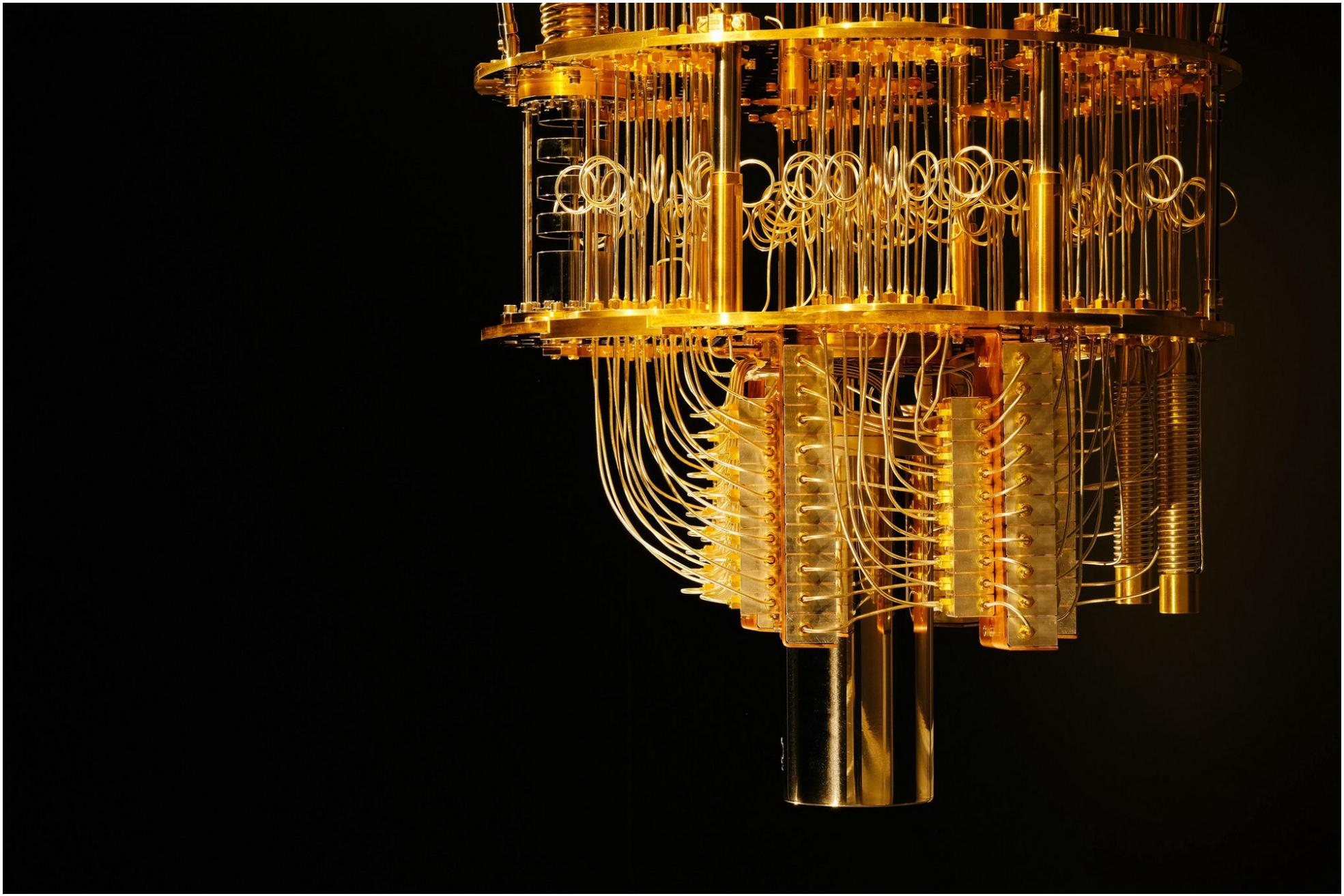
Quantum Computers Are Not What You Think

Ella Alderson Follow

Sep 23, 2018 · 5 min read



A dilution refrigerator, like this one from IBM, cools quantum chips down to low enough temperatures where superpositions and entanglement can occur without losing information.

For the last 50 years, our technology has been following what's known as Moore's Law—a law that tells us that computer power doubles about every 18 months. That is, we expect every new computer and smartphone to be more powerful than the one before it while also being smaller and sleeker in design. However, this isn't a trend that can continue forever. Some researchers even believe we're in the final years of this pattern as our progress in terms of computing power begins to level out. Physicist Michio Kaku suggests this will mean an end to the era of Silicon Valley and could cause a recession if we don't use new materials like graphene or implement tools like quantum computers to continue our progress.

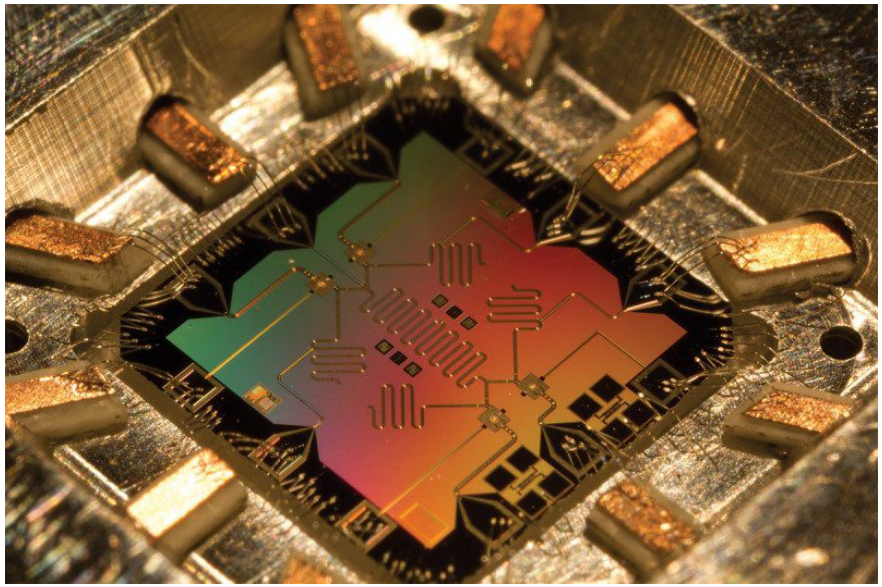
Before we get into quantum computing, here's a brief overview of how ordinary computers work: computer chips are made of basic modules which are made of logic gates which are, in turn, a combination of transistors. This is what the entire computer is—a series of simple steps coming together to create more complex processes. Transistors are electrical switches that work just like a lightbulb switch. They can either be open or closed, allowing or blocking electricity and information from coming through. These simple little components are essential for all our electronics and the great news is, the smaller we make them, the faster they'll be while consuming less energy. That's why transistors now are approaching the size of a single atom.

But there's a problem with this idea.

The billions of transistors in your laptop and smartphone today are about 14 nanometers or smaller (to get an idea of how small this is, the width of a single strand of your hair is about 100,000 nanometers), a number that's already very compact and impressive. But once transistors reach a small enough scale, they're prone to quantum tunneling. This means that when the transistors try to block the electrons from passing, those electrons could simply appear on the other side anyway. This leads to a lot more errors and noise which leads to more error correcting which requires more powerful processors and so on. The idea behind quantum computers is to take these phenomena of the quantum realm and use it to our advantage to create better machines.

In ordinary computers, information is encoded as bits which can be either a 1 or a 0. The more bits you have, the more complex your information can be. These 1's and 0's could come from a computer flipping the voltage in a circuit on or off. Instead of using bits, quantum computers use qubits (quantum bits which can be made using a photon, an electron, or a nucleus) that can be in a state of 1, 0, or a combination of the two. In what's known as superposition, qubits can be *in between* states. They could be said to be 30% 1 and 70% 0, for example. Qubits will only fall into a definite state if they've been observed.

This potential means that while classical bits can only be in 1 of 16 possible combinations, qubits could be all 16 of those combinations at the same time.



A superconducting qubit.

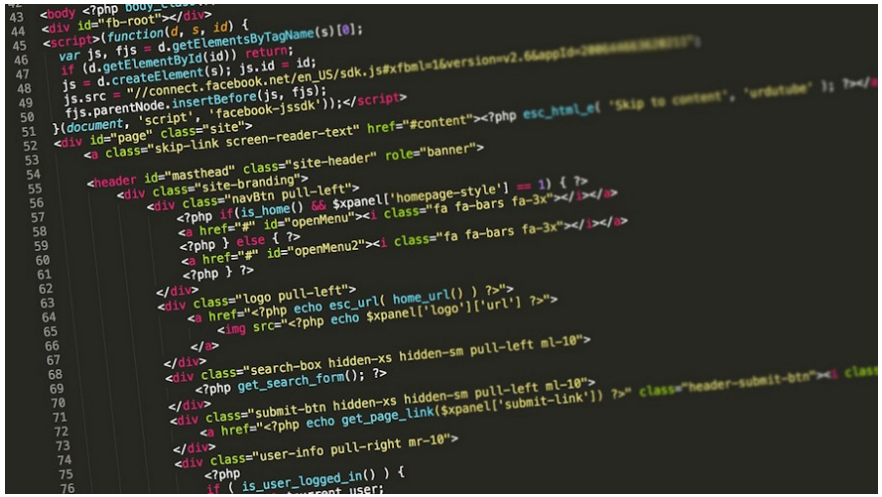
To put it another way, atoms spin up or down in a magnetic field. Spin up and that's 0, spin down and it's a 1. Now imagine spinning at a tilt. That ability to be in multiple states at once is the heart of superposition.

If simply observing these qubits changes them and causes a loss of information, you can imagine how sensitive they are. One of the problems with our quantum computers now is that quantum effects are extremely delicate. Heat, noise, and dust can all cause qubits to change their state of superposition so that they have to be shielded and run at very cold temperatures, sometimes only a few degrees warmer than absolute zero (–459.67°F). Researchers use resonators to see and read the state of qubits since resonators are much easier to interact with.

Other phenomena these computers use is quantum entanglement and interference. Entanglement is the famous "spooky action at a distance"

that Einstein spoke about. It's a connection between particles where changing one will immediately change its counterpart, no matter how big the distance between them. Interference is the ability to control quantum states to promote signals headed towards the right answer and cancel signals heading towards the wrong one, very similar to how noise cancelling headphones use precise waves to cancel out incoming noise waves, leaving only silence.

While all of this sounds—and is—very promising, many people believe quantum computers will be the answer to everything and will usher us into a new age of super advanced technology and futurism. The truth is, you're not even likely to have a quantum computer for personal use at all. They're only better than classical computers for very specific functions such as atomic bonding and database searches. These are problems ordinary computers find difficult to complete. In terms of modeling processes in nature, like photosynthesis, our computers can't do that at all because nature encodes its information in quantum mechanics. It takes a quantum machine to model quantum events.



Microsoft is already developing a new coding language that will integrate Python and C to allow for easier coding on the quantum computers.

Other uses for these computers will be mapping the human brain, simulating chemical bonding, analyzing large amounts of data, spotting patterns, modeling climate change, making transportation more efficient, and enabling progress in the field of artificial intelligence.

If a task required you to find one correct answer out of 100 million choices, an ordinary computer would go through 50 million steps to do so. A quantum computer would only go through 10,000. This is known as Grover's algorithm and it's an example of what quantum machines could do better.

We're facing a lot of the same challenges we took on when the first computers were being programmed as well as new challenges like coherence time—how long a qubit can retain information. Companies have also started taking security measures into question since quantum

computers could easily fly through the math underlying the encryption that secures our chats, social media, online stores, and banking.

For now, anyone without a quantum computer isn't missing out on anything. Quantum computers can't yet function any better than our classic computers can and aren't expected to do so for at least another decade.