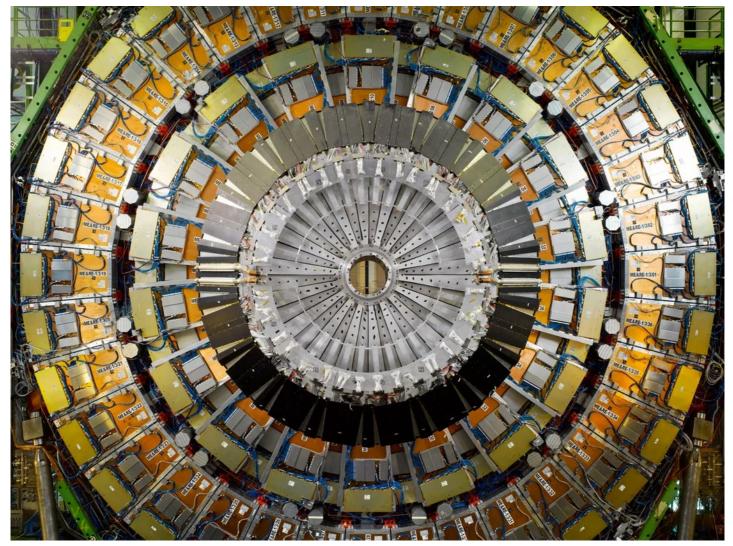
Quantum computers could help explain some of the most fundamental mysteries in the universe and upend everything from finance to encryption—if only someone could get them to work.



VIEW PICTURES/GETTY IMAGES

Deep beneath the Franco-Swiss border, the Large Hadron Collider is sleeping. But it won't be quiet for long. Over the coming years, the world's largest particle accelerator will be supercharged, increasing the number of proton collisions per second by a factor of two and a half. Once the work is complete in 2026, researchers hope to unlock some of the most fundamental questions in the universe. But with the increased power will come a deluge of data the likes of which high-energy physics has never seen before. And, right now, humanity has no way of knowing what the collider might find.

To understand the scale of the problem, consider this: When it shut down in December 2018, the LHC generated about 300 gigabytes of data every second, adding up to 25 petabytes (PB) annually. For comparison, you'd have to spend 50,000 years listening to music to go through 25 PB of MP3 songs, while the human brain can store memories equivalent to just 2.5 PB of binary data. To make sense of all that information, the LHC data was

pumped out to 170 computing centers in 42 countries. It was this global collaboration that helped discover the elusive Higgs boson, part of the Higgs field believed to give mass to elementary particles of matter.

WIRED UK

This story originally appeared on WIRED UK.

To process the looming data torrent, scientists at the European Organization for Nuclear Research, or CERN, will need 50 to 100 times more computing power than they have at their disposal today. A proposed Future Circular Collider, four times the size of the LHC and 10 times as powerful, would create an impossibly large quantity of data, at least twice as much as the LHC.

In a bid to make sense of the impending data deluge, some at CERN are turning to the emerging field of quantum computing. Powered by the very laws of nature the LHC is probing, such a machine could potentially crunch the expected volume of data in no time at all. What's more, it would speak the same language as the LHC. While numerous labs around the world are trying to harness the power of quantum computing, it is the future work at CERN that makes it particularly exciting research. There's just one problem: Right now, there are only prototypes; nobody knows whether it's actually possible to build a reliable quantum device.

Traditional computers—be it an Apple Watch or the most powerful supercomputer—rely on tiny silicon transistors that work like on-off switches to encode bits of data. Each circuit can have one of two values—either one (on) or zero (off) in binary code; the computer turns the voltage in a circuit on or off to make it work.

A quantum computer is not limited to this "either/or" way of thinking. Its memory is made up of quantum bits, or qubits—tiny particles of matter like atoms or electrons. And qubits can do "both/and," meaning that they can be in a superposition of all possible combinations of zeros and ones; they can be all of those states simultaneously.

For CERN, the quantum promise could, for instance, help its scientists find evidence of supersymmetry, or SUSY, which so far has proven elusive. At the moment, researchers spend weeks and months sifting through the debris from proton-proton collisions in the LCH, trying to find exotic, heavy sister-particles to all our known particles of matter. The quest has now lasted decades, and a number of physicists are questioning if the theory behind SUSY is really valid. A quantum computer would greatly speed up analysis of the collisions, hopefully finding evidence of supersymmetry much sooner—or at least allowing us to ditch the theory and move on.

A quantum device might also help scientists understand the evolution of the early universe, the first few minutes after the Big Bang. Physicists are pretty confident that back then, our universe was nothing but a strange soup of subatomic particles called quarks and gluons. To understand how this quark-gluon plasma has evolved into the universe we have today, researchers simulate the conditions of the infant universe and then test their models at the LHC, with multiple collisions. Performing a simulation on a quantum computer, governed by the same laws that govern the very particles that the LHC is smashing together, could lead to a much more accurate model to test.

ADVERTISEMENT

Beyond pure science, banks, pharmaceutical companies, and governments are also waiting to get their hands on computing power that could be tens or even hundreds of times greater than that of any traditional computer.

And they've been waiting for decades. Google is in the race, as are IBM, Microsoft, Intel and a clutch of startups, academic groups, and the Chinese government. The stakes are incredibly high. Last October, the European Union pledged to give \$1 billion to over 5,000 European quantum technology researchers over the next decade, while venture capitalists invested some \$250 million in various companies researching quantum computing in 2018 alone. "This is a marathon," says David Reilly, who leads Microsoft's quantum lab at the University of Sydney, Australia. "And it's only 10 minutes into the marathon."

Despite the hype surrounding quantum computing and the media frenzy triggered by every announcement of a new qubit record, none of the competing teams have come close to reaching even the first milestone, fancily called *quantum supremacy*—the moment when a quantum computer performs at least one specific task better than a standard computer. Any kind of task, even if it is totally artificial and pointless. There are plenty of rumors in the quantum community that Google may be close, although if true, it would give the company bragging rights at best, says Michael Biercuk, a physicist at the University of Sydney and founder of quantum startup Q-CTRL. "It would be a bit of a gimmick—an artificial goal," says Reilly "It's like concocting some mathematical problem that really doesn't have an obvious impact on the world just to say that a quantum computer can solve it."

That's because the first real checkpoint in this race is much further away. Called *quantum advantage*, it would see a quantum computer outperform normal computers on a truly useful task. (Some researchers use the terms quantum supremacy and quantum advantage interchangeably.) And then there is the finish line, the creation of a universal quantum computer. The hope is that it would deliver a computational nirvana with the ability to perform a broad range of incredibly complex tasks. At stake is the design of new molecules for life-saving drugs, helping banks to adjust the riskiness of their investment portfolios, a way to break all current cryptography and develop new, stronger systems, and for scientists at CERN, a way to glimpse the universe as it was just moments after the Big Bang.

Slowly but surely, work is already underway. Federico Carminati, a physicist at CERN, admits that today's quantum computers wouldn't give researchers anything more than classical machines, but, undeterred, he's started tinkering with IBM's prototype quantum device via the cloud while waiting for the technology to mature. It's the latest baby step in the quantum marathon. The deal between CERN and IBM was struck in November last year at an industry workshop organized by the research organization.

Set up to exchange ideas and discuss potential collaborations, the event had CERN's spacious auditorium packed to the brim with researchers from Google, IBM, Intel, D-Wave, Rigetti, and Microsoft. Google detailed its tests of Bristlecone, a 72-qubit machine. Rigetti was touting its work on a 128-qubit system. Intel showed that it was in close pursuit with 49 qubits. For IBM, physicist Ivano Tavernelli took to the stage to explain the company's progress.

IBM has steadily been boosting the number of qubits on its quantum computers, starting with a meagre 5-qubit computer, then 16- and 20-qubit machines, and just recently showing off its 50-qubit processor. Carminati listened to Tavernelli, intrigued, and during a much needed coffee break approached him for a chat. A few minutes later, CERN had added a quantum computer to its impressive technology arsenal. CERN researchers are now starting

to develop entirely new algorithms and computing models, aiming to grow together with the device. "A fundamental part of this process is to build a solid relationship with the technology providers," says Carminati. "These are our first steps in quantum computing, but even if we are coming relatively late into the game, we are bringing unique expertise in many fields. We are experts in quantum mechanics, which is at the base of quantum computing."

ADVERTISEMENT

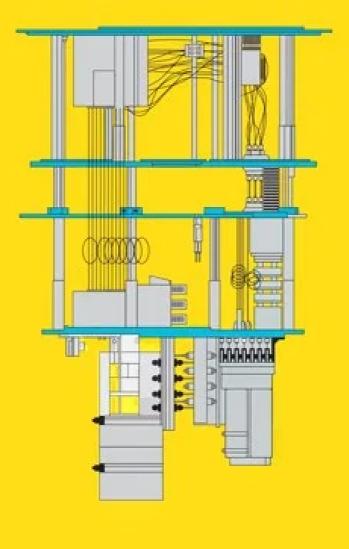
The attraction of quantum devices is obvious. Take standard computers. The prediction by former Intel CEO Gordon Moore in 1965 that the number of components in an integrated circuit would double roughly every two years has held true for more than half a century. But many believe that Moore's law is about to hit the limits of physics. Since the 1980s, however, researchers have been pondering an alternative. The idea was popularized by Richard Feynman, an American physicist at Caltech in Pasadena. During a lecture in 1981, he lamented that computers could not really simulate what was happening at a subatomic level, with tricky particles like electrons and photons that behave like waves but also dare to exist in two states at once, a phenomenon known as quantum superposition.

Feynman proposed to build a machine that could. "I'm not happy with all the analyses that go with just the classical theory, because nature isn't classical, dammit," he told the audience back in 1981. "And if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

And so the quantum race began. Qubits can be made in different ways, but the rule is that two qubits can be both in state A, both in state B, one in state A and one in state B, or vice versa, so there are four probabilities in total. And you won't know what state a qubit is at until you measure it and the qubit is yanked out of its quantum world of probabilities into our mundane physical reality.

In theory, a quantum computer would process all the states a qubit can have at once, and with every qubit added to its memory size, its computational power should increase exponentially. So, for three qubits, there are eight states to work with simultaneously, for four, 16; for 10, 1,024; and for 20, a whopping 1,048,576 states. You don't need a lot of qubits to quickly surpass the memory banks of the world's most powerful modern supercomputers—meaning that for specific tasks, a quantum computer could find a solution much faster than any regular computer ever would. Add to this another crucial concept of quantum mechanics: entanglement. It means that qubits can be linked into a single quantum system, where operating on one affects the rest of the system. This way, the computer can harness the processing power of both simultaneously, massively increasing its computational ability.

LEARN MORE



The WIRED Guide to Quantum Computing

While a number of companies and labs are competing in the quantum marathon, many are running their own races, taking different approaches. One device has even been used by a team of researchers to analyze CERN data, albeit not at CERN. Last year, physicists from the California Institute of Technology in Pasadena and the University of Southern California managed to replicate the discovery of the Higgs boson, found at the LHC in 2012, by sifting through the collider's troves of data using a quantum computer manufactured by D-Wave, a Canadian firm based in Burnaby, British Columbia. The findings didn't arrive any quicker than on a traditional computer, but, crucially, the research showed a quantum machine could do the work.

One of the oldest runners in the quantum race, D-Wave announced back in 2007 that it had built a fully functioning, commercially available 16-qubit quantum computer prototype—a claim that's controversial to this day. D-Wave focuses on a technology called quantum annealing, based on the natural tendency of real-world quantum systems to find low-energy states (a bit like a spinning top that inevitably will fall over). A D-Wave quantum computer imagines the possible solutions of a problem as a landscape of peaks and valleys; each coordinate represents a possible solution and its elevation represents its energy. Annealing allows you to set up the problem,

and then let the system fall into the answer—in about 20 milliseconds. As it does so, it can tunnel through the peaks as it searches for the lowest valleys. It finds the lowest point in the vast landscape of solutions, which corresponds to the best possible outcome—although it does not attempt to fully correct for any errors, inevitable in quantum computation. D-Wave is now working on a prototype of a universal annealing quantum computer, says Alan Baratz, the company's chief product officer.

ADVERTISEMENT

Apart from D-Wave's quantum annealing, there are three other main approaches to try and bend the quantum world to our whim: integrated circuits, topological qubits and ions trapped with lasers. CERN is placing high hopes on the first method but is closely watching other efforts too.

IBM, whose computer Carminati has just started using, as well as Google and Intel, all make quantum chips with integrated circuits—quantum gates—that are superconducting, a state when certain metals conduct electricity with zero resistance. Each quantum gate holds a pair of very fragile qubits. Any noise will disrupt them and introduce errors—and in the quantum world, noise is anything from temperature fluctuations to electromagnetic and sound waves to physical vibrations.

To isolate the chip from the outside world as much as possible and get the circuits to exhibit quantum mechanical effects, it needs to be supercooled to extremely low temperatures. At the IBM quantum lab in Zurich, the chip is housed in a white tank—a cryostat—suspended from the ceiling. The temperature inside the tank is a steady 10 millikelvin or –273 degrees Celsius, a fraction above absolute zero and colder than outer space. But even this isn't enough.

Just working with the quantum chip, when scientists manipulate the qubits, causes noise. "The outside world is continually interacting with our quantum hardware, damaging the information we are trying to process," says physicist John Preskill at the California Institute of Technology, who in 2012 coined the term quantum supremacy. It's impossible to get rid of the noise completely, so researchers are trying to suppress it as much as possible, hence the ultracold temperatures to achieve at least some stability and allow more time for quantum computations.

"My job is to extend the lifetime of qubits, and we've got four of them to play with," says Matthias Mergenthaler, an Oxford University postdoc student working at IBM's Zurich lab. That doesn't sound like a lot, but, he explains, it's not so much the number of qubits that counts but their quality, meaning qubits with as low a noise level as possible, to ensure they last as long as possible in superposition and allow the machine to compute. And it's here, in the fiddly world of noise reduction, that quantum computing hits up against one of its biggest challenges. Right now, the device you're reading this on probably performs at a level similar to that of a quantum computer with 30 noisy qubits. But if you can reduce the noise, then the quantum computer is many times more powerful.

Once the noise is reduced, researchers try to correct any remaining errors with the help of special error-correcting algorithms, run on a classical computer. The problem is, such error correction works qubit by qubit, so the more qubits there are, the more errors the system has to cope with. Say a computer makes an error once every 1,000 computational steps; it doesn't sound like much, but after 1,000 or so operations, the program will output incorrect results. To be able to achieve meaningful computations and surpass standard computers, a quantum machine has to have about 1,000 qubits that are relatively low noise and with error rates as corrected as possible. When you

put them all together, these 1,000 qubits will make up what researchers call a logical qubit. None yet exist—so far, the best that prototype quantum devices have achieved is error correction for up to 10 qubits. That's why these prototypes are called noisy intermediate-scale quantum computers (NISQ), a term also coined by Preskill in 2017.

For Carminati, it's clear the technology isn't ready yet. But that isn't really an issue. At CERN the challenge is to be ready to unlock the power of quantum computers when and if the hardware becomes available. "One exciting possibility will be to perform very, very accurate simulations of quantum systems with a quantum computer—which in itself is a quantum system," he says. "Other groundbreaking opportunities will come from the blend of quantum computing and artificial intelligence to analyze big data, a very ambitious proposition at the moment, but central to our needs."

ADVERTISEMENT

But some physicists think NISQ machines will stay just that—noisy—forever. Gil Kalai, a professor at Yale University, says that error correcting and noise suppression will never be good enough to allow any kind of useful quantum computation. And it's not even due to technology, he says, but to the fundamentals of quantum mechanics. Interacting systems have a tendency for errors to be connected, or correlated, he says, meaning errors will affect many qubits simultaneously. Because of that, it simply won't be possible to create error-correcting codes that keep noise levels low enough for a quantum computer with the required large number of qubits.

"My analysis shows that noisy quantum computers with a few dozen qubits deliver such primitive computational power that it will simply not be possible to use them as the building blocks we need to build quantum computers on a wider scale," he says. Among scientists, such skepticism is hotly debated. The blogs of Kalai and fellow quantum skeptics are forums for lively discussion, as was a recent much-shared article titled "The Case Against Quantum Computing"—followed by its rebuttal, "The Case Against the Case Against Quantum Computing.

For now, the quantum critics are in a minority. "Provided the qubits we can already correct keep their form and size as we scale, we should be okay," says Ray Laflamme, a physicist at the University of Waterloo in Ontario, Canada. The crucial thing to watch out for right now is not whether scientists can reach 50, 72, or 128 qubits, but whether scaling quantum computers to this size significantly increases the overall rate of error.