EDWIN CARTLIDGE

Quantum Com

Industry has joined the race to build a universal quantum comput

But the task is daunting.

Optical setup used by Ronald Hanson and colleagues at the Delft University of Technology, Netherlands, to manipulate spin qubits.

Frank Auperlé

puting

HOW CLOSE ARE WE?

er.

In June 2015, the European Telecommunications Standards Institute (ESTI) warned organizations needing to archive information or protect online transaction privacy for more than ten years to switch to "quantum-safe" encryption techniques. The institute's announcement highlighted the threat posed by future quantum computers, which someday could, in principle, be used to calculate the prime factors of large integers and so break the encryption of sensitive data on the internet.

The ESTI warning is just one of several signs that the long-promised era of quantum computing may finally be at hand. High-tech giants such as Google, Intel and IBM have either started or beefed up research on quantum computing in the last few years. The United Kingdom and the European Union, meanwhile, have announced major programs—worth £270 million and €1 billion, respectively—to develop and commercialize quantum technologies.

> Are quantum computers just around the corner, or a much more distant prospect? The answer depends in part on what is meant by the term "quantum computer."

Sir Peter Knight of Imperial College London, OSA's 2004 president and a key mover behind the U.K. initiative, argues that recent tech industry interest in quantum computing is well-founded. He says that quantum circuitry is nearing a point at which it can be scaled up to make powerful devices, and estimates that the first useful quantum computer might appear a decade from now. "This is the first time that we have been optimistic that we can do something on a reasonable timescale," he says.

Yet today's quantum computers remain technological minnows for now; after three decades of research on the subject, they have at most about a dozen bits and can do no better than calculate the prime factors of 21. Indeed, quantum physicist Thomas Konrad of the University of KwaZulu-Natal in South Africa holds that the ability to scale up to hundreds of bits is still an open question. "Some people claim that with the right control, everything can behave quantum mechanically," he says. "But as long as you don't show me, that is just speculation."

So are quantum computers really just around the corner, or a much more distant prospect? The answer depends in part on what is meant by the term "quantum computer." A "universal" quantum computer would be one capable of carrying out any quantum algorithm much more quickly than the best classical computer, at least for large problems. Experts agree that the technical challenges in building such a machine remain enormous—but not insurmountable.

Complex devices

Information in a classical computer is represented using bits that can exist in one of two states: 0 or 1. Quantum bits, or qubits, on the other hand, can represent 0, 1, or 0 and 1 at the same time, thanks to the quantum-mechanical property of superposition. And the fact that qubits can be entangled with one another means that N of them can in principle process 2^N states simultaneously, making such a computer exponentially faster than a classical device.

Yet quantum computers are extremely complex. Qubits must first be encoded using the quantum states of particular physical objects, such as the spin of electrons or atomic nuclei. The qubits are then manipulated via quantum logic gates consisting of laser beams, microwaves, electric fields or other probes, designed to evolve the system's wavefunction in a well-defined way such that, upon measurement, there's a high probability that the wavefunction will collapse to the classical state corresponding to the right answer for the algorithm in question.

Among the algorithms developed to date are one for factorization put forward by Peter Shor in 1995, and another for searching databases proposed by Lov Grover a year later . However, the complexities of quantum physics mean that devising new algorithms is a tricky business.

Actually building a quantum computer is tougher still. Qubits must be manipulated, yet simultaneously protected from the tiniest external sources of heat or electromagnetic radiation, which would destroy their fragile

1047-6938/16/10/30/8-$15.00 ©OSA

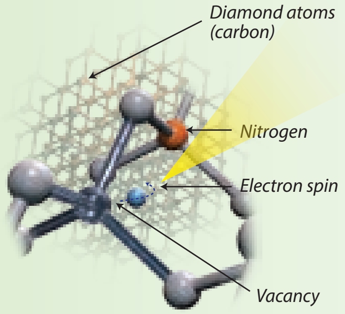
superposition in a process known as decoherence. Striking that delicate balance requires error correction, which involves adding extra bits to cross-check the values of others. But qubits' states cannot simply be copied, since copying causes decoherence. Instead, the information they contain must be "spread out" among many other qubits. These extra qubits can also decohere, so adding them to the quantum system can actually increase the system's vulnerability to outside interference.

All of this imposes a fault-tolerance threshold on a given error correction scheme—a maximum frequency of errors that the computer can encounter when operating on qubits, such that adding more qubits doesn't make it more likely for the algorithm to give the wrong answer. "If you are below the threshold then error correction is beneficial," explains Ronald Hanson, a physicist at the Delft University of Technology in the Netherlands. "Otherwise, errors will accumulate faster and faster, and you won't be able to do anything useful".

The earliest error-correction schemes, introduced about 20 years ago, Hanson says, had very high thresholds; they could tolerate only about one error in every million operations, whereas the best hardware made an error about once every ten operations. But then theorists devised a new scheme, topological error correction, that is based on the topological structure of clusters of qubits rather than individual qubits, and that reduced the fault-tolerance threshold to about one operation in a hundred. At the same time, the fidelity of actual gates has increased by about a factor of ten. As a result, physicists are now "extremely confident," Hanson says, that quantum computing is feasible.

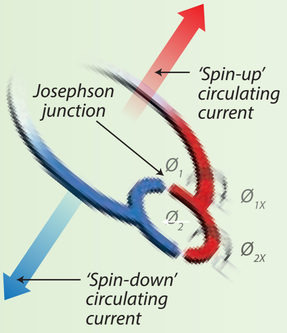
Four routes to quantum computing

Physicists are developing different flavors of quantum computer, based on different types of quantum bits (qubits).



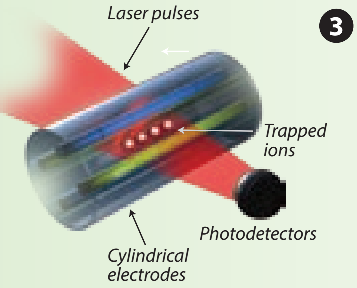
1 Spin qubits

Made from spins of electrons or nuclei trapped in a solid substrate, such as nitrogen vacancy centers in diamond. Can remain in superposition states for up to several seconds and can be compatible with current chip-manufacturing technology. Noise from solid-state environment could hamper scaling up.



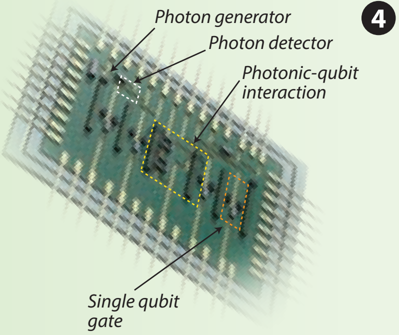
2 Superconducting circuits

Superpositions of currents flowing in opposite directions around a superconductor at the same time. Being solid state, they are potentially easy to manufacture, but have relatively short coherence times and require low temperatures to operate.



3 Ion traps

Qubits reside in arrays of ions trapped in electric fields, with their quantum states manipulated by lasers. Very clean systems that don't suffer from defects, allowing for logic gates with low error rates—but scaling up will require new fabrication infrastructure.



4 Photonic circuits

Qubits are encoded in the quantum states of photons travelling around circuits in silicon chips, which include etched waveguides and tiny linear optical components. Need for qubit redundancy could be minimized by photons' resistance to interference, but building photonic logic gates is difficult, and single-photon sources pose a technical challenge.

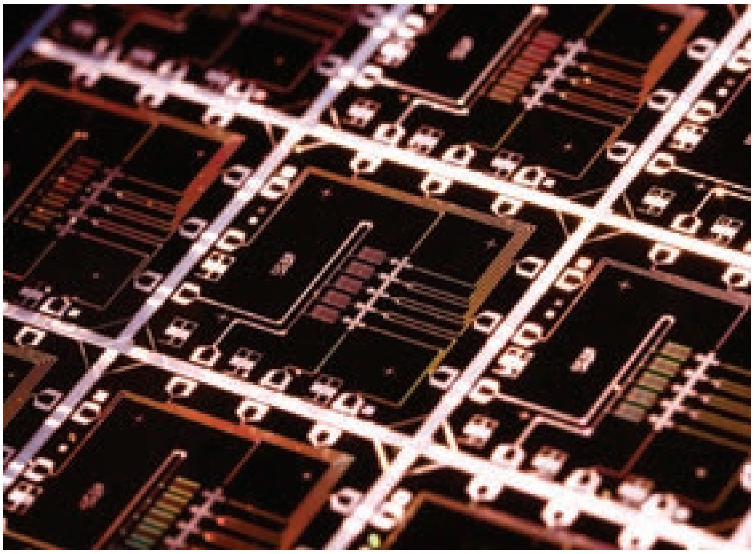
Illustration by Phil Saunders

The prospect of being able to scale up quantum computers into useful devices without errors "cascading out of control" has attracted industry to the field.

On the threshold

Hanson's group in Delft is one of several around the world that creates qubits using the spins of electrons or nuclei within single atoms, ions or molecules embedded in a solid substrate. The Dutch researchers encode qubits in the spin of electrons that are trapped by so called nitrogen vacancy centers in diamond—point defects in the diamond's rigid lattice of carbon atoms where a nitrogen atom has been substituted. The group can maintain the superposition states of electrons for hundreds of milliseconds, and entangle them using radio waves and lasers.

Hanson says that the team can now control five of these so-called spin qubits "pretty reliably," with a gate fidelity slightly below 99 percent when averaged across single-qubit, readout and two-qubit gates. The latter—which include controlled-NOT gates that flip one qubit depending on the value of the other, and which can be combined to create more complex three- and four-qubit gates—are the trickiest to bring under control, and currently have fidelities between 95 and 99 percent.


Arrays of five superconducting qubits made by John Martinis and colleagues at the University of California, Santa Barbara, USA. The researchers were able to carry out operations on these qubits at the fault-tolerance threshold needed for error correction.

Erik Lucero

John Martinis and colleagues at the University of California, Santa Barbara (UCSB), USA, meanwhile, have obtained a two-qubit gate fidelity of up to 99.4 percent using aluminium-on-sapphire superconducting circuits. They encode qubits using the direction of current flow, creating superposition states when current travels in both directions at the same time. They achieved their high fidelities in 2014 by bringing one qubit's oscillation frequency into and out of resonance with that of its neighbour, and followed that up last year with nine-qubit error correction.

Physicists believe that scaling up to a commercially viable qubit technology will require gate fidelities at least an order of magnitude higher than the 99 percent threshold, or the number of physical qubits needed to provide error correction for each logical qubit will become prohibitive. This past June, David Lucas and colleagues at the University of Oxford, U.K., reported a gate fidelity of just that—99.9 percent—using qubits made from laser-cooled trapped ^{43}Ca ions.

Industry steps in

The prospect of being able to scale up quantum computers into useful devices without errors "cascading out of control," as Knight puts it, has attracted industry to the field. In 2014, Google hired Martinis to build a working quantum computer based on his team's superconducting technology. And last year, Intel announced it was investing US$50 million to collaborate on spin qubit technology with co-workers of Hanson at Delft. IBM, meanwhile, has pursued the superconducting option for many years, and made a five-qubit processor available online in May. Microsoft, too, has joined the fray.

So far, industry has largely thrown its weight behind solid-state technology. Daniel Loss, a theorist at the University of Basel, Switzerland, who pioneered the concept of spin qubits, says this makes sense, as semiconductor quantum chips have the dual advantage of being potentially very compact and also compatible with current chip-production technology. Indeed, physicists at the University of New South Wales in Sydney, Australia, are developing a semiconductor device involving spin qubits made from phosphorous atoms embedded in a silicon substrate, in which qubits can reportedly remain in a superposition for up to 30 seconds. Meanwhile, other groups are developing semiconductor chips for photonic quantum computers—devices that could have advantages over matter-based computers, but that also pose major challenges (see box at right).

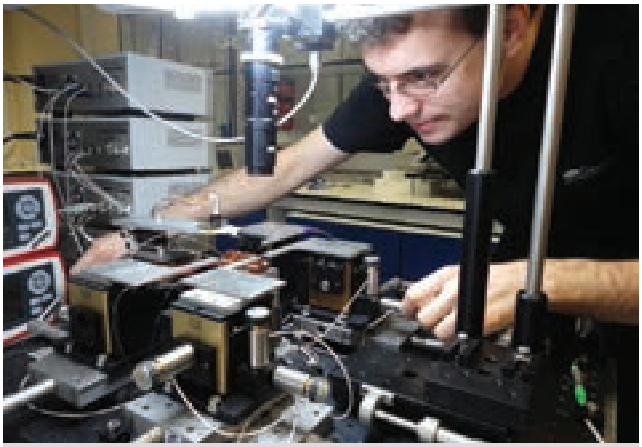
Christopher Monroe of the University of Maryland, USA, who works with trapped ions, believes the potential of semiconductor devices has been overstated. He says that silicon-based quantum computing is several years behind rival schemes, and argues that noise and defects generated by qubits' solid-state environment will get much worse as systems are scaled up. Industry, he maintains, has a "huge blind spot" when it comes to alternatives to silicon.

Silicon chips will feature in ion-trap computers—but as electrodes to suspend up to a few hundred ions, rather than housing millions or even billions of gates as with today's integrated circuits. Monroe envisions linking these chips together using light to create much larger processors, a modular approach also suited to spin qubits. He acknowledges that continually shuttling data between modules will eat up processing power, but believes that quantum circuitry is too complex to allow a whole processor to be built on a single chip. "You are dead if you try that," he says.

Football-field size

The ultimate aim of all this scaling up is to build a full-sized universal quantum computer, which will require an enormous number of qubits. In 2012, Martinis, along with UCSB colleagues Matteo Mariantoni and Andrew Cleland, as well as Austin Fowler, then at the University of Melbourne, Australia, calculated how many qubits would be needed to carry out Shor's factoring algorithm on a 2,000-bit number in around a day. (That's a task far beyond the reach of today's best supercomputers, but is commonly cited as a problem that quantum machines would make tractable.) Their answer: about 10,000 logical qubits—each of which would need about 13,000 physical qubits to perform error correction. Overall, therefore, the calculation would require a whopping 130 million qubits.

Scaling up to that size presents many technical hurdles. According to Hanson, these include how to connect up all of the various subsystems, given that each qubit must be addressed individually. For spin qubits and trapped ions,



Jeremy O'Brien, Damien Bonneau (pictured) and colleagues at the University of Bristol use silicon chips to implement optical quantum computing. QET Labs

What about photons?

In some ways, photons are ideal for making qubits. In particular, the fact that photons don't interact with one another under normal circumstances means that a superposition state of, say, a photon's spin could be immune to decoherence by stray electromagnetic fields. That suggests a need for far less error correction than for a computer based on matter qubits.

Unfortunately, the photons' lack of mutual interaction is also a big problem for creating two-qubit logic gates, which, like their classical equivalents, are non-linear devices that require qubit carriers to interact with one another. One way to get around this is to use matter as an intermediary between two sets of photons. This approach has been explored since the 1990s, but according to Michael Raymer, an optical physicist at the University of Oregon, it is slow, bulky and hard to scale up.

In 2001 Raymond Laflamme, then at Los Alamos National Laboratory, and collaborators put forward an alternative, when they showed theoretically how linear optical devices could in effect be used to carry out nonlinear operations, thanks to the fact that photons are bosons. When two photons enter a 50-percent-reflecting beam splitter from opposite sides at the same time they will always leave the device along the same path, and this sticking together constitutes a kind of interaction.

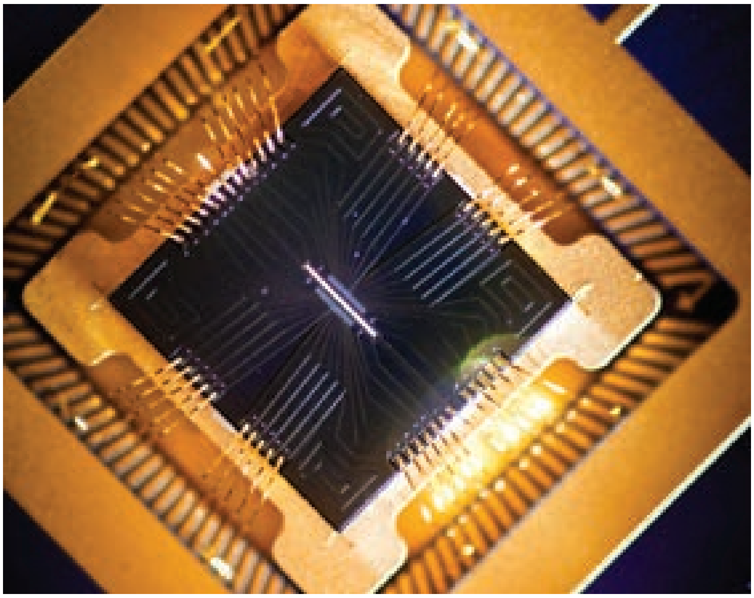
Jeremy O'Brien and colleagues at the University of Bristol, U.K., are pursuing a modern version of this scheme. They etch waveguides in and add tiny analogues of traditional linear optical components to millimeter-sized silicon chips. Group member Nic Harrigan says that the main challenges they face are in engineering, such as how to replace the external sources of single photons that they currently use with chip-mounted ones.

Raymer believes that suitable single-photon sources—such as quantum dots or atoms in optical cavities—can probably be found. But another problem, he believes, could prove insurmountable: the fact that photonic gates give the right output no more than half the time (since photon pairs have an equal probability of exiting a beam splitter to the left or right). That means, he says, that large computers would require prohibitive numbers of redundant qubits. "As in classical information technology, many experts think light will be used for communication, but not for large-scale computing," he says.

With universal computers still a long way off, physicists are building more specialized devices known as quantum simulators, which are designed specifically to model quantum systems.

he says, there is the question of how to supply the necessary laser beams, and whether these lasers can all be extracted from a single master beam. For superconducting circuits, meanwhile, a significant headache will be cooling qubits down to the required millikelvin temperatures. Andreas Wallraff, who works on this technology at ETH Zurich in Switzerland, is confident that this problem can be overcome, but acknowledges that linking each of the numerous cold qubits to room-temperature control electronics will be tricky. “Moving from systems of ten or so qubits to ones containing thousands or millions of qubits will be predominately a large engineering challenge,” he says.

A universal quantum computer would also be physically enormous. According to Monroe, the equipment needed to run a single trapped-ion chip—25 stable power supplies and a high-voltage radiofrequency source for each of the chip’s electrodes, plus lasers—currently fills a small room. In future this volume could shrink to less than a cubic meter, but, as he points out, that would still mean “a football field of these things” (give or take an order of magnitude or two) to build a full-scale quantum computer. And, Wallraff reckons, the bill for constructing such a full-fledged universal device might come in at around US$10 billion, roughly what Intel currently needs for a next-generation chip fab.



A silicon electrical trap made at Sandia National Laboratories, USA, used to capture ions in work at the University of Maryland and other institutions.

Sandia National Laboratories

So when might such a device actually be built? Many researchers believe that more than a decade will be needed, but as to how much more they are reluctant to say. Some, such as Wallraff, speculate that perhaps 20 years is nearer the mark; others are more cautious still. For that reason, Martinis believes that quantum computers pose no imminent threat to internet security. “No one,” he says, “is going to be building a quantum computer in their garage overnight.”

Computing in the real world

With universal computers still a long way off, physicists are building more specialized devices known as quantum simulators, which are designed specifically to model quantum systems but can’t carry out other types of algorithms. Quantum simulators that can outperform today’s best supercomputers might need only 50 to 100 qubits, having little or no need for error correction, and could model, say, the behavior of small molecules—something potentially useful in developing new drugs. According to Hanson, such devices might become reality in the next decade.

Before that, some groups are planning to carry out what are known as “quantum supremacy experiments.” Martinis’ group at Google hopes, within the next two years, to use 40 or 50 superconducting qubits to run an algorithm that is of no practical use (it will compute the equivalent of the speckle pattern generated when a laser beam passes through frosted glass), but that would show a quantum computer doing something that a classical computer can’t. Such a system could, Martinis believes, “make clear to the computing and electronics industries that there is real power to quantum computing."

In a similar vein, several groups around the world are investigating so-called boson sampling. This involves working out the probability that a certain set of photons entering a series of parallel input ports, and then interfering with one another as they travel through an array of waveguides, will generate a particular set of photons in a parallel set of output ports. The amount of classical computing power needed to work out the answer scales exponentially with the input, and becomes prohibitive for more than about 20 photons, according to Knight, who says that one or more groups might reach this point in the next three years.

In fact, a claim already exists for machines that can do things not possible with classical computers. The Canadian company D-Wave has created computers that contain an impressive-sounding 1,000 superconducting qubits. Rather than using gates, which allow individual qubits to be fully controlled, the D-Wave "adiabatic" computers work by keeping all of their qubits in the lowest energy state and then slowly varying three parameters of the system as a whole until the final, desired state emerges. The idea is to find the minimum value of a certain function, which D-Wave claims could be applied to problems such as minimizing risk in financial portfolios or reducing energy loss on an electrical grid.

The company's initial 16-qubit version, unveiled in 2007 as the "world's first commercially viable quantum computer," met with skepticism; some scientists doubted that it behaved quantum mechanically at all. Those doubts were assuaged to some extent four years later when the company reported observations of specific quantum phenomena in its machine, and D-Wave has sold a number of its machines for several million dollars apiece, to clients including Lockheed Martin and Google.

However, in 2014 an independent group of scientists, including Martinis, found no evidence that the computer could solve optimization problems any quicker, on average, than a classical device. Other researchers also remain to be convinced. Konrad, for one, says he doesn't really understand what is going on under the hood of the D-Wave device—but he does believe that the approach of developing machines specifically to tackle optimization problems is promising.

Engineers required

Even though universal quantum computers could still be decades away, and doubts continue to surround some current technology, scientists are excited about quantum computing's recent change in outlook. According to Martinis, "there is a lot more talk now about building actual computing machines." And Monroe notes that "now there is a big push in the community to apply engineering." That, he says, "means building something that doesn't need a bunch of Ph.D. students to run it … That is happening in the field right now."

Even Konrad is enthusiastic. He feels that quantum computers' potential has been exaggerated in the past, but believes that has helped attract interest and funding to the field. As a result, he argues, science and technology could go in unexpected directions, no matter when, or even if, a universal quantum computer gets built. "Like Columbus, who wanted to get to India but ended up discovering America," he says, "someone will find something if they are serious about searching." OPN

D-Wave's machine is said to use quantum mechanics to carry out certain operations more quickly than a classical computer, though the claims have proved controversial.

D-Wave Systems Inc.

Edwin Cartlidge (edwin.cartlidge@yahoo.com) is a freelance science journalist based in Rome.

References and Resources

- E. Knill et al. Nature **409**, 46 (2001).
- R. Raussendorf and J. Harrington. Phys. Rev. Lett. **98**, 150504 (2007).
- A.G. Fowler et al. https://arxiv.org/abs/1208.0928 (2012).
- R. Barends et al. Nature **508**, 500 (2014).
- T.F. Rønnow et al. Science **345**, 420 (2014).
- C.J. Ballance et al. Phys. Rev. Lett. **117**, 060504 (2016).