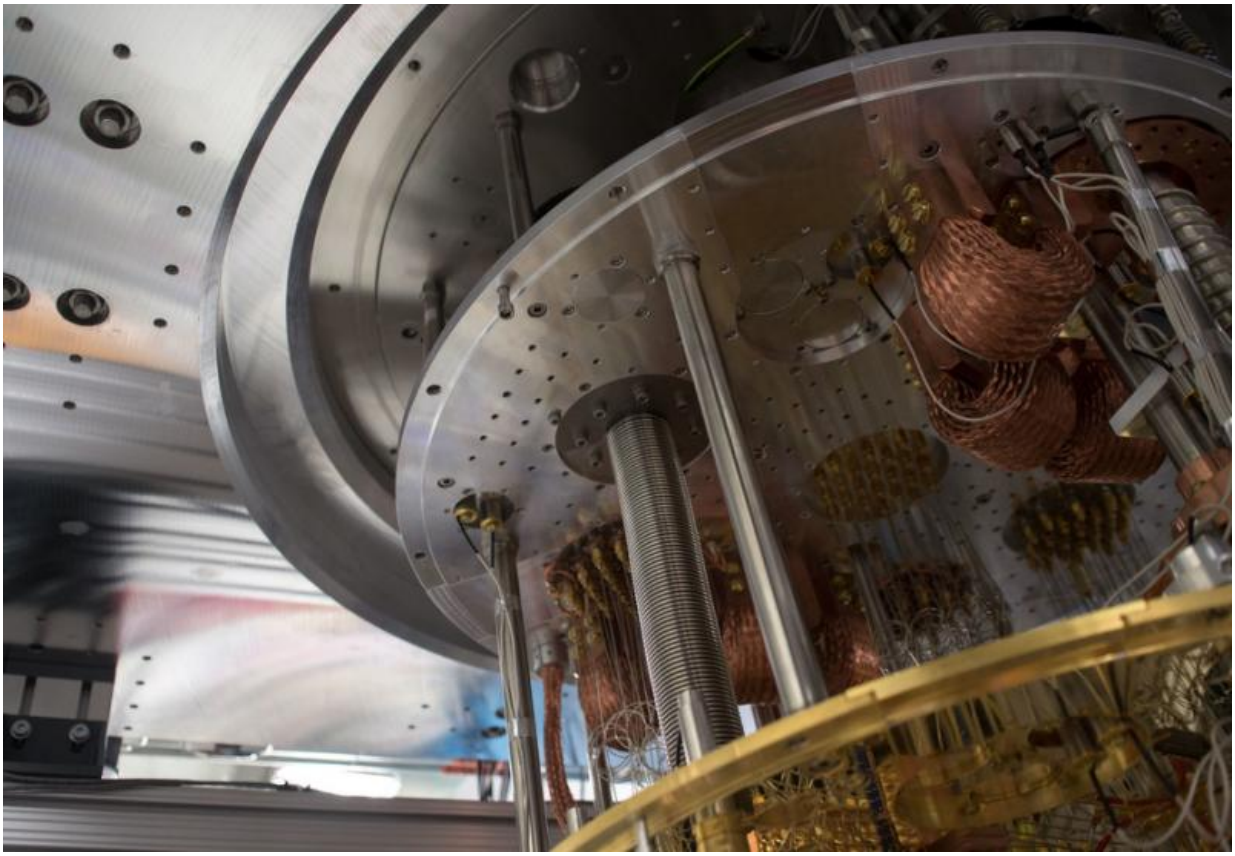
How quantum mechanics can change computing

August 24 2017, by Jonathan Katz



Looking inside a quantum computer. Credit: IBM Research, CC BY-ND

In early July, Google announced that it will expand its commercially available cloud computing services to include quantum computing. A similar service has been available from IBM since May. These aren't

services most regular people will have a lot of reason to use yet. But making quantum computers more accessible will help government, academic and corporate research groups around the world continue their study of the capabilities of quantum computing.

Understanding how these systems work requires exploring a different area of physics than most people are familiar with. From everyday experience we are familiar with what physicists call "classical mechanics," which governs most of the world we can see with our own eyes, such as what happens when a car hits a building, what path a ball takes when it's thrown and why it's hard to drag a cooler across a sandy beach.

Quantum mechanics, however, describes the subatomic realm – the behavior of protons, electrons and photons. The laws of quantum mechanics are very different from those of classical mechanics and can lead to some unexpected and counterintuitive results, such as the idea that an object can have negative mass.

Physicists around the world – in government, academic and corporate research groups – continue to explore real-world deployments of technologies based on quantum mechanics. And computer scientists, including me, are looking to understand how these technologies can be used to advance computing and cryptography.

A brief introduction to quantum physics

In our regular lives, we are used to things existing in a well-defined state: A light bulb is either on or off, for example. But in the quantum world, objects can exist in a what is called a superposition of states: A hypothetical atomic-level light bulb could simultaneously be both on and off. This strange feature has important ramifications for computing.

The smallest unit of information in classical mechanics – and, therefore,

classical computers – is the bit, which can hold a value of either 0 or 1, but never both at the same time. As a result, each bit can hold just one piece of information. Such bits, which can be represented as electrical impulses, changes in magnetic fields, or even a physical on-off switch, form the basis for all calculation, storage and communication in today's computers and information networks.

Qubits – quantum bits – are the quantum equivalent of classical bits. One fundamental difference is that, due to superposition, qubits can simultaneously hold values of both 0 and 1. Physical realizations of qubits must inherently be at an atomic scale: for example, in the spin of an electron or the polarization of a photon.

Computing with qubits

Another difference is that classical bits can be operated on independently of each other: Flipping a bit in one location has no effect on bits in other locations. Qubits, however, can be set up using a quantum-mechanical property called entanglement so that they are dependent on each other – even when they are far apart. This means that operations performed on one qubit by a quantum computer can affect multiple other qubits simultaneously. This property – akin to, but not the same as, parallel processing – can make quantum computation much faster than in classical systems.

Large-scale quantum computers – that is, quantum computers with hundreds of qubits – do not yet exist, and are challenging to build because they require operations and measurements to be done on a atomic scale. IBM's quantum computer, for example, currently has 16 qubits, and Google is promising a 49-qubit quantum computer – which would be an astounding advance – by the end of the year. (In contrast, laptops currently have multiple gigabytes of RAM, with a gigabyte being eight billion classical bits.)

A powerful tool

Notwithstanding the difficulty of building working quantum computers, theorists continue to explore their potential. In 1994, Peter Shor showed that quantum computers could quickly solve the complicated math problems that underlie all commonly used public-key cryptography systems, like the ones that provide secure connections for web browsers. A large-scale quantum computer would completely compromise the security of the internet as we know it. Cryptographers are actively exploring new public-key approaches that would be "quantum-resistant," at least as far as they currently know.

Interestingly, the laws of quantum mechanics can also be used to design cryptosystems that are, in some senses, more secure than their classical analogs. For example, quantum key distribution allows two parties to share a secret no eavesdropper can recover using either classical or quantum computers. Those systems – and others based on quantum computers – may become useful in the future, either widely or in more niche applications. But a key challenge is getting them working in the real world, and over large distances.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How quantum mechanics can change computing (2017, August 24) retrieved 25 April 2024 from https://phys.org/news/2017-08-quantum-mechanics.html