How Google's Quantum Computer Could Change the World

The ultra-powerful machine has the potential to disrupt everything from science and medicine to national security—assuming it works

By Jack Nicas
October 16, 2017

Hartmut Neven believes in parallel universes. On a recent morning outside Google's Los Angeles office, the 53-year-old computer scientist was lecturing me on how quantum mechanics—the physics of atoms and particles—backs the theory of a so-called multiverse. Neven points to the tape recorder between us. What we're seeing is only one of the device's "classical configurations," he says. "But somewhere, not perceived by us right now, there are other versions." According to Neven, this is true for not just tape recorders but all physical objects. "Even for systems like you and me," he says. "There is a different configuration of all of us in a parallel universe."

Neven, who speaks with a thick German accent and favors pink Christian Louboutin sneakers covered in spikes, has led some of Google's most groundbreaking projects, from image-recognition software to Google Glass, a consumer flop that pioneered the idea of head-worn computers. The task in front of him is the most complex of his career: Build a computer based on the strange laws of quantum mechanics.

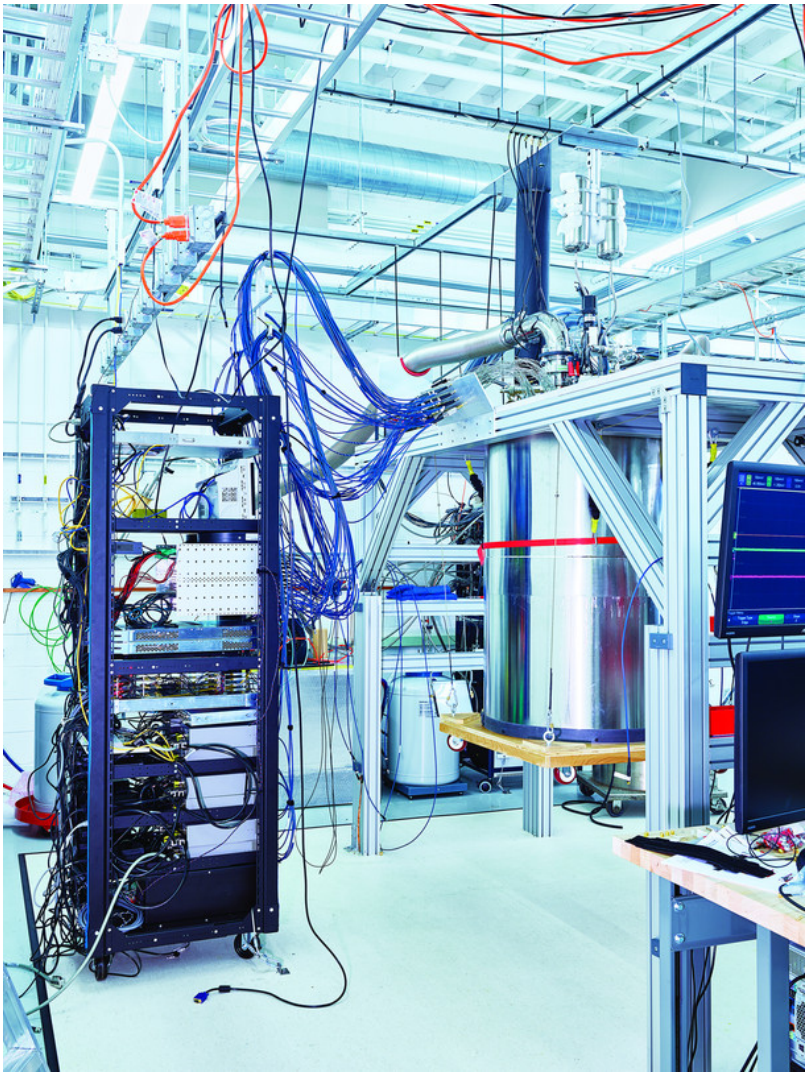
MORE FROM THE FUTURE OF EVERYTHING

- Meet the Man Fighting to Protect Your Secrets
- A Hardware Update for the Human Brain
- The Anti-Anxiety App

There is no quick explanation of quantum mechanics, but the Cliffs Notes version goes something like this: Scientists have proved that atoms can exist in two states at once, a phenomenon called superposition. A single atom, for example, can be in two locations at the same time.

Superposition gets even stranger as it scales. Because everything is made of atoms, some physicists theorize that entire objects can exist in multiple dimensions, allowing—as Neven suggested—for the possibility of parallel universes.

Even Albert Einstein couldn't get his head around this. The Nobel Prize-winning physicist declared the thinking behind quantum mechanics to be fundamentally flawed. Scientists have since proved the theory repeatedly and conclusively.



Inside Google's Santa Barbara, Calif. lab, where the company's delicate quantum chips sit frozen in a cryostat suspended off the floor. **PHOTO:** SPENCER LOWELL FOR THE WALL STREET JOURNAL

These laws are behind the next revolution in computing. In a small lab outside Santa Barbara, Calif., stocked with surfboards, wetsuits and acoustic guitars, Neven and two dozen Google physicists and engineers are harnessing quantum mechanics to build a computer of potentially astonishing power. A reliable, large-scale quantum computer could transform industries from AI to chemistry, accelerating machine learning and engineering new materials, chemicals and drugs.

"If this works, it will change the world and how things are done," says physicist Vijay Pande, a partner at Silicon Valley venture firm Andreessen Horowitz, which has funded quantum-computing start-up Rigetti Computing.

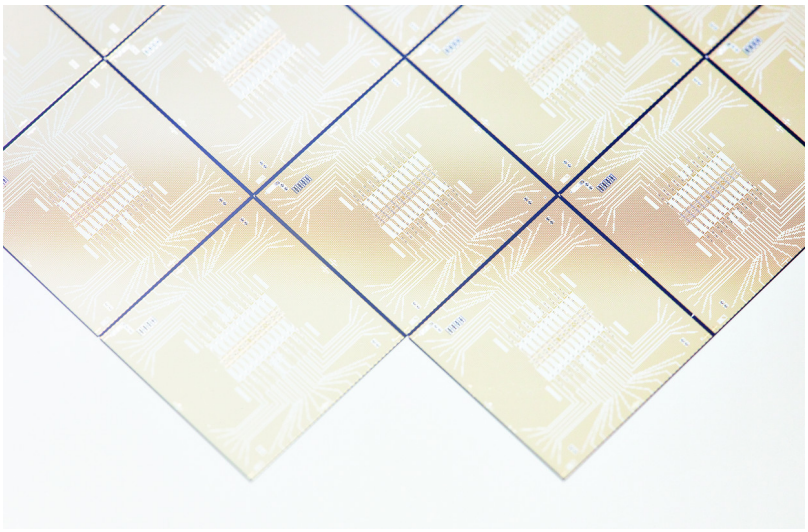
Others, especially those in academia, take a more nuanced view.

“It isn’t just a faster computer of the kind that we’re used to. It’s a fundamentally new way of harnessing nature to do computations,” says Scott Aaronson, the head of the Quantum Information Center at the University of Texas at Austin. “People ask, ‘Well, is it a thousand times faster? Is it a million times faster?’ It all depends on the application. It could do things in a minute that we don’t know how to do classically in the age of the universe. For other types of tests, a quantum computer probably helps you only modestly or, in some cases, not at all.”

For nearly three decades, these machines were considered the stuff of science fiction. Just a few years ago, the consensus on a timeline to large-scale, reliable quantum computers was 20 years to never.

“Nobody is saying never anymore,” says Scott Totzke, the chief executive of Isara Corp., a Canadian firm developing encryption resistant to quantum computers, which threaten to crack current methods. “We are in the very, very early days, but we are well past the science-fiction point.”

Companies and universities around the world are racing to build these machines, and Google, a unit of Alphabet Inc., appears to be in the lead. Early next year, Google’s quantum computer will face its acid test in the form of an obscure computational problem that would take a classical computer billions of years to complete. Success would mark “quantum supremacy,” the tipping point where a quantum computer accomplishes something previously impossible. It’s a milestone computer scientists say will mark a new era of computing, and the end of what you might call the classical age.



Google's 64-square-millimeter chips are currently the most advanced general-purpose quantum computers in the world.
PHOTO: SPENCER LOWELL FOR THE WALL STREET JOURNAL

Classical computers, like your laptop or phone, store and process information using bits, which have a value of either 1 or 0. Bits are represented by tiny electrical circuits called transistors that toggle between on (1) and off (0). To your iPhone, every finger tap, selfie and Rihanna hit is simply a long sequence of ones and zeros.

Quantum bits, or qubits, use superposition to exist in both states at once—effectively one and zero at the same time. In a classical computer, bits are like coins that display heads or tails. Qubits, on the other hand, are like coins spinning through the air in a coin toss, showing both sides at once.

That dynamism allows qubits to encode and process more information than bits do. So much more, in fact, that computer scientists say today's most powerful laptops are closer to abacuses than quantum computers. The computing power of a data center stretching several city blocks could theoretically be achieved by a quantum chip the size of the period at the end of this sentence.

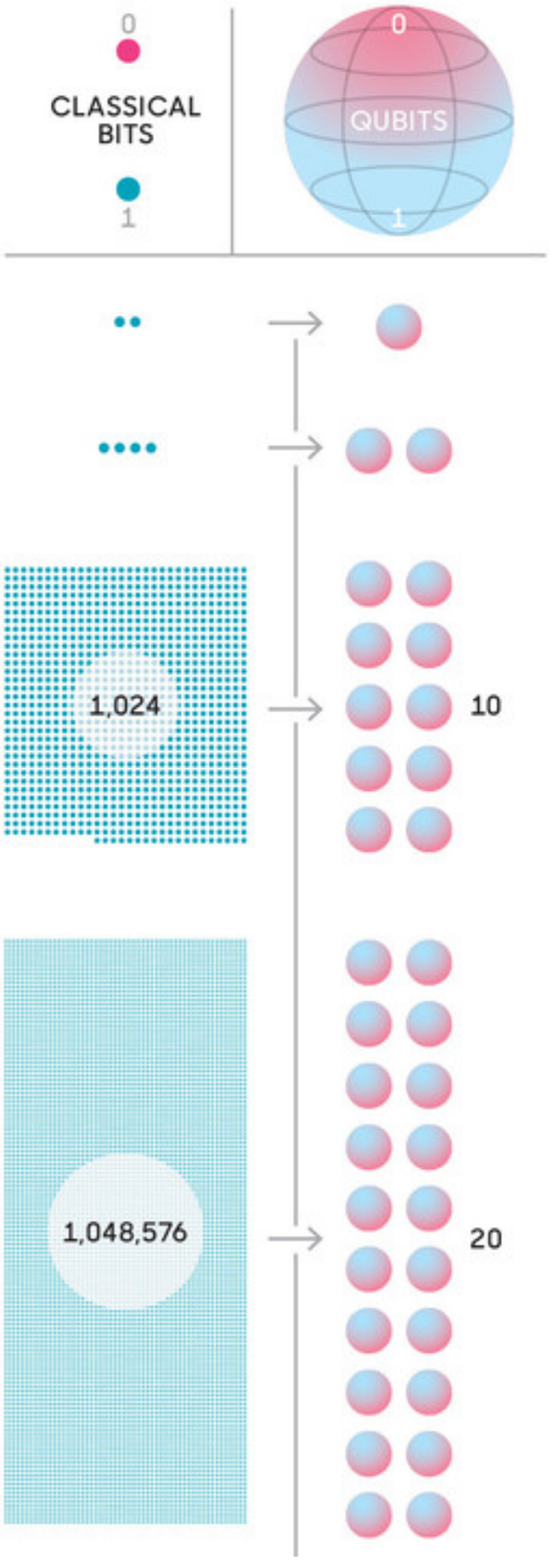
That potential is a result of exponential growth. Adding one bit negligibly increases a classical chip's computing power, but adding one qubit doubles the power of a quantum chip. A 300-bit classical chip could power (roughly) a basic calculator, but a 300-qubit chip has the computing power of two novemvigintillion bits—a two followed by 90 zeros—a number that exceeds the atoms in the universe.

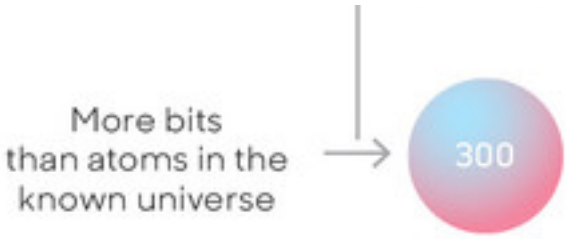
But this sort of comparison works only for specific computational tasks. Comparing bits to qubits is facile because quantum and classical computers are fundamentally different machines. Unlike classical computers, quantum computers don't test all possible solutions to a problem. Instead, they use algorithms to cancel out paths leading to wrong answers, leaving only paths to the right answer—and those algorithms work only for certain problems. This makes quantum computers unsuited for everyday tasks like surfing the web, so don't expect a quantum iPhone. But what they

QUANTUM VS. CLASSICAL COMPUTERS

Classical computers run on bits, units of information that are either one or zero. Quantum computers use qubits, which can be both one and zero at the same time. This allows qubits to process far more information than bits for specific tasks—particularly when combined. Each additional qubit doubles a quantum computer's power, and this exponential growth creates a dramitically more powerful machine at scale.

ILLUSTRATION: TODD DETWILER


0
CLASSICAL BITS
1
0
QUBITS
1
1,024
10
1,048,576
20



can do is tackle specific, unthinkably complex problems like simulating new molecules to engineer lighter airplane parts, more effective drugs and better batteries.

Quantum computers are also subject to high error rates, which has led some scientists and mathematicians to question their viability. Google and other companies say the solution is error-correction algorithms, but those algorithms require additional qubits to check the work of the qubits running computations. Some experts estimate that checking the work of a single qubit will require an additional 100.

Confused? You're in good company. In a recent interview with "WSJ. Magazine," Microsoft Corp. co-founder Bill Gates said the company's quantum-computing project is "the one part of Microsoft where they put up slides that I truly don't understand."

Richard Feynman, a Nobel Prize-winning theoretical physicist, put it this way: "I think I can safely say that nobody understands quantum mechanics."

Feynman was one of the first to introduce the idea of a quantum computer. In a 1981 lecture, he said simulating physics would require a computer based on nature or quantum mechanics. "Nature isn't classical, damn it," he said. "If you want to make a simulation of nature, you'd better make it quantum mechanical."

For the next two decades, researchers tried and failed to create the machines Feynman envisioned. Qubits proved extremely fragile and fickle. They could maintain superposition—the state that enables their massive computing power—for just a few nanoseconds, or billionths of a second. And an almost imperceptible temperature change or even a single molecule of air could knock them out of that state.

"It's a bit like trying to balance an egg at the end of a needle," IBM's quantum-computer scientist Jerry Chow said in a speech. "You certainly can do it, but any little disturbance from noise, from heat, from vibrations, and you've suddenly got yourself a sunny-side up."

In the past five years, scientists have made major progress on that balancing act. In response, investment has surged, with projects under way at Google, Microsoft, IBM and Intel Corp. , and interest from potential customers has followed.

Volkswagen AG is testing quantum computers made by Canadian firm D-Wave Systems Inc. In March, the companies said that, using GPS data from 10,000 taxis in Beijing, they created an algorithm to calculate the fastest routes to the airport while also minimizing traffic. A classical computer would have taken 45 minutes to complete that task, D-Wave said, but its quantum computer did it in a fraction of a second.

This makes it sound like D-Wave has won the race, but the company's $15 million 2000Q model is useful only for a narrow category of data analysis, which includes the Volkswagen test. While the 2000Q has 2,000 qubits—-a figure scientists warn shouldn't be compared with general-purpose quantum computers like Google's—the machine hasn't achieved quantum supremacy. D-Wave President Bo Ewald says the 2000Q isn't designed to get the best answer, but rather a "good enough answer in a short period of time."

Not everyone is eager for large-scale, accurate quantum computers to arrive. Everything from credit-card transactions to text messaging is encrypted using an algorithm that relies on factorization, or reverse multiplication. An enormous number—several hundred digits long—acts as a lock on encrypted data, while the number's two prime factors are the key. This so-called public-key cryptography is used to protect health records, online transactions and vast amounts of other sensitive data because it would take a classical computer years to find those two prime factors. Quantum computers could, in theory, do this almost instantly.

Companies and governments are scrambling to prepare for what some call Y2Q, the year a large-scale, accurate quantum computer arrives, which some experts peg at roughly 2026. When that happens, our most closely guarded digital secrets could become vulnerable.

The NSA warns that code-breaking quantum computers could be "devastating" to national security

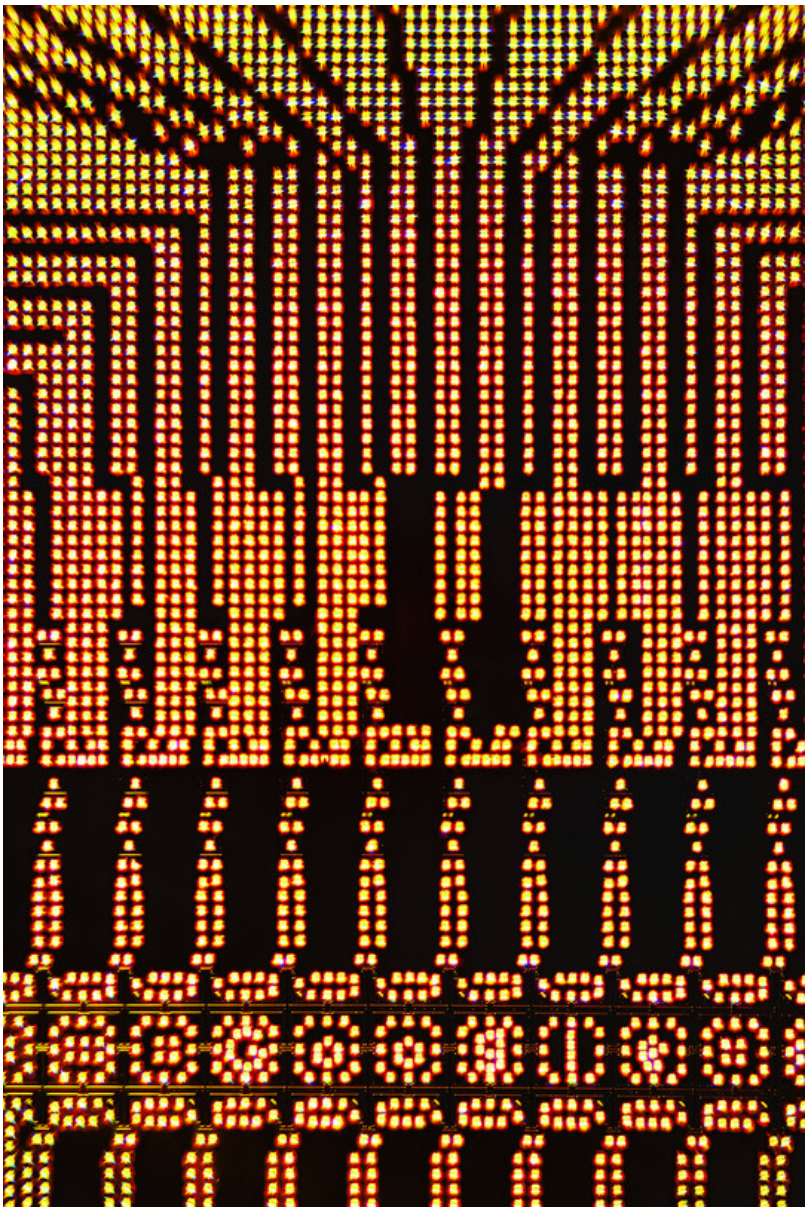
Last year the National Security Agency issued an order that U.S. national-security employees and vendors must, "in the not-too-distant future," begin overhauling their encryption to guard against the threat posed by quantum computers. Because national-security information must be protected for decades, the agency says new encryption needs to be in place before these machines arrive. Otherwise, the NSA warns, code-breaking quantum computers would be "devastating" to national security.

Governments aren't just playing defense. Documents leaked by former NSA contractor Edward Snowden in 2013 showed that the NSA is building its own quantum computer as part of an $80 million research program called Penetrating Hard Targets, according to the Washington Post. It's unclear how far the NSA has gotten in its quest. The agency declined to comment.

The primary impetus in the race for quantum computers is the potential to upend industries. Experts believe their biggest near-term promise is to supercharge machine learning and AI, two

rapidly growing fields—and businesses. Neven of Google says he expects all machine learning to be running on quantum computers within the decade.

This commercial race heated up considerably earlier this year. In May, IBM unveiled a chip with 16 qubits, a milestone for general-purpose quantum computers. The day before, a trade group published an interview with John Martinis, Google's head of quantum hardware, in which he let slip that Google had a 22-qubit chip.



A look under the microscope at Google's 64-square-millimeter chip reveals a sly bit of branding: the company's name spelled out along the bottom. PHOTO: SPENCER LOWELL FOR THE WALL STREET JOURNAL

Today Google's chips sit frozen inside elaborate vats called cryostats in the company's Santa Barbara lab, a laid-back outpost of the quantum project led by Neven in Los Angeles. With its ping-pong table and assorted bongos, the space feels like an extension of the nearby University of California, Santa Barbara campus. Martinis, who runs the office, is a physics professor at UCSB,

and many of his hires are graduates. Staff meetings are occasionally interrupted by the resident lab dog, a Papillon-Pomeranian mix named Qubit.

On a recent afternoon, Daniel Sank and Amit Vainsencher, two laid-back engineers with mops of curly hair and recent Ph.D.s from UCSB, led me to a gleaming cryostat in one corner of the lab. Because particles lose superposition with the slightest interference, quantum computers must be radically isolated from the outside world. The cryostat's mu-metal exterior, a soft magnetic alloy that blocks the Earth's magnetic field, was adorned with a single bumper sticker: "My other computer is classical."

Compressed helium and liquid nitrogen, pumped from an adjacent frost-covered tank, cool the inside of the cryostat to minus 459.6 degrees Fahrenheit, a fraction of a degree above the lowest temperature possible, which enables the conductivity necessary for Google's qubits to run computations. "If you were to vibrate this frame, you can actually see the temperature rise on the thermometer," Vainsencher says before shaking the structure that suspends the cryostat above the ground to limit interference from vibration. "I probably shouldn't do that," he says.

Such a complex and expensive setup means that Google and its peers will likely sell quantum computing via the cloud, possibly charging by the second.

For now, Neven's team in Southern California is racing to finish the 49-qubit chip that they hope will carry them to quantum supremacy and into a new frontier of technology, where computers leverage unthinkably complex natural laws rather than converting the world into ones and zeros.

"There is no transistor in this computer," Neven says. "It's a completely different beast. It's a native citizen of the multiverse."