

TECHNOLOGY QUARTERLY HERE, THERE AND EVERYWHERE

Quantum technology is beginning to come into its own

1

After decades as laboratory curiosities, some of quantum physics' oddest effects are beginning to be put to use, says Jason Palmer

PATRICK GILL, a director of the new Quantum Metrology Institute at Britain's National Physical Laboratory (NPL) in south-west London and an expert in atomic clocks, points to a large table full of lenses and mirrors, vacuum chambers and electronics. "And there's a smaller one over there," he says.

NPL is part of a consortium of the planet's official

timekeepers. In all its atomic-clock laboratories, each of the flagship devices—some of which are huge—is flanked by a smaller one under construction. Miniaturisation is the name of the game. Here is one that fits into a standard electronics rack, 19 inches wide. Over there is a fist-sized gizmo designed to hold an atomic clock's precious innards safe within a satellite.

The caesium atomic clock, developed at NPL, was arguably the world's first quantum technology, though it was not labelled as such. The most common approach, first used in 1950, works by putting energy into atoms to create a “superposition” in which they are, in a measurable way, in more than one energy state at the same time—both excited and relaxed. Probing this strange condition reveals the “clock frequency” of those atoms—a constant for clocks on every continent, and the basis for a precise, internationally agreed definition of the second.

After decades of work in the laboratory, a raft of different devices and approaches relying on quantum-mechanical effects are now nearing market-readiness. It has taken so long mainly because the components that make them up had to be developed first: ever-better lasers,

semiconductors, control electronics and techniques to achieve the low temperatures at which many quantum systems perform best.

Britain did not exploit the atomic clock's discovery in the market. Instead, a year after the device was invented, it was commercialised by the National Company, an American firm. Given the potential of these new quantum technologies, this time commercialisation is on many minds. The NPL's ever-smaller clocks are just one step towards marketable products that could vastly outdo GPS (which itself is an application of atomic timekeeping) in navigation, or help spot what lies underground. The era of quantum technology is almost here.

The odds are good; the goods, odd

Everything in the natural world can be described by quantum mechanics. Born a century ago, this theory is the rule book for what happens at atomic scales, providing explanations for everything from the layout of the periodic table to the zoo of particles spraying out of atom-smashers. It has guided the development of everyday technologies from lasers to MRI machines and put a solid foundation under astrophysicists' musings about unknowables such as the interiors of black holes and the dawn of the

universe. Revealed by a few surprising discoveries, such as that atoms absorb and emit energy only in packets of discrete sizes (quanta), and that light and matter can act as both waves and particles, it is modern physics' greatest triumph.

It has a weird side, though, and it is this that has captured interest in what is now being called the second quantum revolution. The first one was about physics: about understanding how the world worked at the tiny scales where quantum mechanics rules. Not only can particles be in two states at once, as with the atoms in an atomic clock; sometimes two of them, separated by a great distance, seemingly sense something about each other's condition, a situation called entanglement. A particle's exact position or state is never certain until a measurement is made; there are only higher or lower likelihoods of a given outcome, and the measurement changes the situation irrevocably. All this has been clear from the mathematics since the mid-1920s but was made manifest in laboratory experiments only later in the 20th century. As the theory's more straightforward predictions were put to use, for instance in electronics, quantum mechanics gained a reputation for being counterintuitive, even downright spooky.

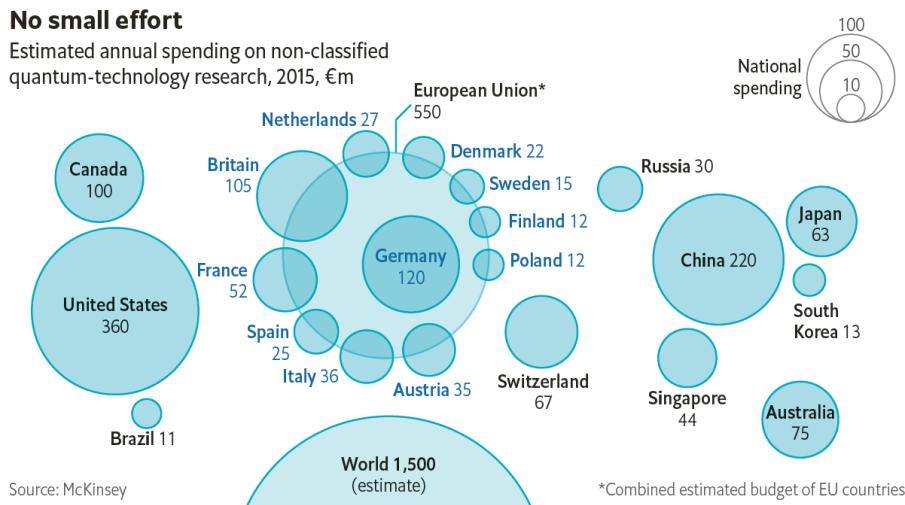
The expertise gained during those years is now paying dividends. The most counterintuitive quantum-mechanical predictions are being harnessed to make measurements of staggering precision, to generate uncrackable codes and to form the basis of impenetrable communications networks. Quantum computers may eventually crunch through currently unapproachable problems, improving the transmission of electric power or the manufacture of energy-intensive fertiliser, or simply sifting through impractically large data sets.

However, long before then computing systems that still fall far short of a general-purpose machine are likely to start providing solutions in industries such as finance, energy and aerospace, and even help with things as mundane as recommendation engines.

From small beginnings

Much work remains to be done. Although a handful of quantum-enabled sensors, modest quantum networks and rudimentary quantum computers are already in use, they still fall short of fully exploiting quantum advantages, and few of them are ready to be widely deployed. According to McKinsey, a consulting firm, in 2015 about 7,000 people worldwide, with a combined budget of about

\$1.5bn, were working on quantum-technology research (see chart). Industrialisation will boost those numbers.



What is notable about the effort now is that the challenges are no longer scientific but have become matters of engineering. The search is on for smaller atomic clocks, for example; for a means to amplify and route quantum-communications signals; and for more robust “qubits” (of which more later) for quantum computing. Startups are embracing the technology with gusto, and tech giants have already planted their flags. There is wide agreement that Google is furthest along in quantum-computer technology and that Microsoft has the most comprehensive plan to make the software required.

Public money is flowing in, too. National and

supranational funding bodies are backing increasingly ambitious quantum-technology efforts. Britain has a programme worth £270m (\$337m) and the European Union has set aside €1bn (\$1.08bn) for a pan-European programme. Many quantum technologies have security implications, so defence departments are also providing funding.

Many firms are already preparing for a quantum-technology future. In 2015 IBM set up its Research Frontiers Institute, inviting corporate participants to share ideas about growth areas in technology, the quantum kind being one. The research fund of AXA, a big insurer, has endowed a professorship in quantum information at the Institute of Photonic Sciences in Barcelona to consider the data-privacy risks presented by the coming quantum boom.

Quantum technology looks set quickly to find its way into all manner of products and services—mostly behind the scenes, as artificial intelligence has recently done. It may be weird, but it promises to be wonderful too.

Metrology: Sensing sensibility

2

Quantum technology's supersensitivity makes it great for measuring
SINCE its inception a century ago, quantum physics

has faced something of an experimental problem. The theory promises all manner of interesting and perhaps useful behaviours of particles in isolation, under rigidly controlled conditions. But on the lab bench particles and atoms are never fully isolated, so quantum experiments can be damnably difficult.

However, that difficulty also presents an opportunity for quantum technology: sensing. “We turn that on its head,” says Sir Peter Knight, a British quantum expert. “If it couples to the outside world so effectively, it’s sensing the outside world really effectively.” Take the first quantum technology to make it to market, the atomic clock. Most designs work by tapping into the energy levels of atoms that are prodded with microwaves. Some of those atoms absorb the light in such a way that they are neither in their unperturbed, lowest-energy state nor in an elevated-energy state but in both at the same time, an effect that is central to quantum mechanics. An improved design “entangles” these microwave levels in one atom with different energy levels in another—levels that correspond to visible light, which has a much higher frequency. Such entanglement, another quantum effect, links the fates of two atoms, temporarily but inextricably, so that experiments on one yield information about the

other. Entangling microwave levels with higher-frequency ones associated with visible light allows the clock to access the higher precision that goes with them. In 2012 David Wineland, of NIST, the American national metrology facility, received a Nobel prize for working out how to do this. For some years, his clock was the most accurate measuring device on Earth: had it been set ticking at the time of the Big Bang, 13.8bn years ago, it would still be accurate to within a second.

Precise timing, particularly from the small, cheap devices that are now being developed, has a wealth of uses, from time-stamping high-frequency market trades to quickly changing settings within a dynamic energy grid. Even lifting an atomic clock up can change how long a tick appears to take: according to the general theory of relativity, time moves ever so slightly more slowly closer to the Earth than further away. Nuisance or opportunity? It's all relative. A well-calibrated atomic clock could use this discrepancy to make an ultra-precise height measurement. Or, at a fixed height, it could sense the gravitational attraction of what is below; solid bedrock would give a different reading from an oil-and-gas pocket.



Precise
timing has a
wealth of uses

Laws of attraction

Clocks are not the only means to get a handle on gravity. At the microscopic scales where quantum mechanics rules, streams of matter particles can behave like waves. Like those on a pond's surface, those waves can interfere, adding to and subtracting from one another—in the quantum description, altering the probability of finding a particle here or there. In a device called an atom interferometer, two particle streams are sent at differing heights and then brought back together to interfere with each other. The degree to which the two paths are different, indicating the relative strength of the gravitational tug from below, measurably alters the degree of addition and subtraction.

Such devices have a multitude of uses. In Britain, for example, 4m holes are dug every year in the course of roadworks and construction, but two-thirds of the time the diggers have no idea what they will find beneath the surface. Test boreholes cover only a small area, and ground-penetrating radar does not reach deep enough. A gravity sensor that could tell pipework from pebbles would save a lot of trouble.

RSK, an environmental consultancy involved in cleaning up brownfield sites and the like, reckons that a third of construction projects overrun by up to

a month, and another third by two months or more, and that half of these delays arise because of underground surprises. The company is collaborating with the University of Birmingham in Britain on fieldworthy quantum gravity sensors, in the hope of deploying them in big infrastructure projects. Other efforts to develop cheap sensors have drawn interest from companies such as Schlumberger, an oilfield-services giant, and Bridgeporth, a surveying firm.

Military types are interested, too. “You can’t shield gravity,” says David Delpy, who leads the Defence Scientific Advisory Council in Britain’s defence ministry. Improved gravity sensors would be able to spot moving masses under water, such as submarines or torpedoes, which could wipe out the deterrent effect of French and British nuclear submarines. Quantum gravimeters could precisely map geological features from the gravitational force they induce. That would help with getting around in places where satellite-navigation signals are not available—“a kind of Google Maps for gravitation”, as Dr Delpy puts it.

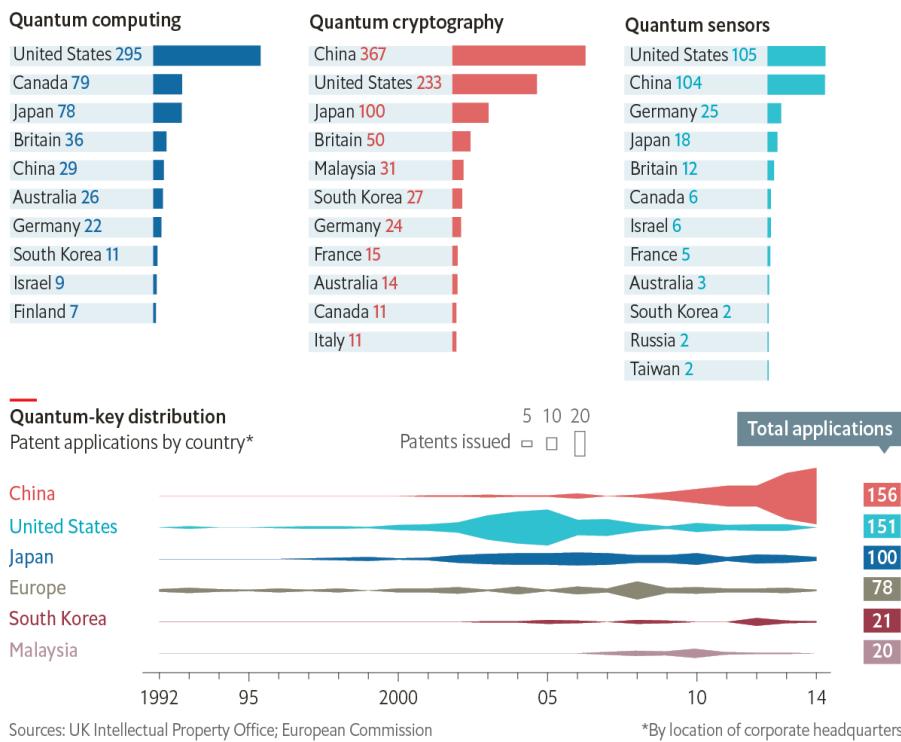
And gravity, the theory of relativity also says, is just one manifestation of acceleration: a good gravimeter is a good accelerometer. And a good

accelerometer is a good vibration sensor. Once they are small enough and good enough, all these high-precision devices will be of great interest to carmakers, and in particular to the autonomous-vehicle industry, the success of which will depend on accurate sensing of the movements of cars and their surroundings. Bosch, a German firm that is the world's largest maker of automotive components and a supplier to many other industries, already has its eye on quantum-technological enhancements to its products.

Michael Bolle, the firm's head of research and development, believes sensors will be quantum technology's first market success. "I'm not talking about niche markets," he says. "I'm interested in the trigger point where things really go into mass production." Quantum technologists the world over are preparing for this market explosion by patenting their findings. In some countries, such as Japan and Australia, quantum sensors make up a large part of national patent portfolios (see chart).

Excited states

Patent applications to 2015, in:



Mr Bolle and others are also interested in sensors based on “nitrogen vacancies”—places where a diamond’s all-carbon network has been disrupted by one nitrogen atom next to a missing carbon atom. This is a quantum physicist’s playground: mostly isolated by its rigid cage of carbon neighbours from the bumpy, fluctuating world outside, electrons from the nitrogen atoms can be easily manipulated and measured, placed in superpositions and even entangled with one another. Just like the hypersensitive clock, these systems are extraordinarily responsive to their environment and can act as precise sensors of pressure, temperature and electric current.

Where they have shown the most promise is in measuring magnetic fields. Recent studies show that nitrogen vacancies can detect the on-and-off magnetic field of single nerve cells. The same principles can work inside the human body, too. Nanoscale diamonds with nitrogen vacancies have been used to spot chemical changes in living cells, and researchers from the Institute of Theoretical Physics and the Institute of Quantum Physics in Ulm, Germany, have formed NVision, a startup that uses such nanodiamonds to match the current best magnetically enhanced MRI techniques, but 40 times faster and at a quarter of the cost.

High performance in these applications depends on well-understood nitrogen vacancies, which occur sporadically in natural diamonds but whose positions and number must be known for precision measurement. Enter Element Six (a subsidiary of DeBeers, the world's largest diamond producer), which manufactures diamonds with precision-engineered nitrogen vacancies.

Capture the friendly ghost

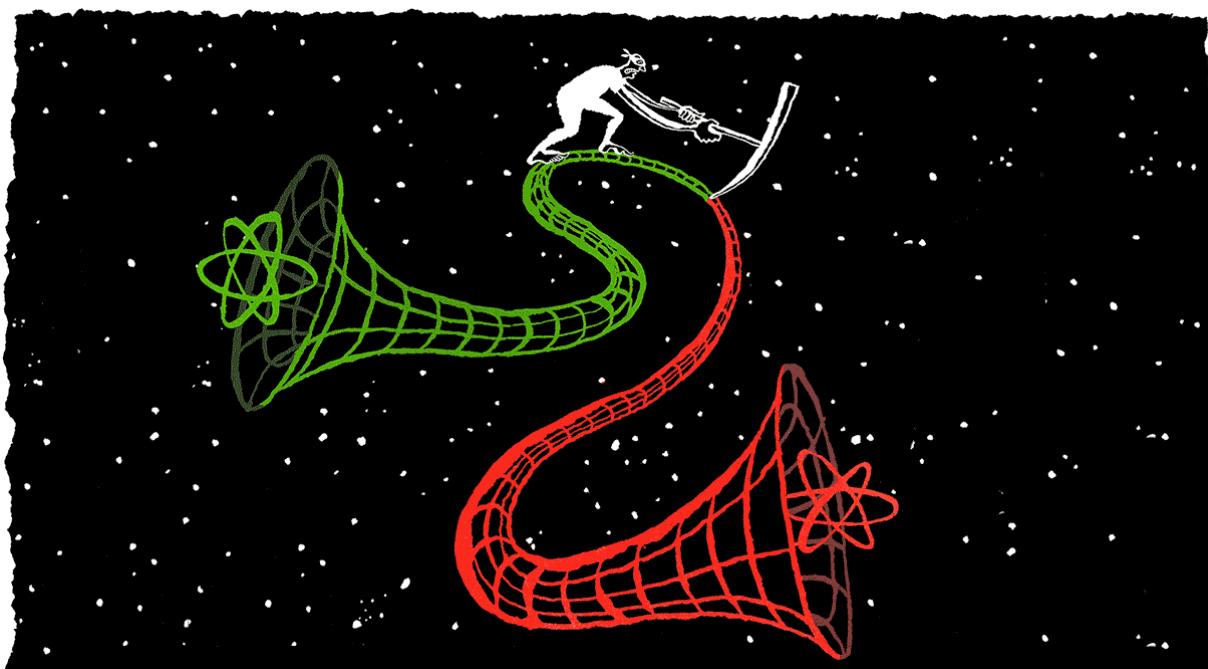
Quantum-enhanced approaches may also supplement other biological imaging techniques, such as positron emission tomography (PET), which takes pictures of the high-energy gamma-ray

light flying out of injected radioactive tracers. Each tracer molecule's interaction with tissue spits out two photons in opposite directions. Quantum-entanglement tomography aims to make use of the fact that those photons are entangled when they are created. In PET, the photons can be hard to track because they bounce off body tissues. The entanglement of each pair makes it easier to work out which came from where, so scans take less time and radioactive material.

Ghost imaging is another promising way of making use of light's quantum nature. The technique involves splitting a beam of light in two and aiming the resulting two beams at two detectors, one directly and one through a somewhat opaque medium, such as turbulent air rising from hot ground or a smoke-filled room. Because the photons making up the beam are correlated, a rigorous accounting of what the two detectors can see yields images of what the eye cannot. In 2013 researchers from America's army showed that the technique worked over more than 2km.

The technique points to a fascinating debate that underpins many discussions in the broader quantum-technology community about exactly how quantum effects confer an advantage. Though ghost

imaging was predicted in the 1990s, arguments still rage about whether entanglement is playing a role or whether it works simply because light comes in discrete, countable photons. “There are plenty of physicists that don’t understand the distinction,” says Miles Padgett of the University of Glasgow, a quantum-imaging expert. “And I don’t think it matters. What matters is, are we using our knowledge in the quantum world to bring competitive advantage?” With hand-held detectors that can sense height differences down to a millimetre, magnetometers that can in principle watch your every neuron and imaging kit that can see across a smoky battlefield, the answer is ever more clearly yes.



Communications: Oh what entangled web we weave

3

Quantum networks could underpin unhackable communications links

IN 2004 the Bank of Austria and Vienna's city hall notched up the first quantum-encrypted bank transfer. Anton Zeilinger, a quantum-cryptography pioneer whose lab facilitated the transfer, expressed his hope that "all problems of implementation will be solved within three years." They were not.

The technology was put to the test again in 2007 when quantum-encrypted vote tallies from the Swiss federal election were sent from polling stations to the Geneva state government. Engineers insisted that the transmission was utterly impervious to eavesdropping or tampering; a company called ID Quantique had developed a system that harnessed one of the rules of quantum mechanics to offer total security.

That claim, too, turned out to be premature. Hackers have since demonstrated that equipment used in such transfers could be vulnerable to attack. What is more, such quantum encryption also required a single, dedicated fibre between sender and receiver, which limited the technique to high-profile transactions, and precluded the cross-linking of many senders and receivers that has made networking and the internet so successful.

Key findings

That is now changing. In response to hackers' attacks, the kit has become markedly more secure. Field trials have shown that delicate quantum light signals can be sent through the same fibres that bring the internet to homes and businesses. And efforts to make quantum-enhanced versions of the equipment that amplifies and distributes standard optical signals are bearing fruit. Quantum networks are springing up or expanding. And quantum communications, just like their conventional counterparts, will soon be whizzing through space, too.

The most discussed and deployed technique is called quantum-key distribution (QKD). In one set-up, a sender launches single photons toward a receiver, randomly choosing one of four planes along which the light particles are polarised, two of them associated with a 0 and the other two with a 1. The receiver likewise randomly chooses which kind of polarisation to check for. After sending a string of these bit-associated photons, the pair can publicly compare notes on which polarisations they employed; whenever they happen to have chosen the same one, the 0 or 1 associated with that polarisation can be used as a bit in a cryptographic

key.

What contributes to the system's security is Heisenberg's uncertainty principle, a much-touted quantum rule which, in this case, guarantees that an eavesdropper would disrupt the system's randomness, because intercepting and measuring a given photon forces it into a given polarisation.

That disturbance to the system would reduce the number of coincidences the pair sees; if there are too few (they should be seen about half the time), they know someone is on the line.

Physics textbooks will tell you that a sufficiently long cipher, randomly generated this way and used only once, is absolutely secure. But Vlatko Vedral, of the Centre for Quantum Technologies in Singapore, says that hackers who have been invited to try to break into the centre's quantum-communications experiments have often succeeded —not by beating quantum rules but by ruthlessly exploiting shortcomings of the kit itself. For example, storing a digital 0 generates a slightly different amount of heat from storing a 1, so careful observation of the heat being generated can expose the string of digits being received. Once discovered, such hacks are easily prevented. As time has gone on, such shortcomings have narrowed in scope, and

have driven innovation.

Thanks to the development of ever more secure links, quantum cryptography has recently been deployed more widely. ID Quantique has installed quantum links between data centres of KPN, a Dutch telecoms firm; of Battelle, an American non-profit research firm; and of HypoSwiss and Notenstein, two Swiss private banks. It offers links between financial institutions in Geneva and a disaster-recovery centre 50km away. In 2015 researchers at Toshiba in Japan began sending quantum-encrypted genomic data from a research facility in Sendai to Tohoku University, 7km away.

But the future of the technology lies in quantum networks—the infrastructure required to connect many senders and receivers. These are springing up within and between major metropolitan areas. South Korea's government is funding a 250km link to join existing metro quantum networks. In Britain a network of similar length will be deployed between the cities of Bristol and Cambridge, via London. Australia is building a closed government network in the capital, Canberra.

No quantum network is more ambitious than the one completed in China at the end of last year.

The future of
the
technology
lies in
quantum
networks

Funded by the central government, it links Beijing and Shanghai via Jinan, which already has a metro network over 70 square kilometres, made up of 50 “nodes”—switchboards connecting senders and receivers—and Hefei, which has a 46-node network. Its customers include China Industrial and Commercial Bank, the China Banking Regulatory Commission and the Xinhua news agency.

Distance presents a problem. As the meticulously prepared photons with their delicate quantum states bounce along lengths of fibre, those states eventually get scrambled and their information is lost. To ensure fidelity and security, the fibre link should be no longer than about 200km. Standard fibre-optical signals suffer from the same weakening of the signal, so “repeaters” to boost it are placed at regular intervals along their path. But under the quantum rule book, unknown quantum states cannot be copied, so quantum data would need to be temporarily decrypted before receiving a boost, creating a security loophole.

There are two ways to get round this, one by land and one by air. The land-based solution is to develop quantum analogues of the repeater. That will require a quantum memory that can store incoming information, and a means of sending them

on that does not compromise quantum security. That last part requires another bit of quantum trickery: teleportation. This is a way of projecting the quantum state of one particle (not, it should be stressed, the particle itself) onto another, distant one. Last year two research groups showed the benefits of teleportation across two metropolitan networks, in Calgary and Hefei. Crucially, they carried out their experiment using the same wavelengths as those used in existing telecoms networks, to ensure that the new technique can be used with existing fibre infrastructure. It did the trick.

Spooks reacting at a distance

Another tack is to take to the air, over similar distances but without the need for a particular fibre link. The current record for teleportation of quantum states in this way was set in 2012, when researchers sent a quantum-encrypted message between two of the Canary islands, 143km apart. A long-standing ambition is to apply the idea to space: for a photon, the disturbance caused by the whole thickness of the Earth's atmosphere is equivalent to that caused by just a few kilometres of air at the surface.

Last August China launched Micius, a quantum-

key-distribution-enabled satellite backed by tech companies including Huawei and Lenovo. The goal at this stage is to link the Beijing-to-Shanghai network to another in Urumqi, in Xinjiang province, some 3,000km away. Efforts to develop satellite communications are also under way in Singapore, Canada, Japan, Italy and America. Once the challenges of getting quantum signals into space—through turbulent air, clouds and so on—are overcome, a global network could easily follow.

With country-spanning networks and quantum-enabled satellites, it is easy to envisage a global “quantum internet” in which each link offers quantum-enhanced security. But the kind of innovation that will allow the development of such networks will also be of use, for example, in shuttling information within, and between, future quantum-computing devices: think quantum distributed computing and quantum cloud computing. Just as the internet has demonstrated the power of linking many standard computers, says Seth Lloyd, a theorist at the Massachusetts Institute of Technology, “the quantum internet has the potential to change the way in which people and organisations collaborate and compete, establishing trust while protecting privacy.”

Not everyone is convinced yet. The defence establishment seems to have been put off by some of the early setbacks to quantum links. Quantum-communications efforts are under way, for example in the research arms of America's army and navy, but an analysis by the air force's Scientific Advisory Board suggested that QKD had "little advantage over the best classical alternatives". And doubters rightly point out that encryption is not the weakest link in many security chains.

Yet as the hardware improves and heavy investment continues, quantum networks may begin to look like a strategic must-have; if so, consumer applications are likely to proliferate. The European Telecommunications Standards Institute (ETSI), which sets global benchmarks for the industry, is working to define quantum-cryptography standards. ETSI scientists want to ensure that kit from multiple vendors can work together, and to create a certification so that consumers (including spooks) are guaranteed a widely agreed level of security. Miniaturisation efforts are well under way too, so before long the equipment may fit in the palm of your hand—or in your phone.



Cue bits: Why all eyes are on quantum computers

4

Tech giants and upstarts alike are piling into a technology with huge potential

IN 1981 Richard Feynman, a visionary physicist, had a clever idea. Could the odd properties of quantum mechanics, he wondered aloud in a lecture, be used to carry out simulations of physical systems that computers of the time could not cope with? Others took up the question. In 1985, David Deutsch, now at Oxford University, showed how quantum systems could be set up as a “universal” computer—that is, like current computers, able to run any program. Though fascinating, at that point it was all rather theoretical, involving hardware that

no one knew how to build.

What made the world sit up and take notice was a paper published in 1994 by Peter Shor, then at Bell Labs. Dr Shor showed that a quantum computer would be capable of working out the prime numbers that, multiplied together, make up an exceedingly large number. The fact that this “decomposition” is mathematically very hard is the basis of cryptographic protocols still used today.

Since then, researchers have come up with a rich variety of problems for which quantum computers should be superior to the best supercomputers—and a number of algorithms, or sets of steps, to break down problems in such a way that quantum computers can crunch through them. This evident utility started an international competition to build one that was, for many years, confined to quiet labs and the academic literature. These days, big business is seriously interested, and blue-chip companies including Intel, Hewlett-Packard, Google and Microsoft all have research programmes. Last year IBM released Quantum Experience, which lets all comers play around with a crude quantum computer over the internet. Governments too are putting money into academic efforts, both directly and via defence contractors,

and a growing band of startup companies are striking out on their own.

A computer big enough to do what Dr Shor envisaged would also be useful for all manner of currently intractable problems. Although that remains a distant prospect, steps towards developing one could have big benefits; for many applications, a much simpler or special-purpose computer will do.

Bit by bit

What makes the idea of quantum computers so attractive is not so much that they will work faster than traditional computers—they may for some applications but not for others—but that they will work fundamentally differently. Three intuition-defying concepts play a role. The first is superposition. Today's computers depend on bits taking one of two values, 0 or 1. Qubits, their quantum analogues, can be arranged in “states” that are best thought of as some mixture of both 0 and 1. To carry out a computation using one of these strange beasts is to act on both the 0 and the 1, in a sense to create within the calculation the potential outcome of either at the same time.

The power of this indeterminate state is unleashed

through the second quantum-mechanical effect, entanglement. A standard computer depends on the complete isolation of one bit from the next to prevent a computation from going awry or a document from getting corrupted. For a quantum computer, the entangling of multiple qubits is paramount; in the best case, all of a given device's bits are entangled with one another. Again, to operate on one qubit is to operate, to varying degrees, on all the entangled ones. It is therefore impossible to describe such a machine in strict terms of its constituent parts. There is a need to consider how one qubit is connected to its neighbour, and to the next-but-one, and so on through all the cross-correlations. To describe all the states of a 50-bit standard computer requires 50 bits of digital memory; a description of a 50-qubit computer would require a quadrillion.

It gets weirder. Whereas it is easy to imagine an equation that predicts a low or even zero probability of a given event, it is much harder to reckon with what are called probability amplitudes in quantum mechanics, which can actually be negative. In the course of a quantum computer's crunching, these amplitudes can (again like waves) interfere, positive with positive and negative with negative—in

essence, to reduce the probability of the wrong answer and boost that of the right one.

Posing a question starts with choosing an algorithm suitable for the problem. This algorithm is actually manifest as the starting states of the qubits: 0 here, 1 there, a bit of a mix over there. The calculation is then just a matter of letting quantum-mechanical laws play out on this system of superposed and entangled qubits. Changing states, shifting qubit couplings and so on represent a vast cross-multiplication of all those states and combinations, with probability amplitudes reinforcing and diminishing until the system settles into a final state that represents the answer. It is a matter of setting up the problem, and the machine, so that all the possibilities are sifted through at lightning speed.

Efforts to make qubits often centre on the use of tiny loops of superconducting wire, arranged like the “gates” of standard computers. Single charged atoms, trapped by electric or magnetic fields, can also do the job; in February an international consortium of researchers published an open-source blueprint for a trapped-ion machine. Several groups use single photons as qubits—an approach that looks easy to integrate with existing semiconductor-fabrication techniques. Microsoft’s planned

“topological” quantum computer uses something else entirely: “anyons”, particles that would be more easily tamed than other qubit candidates but which have never been seen outside the pages of theoretical physics textbooks.

Setting up a qubit is no longer difficult. The problem is looking after it. Quantum states are notoriously delicate, requiring complete isolation from the actual stuff of the experiment. But isolation can never be complete, and errors creep in; for a calculation to succeed these must be noticed and corrected. It has become clear that as computers scale up, the number of logical qubits (the ones actually doing the calculation) will be dwarfed by an “overhead” of perhaps thousands of times as many error-correcting and command-and-control qubits. The kind of machine required to implement Shor’s famed algorithm on the sort of large numbers used in encryption will need to contain something like a million qubits.

Such machines will, to put it mildly, be an engineering challenge. But in a clear indication that quantum computing is getting closer, names familiar from traditional computing are increasingly getting involved. Hewlett-Packard is trying to build its own machine. Intel’s global quantum

investments include \$50m going into work at QuTech, the Netherlands' national quantum-technology hub. Microsoft's topological quantum approach, if it works, will be much less error-prone.

The quantum-computing startup scene is also becoming increasingly vibrant. Researchers from Yale and the University of Maryland have spun off companies, and physicists who had worked at IBM and America's Department of Energy have started their own firms.

Governments are getting in on the action too. Australia's has invested A\$26m (\$20m) in a laboratory at the University of New South Wales in Sydney (and the Commonwealth Bank of Australia and Telstra, a telecoms firm, have together chipped in about the same amount). A lab at the University of Sydney down the road is being funded as part of LogiQ, a programme of the Intelligence Advanced Research Projects Activity, an American government defence outfit. Leaked documents have revealed that America's National Security Agency has been exploring "if a cryptologically useful quantum computer can be built". Experts now reckon it can. But when?

Simulating discussion

Very few in the field think it will take less than a

decade, and many say far longer. But the time for investment, all agree, is now—because even the smaller and less capable machines that will soon be engineered will have the potential to earn revenue.

Already, startups and consulting firms are springing up to match prospective small quantum computers to problems faced in sectors including quantitative finance, drug discovery and oil and gas.

Perhaps the most interesting early applications will take the form of “quantum simulators”: computers that mimic real physical systems. This is what

Feynman had in mind, imagining in his lecture “that the computer will do exactly the same as nature”.

Quantum simulators might help in the design of room-temperature superconductors allowing electricity to be transmitted without losses, or with investigating the nitrogenase reaction used to make most of the world’s fertiliser.

Quantum simulation has its fans in industry, too.

Michael Bolle at Bosch foresees using simulators to design batteries that will supersede the current lithium-ion technology. Paolo Bianco, who heads the quantum-technology research team at Airbus, a big European aerospace firm, says that quantum-simulating a new material such as a stiffer or lighter alloy for use in aeroplanes or satellites would be

much faster and cheaper than manufacturing and then testing the material itself. “The promise of quantum technologies”, he says, “is in engineering terms a step up in performance—not of 20%, but of a couple of orders of magnitude.”

For some applications and classes of problems that may well be true. But the experience of D-Wave Systems, a Canadian company that began selling the first commercially available quantum computer in 2011, shows how little is known about what future machines will be able to do. D-Wave makes what is known as a quantum annealer, a special-purpose quantum computer (as opposed to a universal one) that works best on “optimisation” problems, such as finding the shortest possible route for a travelling salesman. The firm’s customers include Lockheed Martin and a consortium including Google and NASA. In January Temporal Defense Systems, a cyber-security firm, bought one.

Brain scan: David Deutsch



The father of quantum computing sees it as a fundamentally new way of harnessing nature

“I OCCASIONALLY go down and look at the experiments being done in the basement of the Clarendon Lab, and it’s incredible.” David Deutsch, of the University of Oxford, is the sort of theoretical physicist who comes up with ideas that shock and confound his experimentalist colleagues—and then seems rather endearingly shocked and confounded by what they are doing. “Last year I saw their ion-trap experiment, where they were experimenting on a single calcium atom,” he says. “The idea of not just accessing but manipulating it, in incredibly subtle ways, is something I totally assumed would never happen. Now they do it routinely.”

Such trapped ions are candidates for the innards of eventual powerful quantum computers. These will be the crowning glory of the quantum theory of computation, a field founded on a 1985 paper by Dr Deutsch. He thinks the widely predicted “quantum supremacy” that eventually puts a quantum computation incontrovertibly ahead of a classical one will be momentous for scientists and laymen alike. He brushes off the fervent debate about whether the commercially available D-Wave computer offers a speed advantage. “If it works, it works in a completely different way that cannot be expressed classically. This is a fundamentally new way of harnessing nature. To me, it’s secondary how fast it is.”



Still, these are steps towards a powerful, universal quantum computer that could solve a lot of thorny problems. To describe such a device properly is to account not only for the states of each of its constituent bits but also for all the couplings between them, for each is entangled with every other. A good-sized one would maintain and manipulate a number of these states that is greater than the number of atoms in the known universe. For that reason, Dr Deutsch has long maintained that a quantum computer would serve as proof positive of universes beyond the known: the “many-worlds interpretation”. This controversial hypothesis suggests that every time an event can have multiple quantum outcomes, all of them occur, each “made real” in its own, separate world.

At the same time, quantum computation, and the quantum-mechanical theory from which it springs, are all subsumed in a newer idea that Dr Deutsch is pursuing. He contends that what he calls his “constructor theory” provides a perspective that will lead to the rewriting of physics altogether. As with classical computer science, quantum computation and even genetics, it is based on the role of information. But rather than letting physical laws define what is and is not possible, as science does now, constructor theory asserts that those laws actually arise from what is and is not possible.

From observed possibilities, a mathematical object called a constructor can be fashioned. Operating with and on these constructors gives rise to what Dr Deutsch reckons is a theory even

more fundamental than quantum mechanics. He is enthusiastic about the theory's potential to upend the very foundations of science, but concedes that testing it experimentally remains a distant

The
Economist

TQ



computers.



For years experts questioned whether the devices were actually exploiting quantum mechanics and whether they worked better than traditional computers. Those questions have since been conclusively answered—yes, and sometimes—but only by exhaustively testing the machines' mettle directly. The current best supercomputers are able to simulate only what more general-purpose quantum computers of about 50 qubits can do. Tantalisingly, it is difficult to tell at what problems bigger machines will excel.

Google is aiming to use its own machinery, a so-called gate-model quantum computer of the sort most groups are pursuing, to achieve “quantum supremacy”, whereby a quantum computer performs a calculation faster than any known

computer could. Google researchers have laid out an ambitious plan which may let them achieve that feat this year. D-Wave has hinted it has already done so, but has made similar claims in the past; their current numbers are still to be checked.

Whenever, and by whomever, this is accomplished, it will launch an era of small-scale machines offering quantum-enhanced solutions and services. The first publicly accessible one, IBM's Quantum Experience, may be an indication that the machines' future will be in the cloud. Most users have no more need for one at home than they have for a supercomputer.

But some do. In 1982, a year after Feynman gave his quantum-computing lecture, he was touring the supercomputer facility at Los Alamos National Laboratory, where he had worked on the first atomic bomb. Talking to Bo Ewald, then in charge of the lab's computing efforts and now running D-Wave, Feynman said, "You know, young man, one day all of these will be replaced by quantum computers." One has already moved in.



Software: Program management

5

Quantum-computer code could do wonders—but also unravel well-kept secrets

IT DOESN'T help to have a quantum computer if no one knows how to program it," says Tim Polk, of the White House Office of Science and Technology Policy in Washington. Although academic efforts to build quantum-computer hardware have been going on for two decades, comparatively little has been done to develop the software needed to run the machines when they come.

That is changing, because in the past few years it has become clear that those machines are getting closer. Two parallel efforts are under way. One is to create software as generally understood—the graphical interfaces, programming languages and so on, a kind of "Windows for quantum". The other is to develop novel algorithms, step-by-step instructions that break down problems into discrete

parts amenable to quantum computing.

Innovation abounds in both camps, and among big tech firms as well as plucky startups. Some big players are working on both sides of the problem, and a growing ecosystem of quantum-friendly consultancies advises companies on what quantum computing might do for them.

“Machine” language for quantum computers, which actually tells the computer what to do, is fairly well understood. It is not so different from the logic gates of standard computing, except that it allows for “superpositions” of qubits in which they can be both 0 and 1 at the same time. But how to write computer code to interact with such a machine, or to simulate what it can do? Options are multiplying, including open-source software packages such as QuTip, funded by a number of research outfits in Asia. On March 6th IBM released the first commercial program for universal quantum computers (the general-purpose kind). And various startups have released their own quantum software.

One of the most ambitious, LIQUi|> (whose name plays on a symbol in quantum mechanics), comes from Microsoft. It aims to tackle the whole “software stack”, from the user interface to code-

compilers and ultimately to a machine language suitable for Microsoft's planned hardware, and that of others.

Krysta Svore, who leads Microsoft's quantum-software team, says that the group is also working on reducing the total number of qubits and operations required for quantum calculations, known as "overhead", and on making standard computers better at emulating quantum ones (the group recently hired a world expert in that field, Matthias Troyer). The team's full-scale simulation of a 32-qubit computer requires 32 gigabytes of memory, more than the average desktop can muster but still manageable.

Dr Svore and her colleagues are also making estimates of how many qubits, and minutes, would be needed to crack specific problems. She says the numbers are "down dramatically", thanks to recent improvements in keeping qubits under tighter control. For example, she reckons that a thorough analysis of the energy-intensive nitrogenase reaction to make fertiliser would take a 100-logical-qubit quantum computer hours or perhaps days, whereas a conventional supercomputer would need billions of years. The prize might be a cut of 1-2% in global natural-gas consumption.

But the key to getting the most out of quantum computers are the algorithms that these various software packages implement. The first of them, including the one by Peter Shor that showed how quantum computers could crack global encryption systems, tested the theoretical idea by aiming at the most intractable problems on the biggest notional machines.

Even deeper learning

These days, says Aram Harrow of the Massachusetts Institute of Technology, the focus has shifted to algorithms that smaller machines can make use of, because that kind of hardware will soon be widely available. “We’re still interested in what you can do with a million or a billion qubits, but it’s interesting to see if you can figure out what you can do with 100,” he says.

A lot, it seems. One of the most promising areas is in machine learning and deep learning, two facets of artificial intelligence that have attracted much attention recently. Applications include searching through vast swathes of data to find patterns, such as in image recognition, cyber-security and, more prosaically, recommendation engines that suggest products consumers might like. But there are all

manner of other algorithms, from those that crunch numbers to those that mimic atoms.

All these quantum recipes call for some means of cataloguing them. Stephen Jordan heads the Quantum Algorithm Zoo at the National Institute of Standards and Technology in Maryland, a comprehensive collection of known algorithms. He has devised a taxonomy of 59 mathematical families they fit into, each suited to particular kinds of problems or breaking down problems in a particular, quantum-friendly way.

Many such algorithms, when run on existing special-purpose machines or as emulations on standard computers, fail to beat their “classical” counterparts. Vlatko Vedral, of the National University of Singapore’s Centre for Quantum Technologies, stresses that traditional techniques, particularly for quantum-chemistry problems like the nitrogenase reaction, are already quite sophisticated. The trouble is that no beefy general-purpose quantum computer exists as yet, so no one knows whether a given algorithm run on one would beat its classical counterpart. At the same time, astonishingly efficient algorithms suited to quantum computing are waiting to be discovered.

Those 59 families of algorithms, and ever-better emulators for eventual machines, are an excellent starting point for planning the quantum-computing future, and nowhere is interest greater than in finance. Commonwealth Bank of Australia is getting in early, collaborating closely with a research group led by Michelle Simmons at the University of New South Wales. D-Wave has partnered with 1Qbit, a startup, to develop “Quantum for Quants”, a forum for the quantitative-finance industry. Its editors include Michael Sotiropoulos, head of global equities at Deutsche Bank. UBS, a big Swiss bank, is working with QxBranch, another startup, on using quantum algorithms in foreign-exchange trading and arbitrage. Hyder Jaffrey, head of Strategic Investments and Fintech Innovation at UBS Investment Bank, says he puts quantum computing in the same category as artificial intelligence and blockchains, “all these evolving technologies with the potential to change markets”.

Banking on it

Companies such as QxBranch and 1Qbit play a new role of middleman between the quantum experts and industry, examining whether and how a given firm’s business might be improved by quantum

methods, for example optimising trading strategies or supply chains, or monitoring network activity to spot cyber-attacks. Landon Downs, a co-founder of 1Qbit, says that can lead to solutions which can already be put to use. “By taking the lens of how you would formulate an algorithm on a quantum computer you often find very good improvements on classical algorithms,” he says. “That’s where lots of our successes come from.”

The biggest benefit is expected to come from quantum-computing hardware once it arrives, so much of this business depends on simulating that hardware on standard machines as accurately as possible. Michael Brett, chief executive of QxBranch, says the idea is that “some Tuesday morning when one becomes available we just swap out our simulation for the real hardware.”

Even as all these computer scientists and consultants are working on software for the quantum future, a handful of others are working on software to combat it. After all, what got researchers going in the first place was the fear that global encryption standards would crumble in the face of quantum computing. That remains a danger for the future, and retrospectively perhaps even for the present, if encrypted communications filed away

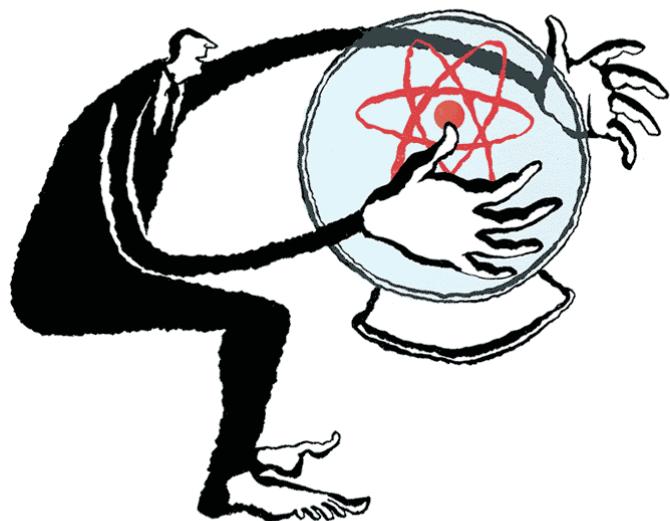
now are analysed by powerful quantum computers later. That is the idea behind post-quantum cryptography, an effort to create ciphers that even future quantum computers will be unable to crack.

PQCrypto is a three-year, European-funded project to develop post-quantum ciphers. Its goal is not to find the most mathematically gnarly way of encrypting data, but rather to identify one that is sufficiently difficult to break without needing too much memory or computation to implement. RSA, a current global standard, could be made hard enough to break, but the cryptographic keys would have to be a terabyte long—an impracticable option. Keys for elliptic-curve cryptography, another current standard, are just 32 bytes long; any post-quantum solution needs to aim for a similar ratio of brevity to security.

Tanja Lange, who leads the project, says that post-quantum efforts are now attracting a lot of attention, particularly from nervous Silicon Valley outfits. In 2015 America's National Security Agency said it would be updating all its cryptography to make it quantum-computer-proof. Last year Google quietly ran its own post-quantum cryptography test in Chrome, its web browser. Some of its users' communications were protected both with elliptic-

curve encryption and New Hope, a post-quantum protocol developed as part of PQCRYPTO. The median delay added to those communications turned out to be just a millisecond.

“The power of quantum computing is rediscovering all the problems that computers cannot solve, and having a path to solving them,” says Dario Gil, vice-president of science and solutions at IBM. “It’s a reorientation of what we think about computers.” But a device capable of solving big problems will create new ones if it can unravel protocols that have protected secrets for decades.



Commercial breaks: The uses of quantum technology

6

The most exciting thing about a quantum-enhanced world is the promise of what it may yet bring

WHEN the first atomic clocks were built and swiftly commercialised, no one used the term “quantum technology”. The clocks simply harnessed the power of quantum mechanics to improve results. At the time there were no other examples of how the odd predictions of quantum mechanics such as entanglement and superposition could be put to practical use. Mostly they informed fundamental science, yielding an ever-subtler view of the world at the tiniest scales.

Here and there, quantum weirdness did escape the lab, as in the case of the superconducting quantum interference device, an exquisitely sensitive magnetic-field sensor. The first of these was developed in 1964 at Ford Research Laboratory, the American carmaker’s blue-skies research facility.

Now they are widely used, for example in MRI machines. In the early 1980s researchers at IBM turned the quantum effect of tunnelling, in which particles seem to pass straight through impenetrable barriers, into a way to see the microscopic world with staggering resolution.

The current quantum-technology push is on a far grander scale, with multiple research efforts being funded by national governments and supranational bodies, sometimes for strategic reasons. Freeke

Heijman has led efforts to build QuTech, the quantum-technology institute of the Netherlands. “We don’t want to risk the scenario that we have invested all this money for years and in the end the money is going to be made in the US or China,” she says. And in the case of defence applications, she says security plays a role too: “If you have to buy it off the shelf, it’s not just an economic disadvantage, it’s also dangerous.”

But quantum technologies will not pass into the wider world in the same way as the global positioning system, which was developed with copious government funding behind closed doors and then handed over as a public good. “It’s just not like that today,” says Neil Stansfield, formerly of the British government’s Defence Science and Technology Laboratory. “We’re not the big kid on the government block, and certainly not on the global block.”

That leaves business to step into the breach. But Trevor Cross, chief technology officer of E2v, a British company whose detectors brought the world pictures from the Hubble Space Telescope and which is now doing pioneering work for quantum devices, says that quantum technologies are still viewed by many industries as risky. That may be

because many of the approaches are technologically so far beyond the current state of the art. Richard Murray, an emerging-technologies expert at Innovate UK, Britain's technology-strategy agency, says that the more transformative the technological change, the easier it is to miss opportunities.

Material evidence

The opportunities are many, because at the level of components these technologies are intimately connected. Many of them depend, for example, on light sources that can spit out photons one at a time, every time, and detectors that can just as unfailingly catch just one—no small feat, considering that a 60-watt bulb is putting out 100,000,000,000,000,000 or so of them every second. This kind of kit was unimaginable a decade ago.

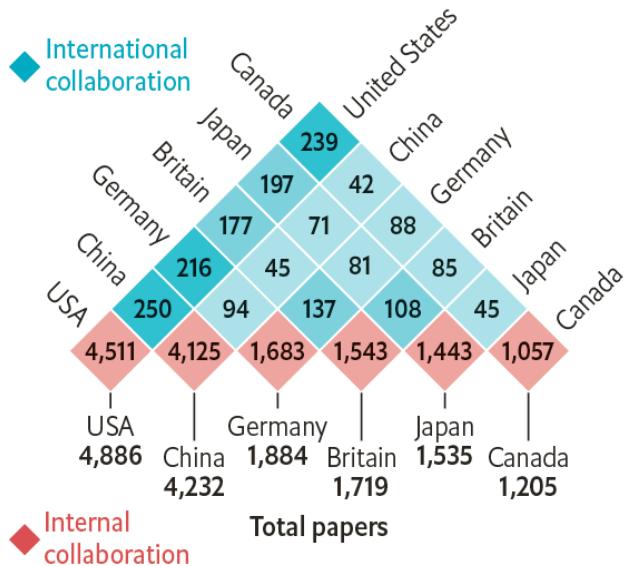
New materials, and precisely engineered versions of existing ones, will be needed too. Element Six, a subsidiary of De Beers, a diamond giant, has carved out a niche selling diamonds with bespoke “nitrogen vacancies”—flaws that turn them into sensors. Silicon carbide is tipped to be just as quantum-amenable as those diamonds, but so far expertise with it is thin on the ground.

New alliances will be forged as the work on materials intensifies. Intel aims to build qubits into silicon, in order to piggyback on existing fabrication infrastructure. But that will require the material to be produced to a much higher purity. To that end, Intel has joined forces with Urenco and Air Liquide, two materials firms.

Michael Bolle at Bosch, the multinational engineering firm, envisages a seamless coming together of these diverse approaches in applications such as autonomous vehicles or the internet of things: quantum sensors to gather sensitive readings, quantum cryptography to transmit them securely and quantum computing to gather insights from the resulting copious streams of data.

Foreign entanglements

Authorship of papers on quantum computing
by nationality of authors*, top 6 nations
2004–13



Sources: Digital Science; Clarivate

*Collaborations between more than two countries may be counted multiple times

Many practitioners believe that the applications and technologies outlined in this report are just the beginning. As they become more familiar, they will give rise to new applications and wholly new hardware. Subjects that used to be mere footnotes to physics will rule, and engineers (and perhaps even consumers) will have to learn to speak quantum.

Yet some innovators may find themselves stymied. “The question is to what extent will export controls on these technologies become an issue, particularly if any of it has some defence potential,” says Stephen Ezell, of the Information Technology and

Innovation Foundation, an American think-tank. Tech firms such as Intel and IBM have had trouble exporting parts and computers to countries like China, he says.

Such challenges aside, what is exciting about these efforts is how much is simply not known about their future. Bob Wisnieff, a manager at IBM's microelectronics-research labs, says that "we're not that far from being capable...of building quantum computers that will do things we cannot predict exactly." John Preskill, a quantum expert at the California Institute of Technology, who coined the phrase "quantum supremacy", has said that "a quantum computer can simulate efficiently any physical process that occurs in nature. Maybe. We don't actually know for sure."

That brings the potential of quantum technologies full circle, to the fundamental-science considerations from which they were born.

Quantum computers and simulators should eventually be capable of solving some of science's most basic and yet most daunting questions.

Sensors of unparalleled precision may at last make it possible to test the predictions of physicists' most abstract ideas, perhaps linking the theories of quantum mechanics and gravity.

“We certainly expect there are many additional things that we’ll be able to do with quantum beyond the things we know of,” says Tim Polk of the White House Office of Science and Technology Policy.

“We had no idea of all the things we’d be able to build with the transistor, and we see the same thing with quantum.”

Acknowledgments

In addition to those named in the text, the author would particularly like to thank: Scott Aaronson, John Bagshaw, Dan Bernstein, Kai Bongs, Altaf Carim, Adam Davison, Marc de Jong, Iulia Georgescu, Aram Harrow, Ray Johnson, David Kaiser, Leon Lobo, Graeme Malcolm, Mike Mayberry, Jian-Wei Pan, Martin Plenio, Dilan Rajasingham, John Rarity, Tanya Reeves, Andrew Shields, Marie Skelton, Tim Spiller, Andrea Taroni and Qiang Zhang.

[Read more from the print edition »](#)

Subscribe to The Economist

Subscribers can enjoy each week's complete issue in print, online or via our apps

	Monitoring nuclear weapons: The nuke detectives New ways to detect covert nuclear weapons are being developed, which	Brain scan: Britain's spaceman The pioneer of small satellites is laying plans for the developed, which	Green food: Silicon Valley gets a taste for food and infrastructure	Nuclear fusion: A big bet on small An American company thinks it can have a commercial reactor ready and working	The connected car: Smartphones on wheels The way cars are made, bought and driven is changing with mobile
--	--	---	--	---	---