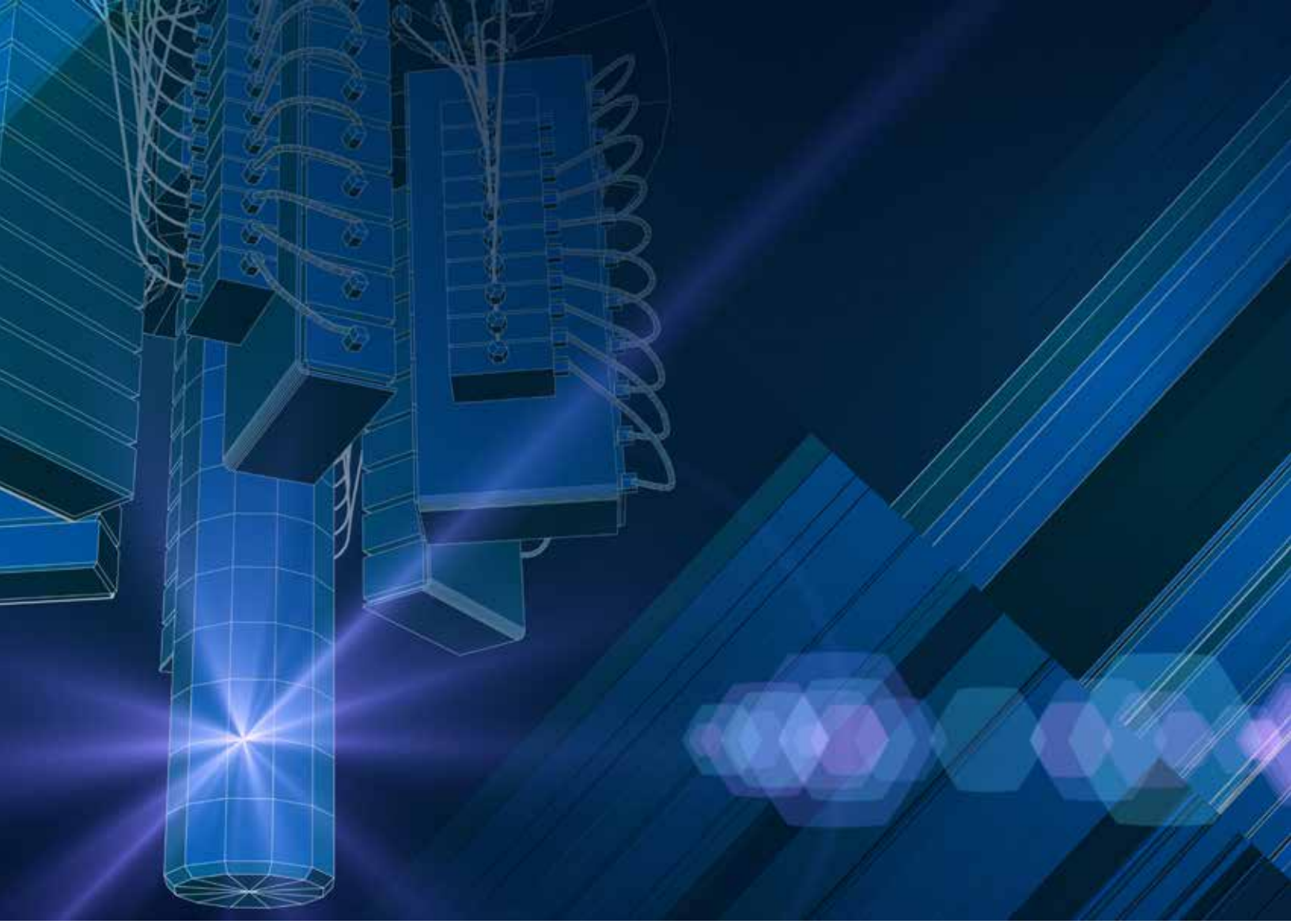


THE CIO'S GUIDE TO QUANTUM COMPUTING

November 2020

ZDNet

TechRepublic

TABLE OF CONTENTS

INTRODUCTION

Quantum computers offer great promise for cryptography and optimization problems, and companies like IBM, Google, and D-Wave are racing to make them practical for business use. This special feature from TechRepublic and ZDNet explores what quantum computers will and won't be able to do and the challenges we still face.

QUANTUM COMPUTERS ARE COMING. GET READY FOR THEM TO CHANGE EVERYTHING

Quantum computers are not yet creating business value, but CIOs should nonetheless lose no time in getting involved.

BY DAPHNE LEPRINCE-RINGUET/ZDNET

Supermarket aisles filled with fresh produce are probably not where you would expect to discover some of the first benefits of quantum computing.

But Canadian grocery chain Save-On-Foods has become an unlikely pioneer, using quantum technology to improve the management of in-store logistics. In collaboration with quantum computing company D-Wave, Save-On-Foods is using a new type of computing, which is based on the downright weird behaviour of matter at the quantum level. And it's already seeing promising results.

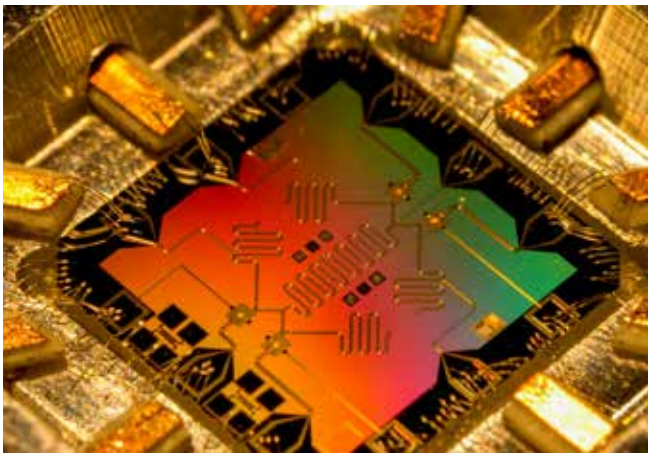


IMAGE: ISTOCKPHOTO/LYAGOVY

The company's engineers approached D-Wave with a logistics problem that classical computers were incapable of solving. Within two months, the concept had translated into a hybrid quantum algorithm that was running in one of the supermarket stores, reducing the computing time for some tasks from 25 hours per week down to mere seconds.

Save-On-Foods is now looking at expanding the technology to other stores, and exploring new ways that quantum could help with other issues. "We now have the capability to run tests and simulations by adjusting variables and see the results, so we can optimize performance, which simply isn't feasible using traditional methods," a Save-On-Foods spokesperson tells ZDNet.

"While the results are outstanding, the two most important things from this are that we were able to use quantum computing to attack our most complex problems across the organization, and can do it on an ongoing basis."

The remarkable properties of quantum computing boil down to the behaviour of qubits -- the quantum equivalent of classical bits that encode information for today's computers in strings of 0s and 1s. But contrary to bits, which can be represented by either 0 or 1, qubits can take on a state that is quantum-specific, in which they exist as 0 and 1 in parallel, or superposition.

Qubits, therefore, enable quantum algorithms to run various calculations at the same time, and at exponential scale: the more qubits, the more variables can be explored, and all in parallel. Some of the largest problems, which would take classical computers tens of thousands of years to explore with single-state bits, could be harnessed by qubits in minutes.

The challenge lies in building quantum computers that contain enough qubits for useful calculations to be carried out. Qubits are temperamental: they are error-prone, hard to control, and always on the verge of falling out of their quantum state. Typically, scientists have to encase quantum computers in extremely cold, large-scale refrigerators, just to make sure that qubits remain stable. That's impractical, to say the least.

This is, in essence, why quantum computing is still in its infancy. Most quantum computers currently work with less than 100 qubits, and tech giants such as IBM and Google are racing to increase that number in order to build a meaningful quantum computer as early as possible. Recently, IBM ambitiously unveiled a roadmap to a million-qubit system, and said that it expects a fault-tolerant quantum computer to be an achievable goal during the next ten years.

Although it's early days for quantum computing, there is still plenty of interest from businesses willing to experiment with what could prove to be a significant development. "Multiple companies are conducting learning experiments to help quantum computing move from the experimentation phase to commercial use at scale," Ivan Ostojic, partner at consultant McKinsey, tells ZDNet.


IMAGE: CONNIE ZHOU FOR IBM

IBM's CEO Arvind Krishna and director of research Dario Gil in front of a ten-foot-tall super-fridge for the company's next-generation quantum computers.

Certainly tech companies are racing to be seen as early leaders. IBM's Q Network started running in 2016 to provide developers and industry professionals with access to the company's quantum processors, the latest of which, a 65-qubit device called Hummingbird, was released on the platform last month. Recently, US multinational Honeywell took its first steps on the quantum stage, making the company's trapped-ion quantum computer available to customers over the cloud. Rigetti Computing, which has been operating since 2017, is also providing cloud-based access to a 31-qubit quantum computer.

Another approach, called quantum annealing, is especially suitable for optimisation tasks such as the logistics problems faced by Save-On-Foods. D-Wave has proven a popular choice in this field, and has offered a quantum annealer over the cloud since 2010, which it has now upgraded to a 5,000-qubit-strong processor.

A quantum annealing processor is much easier to control and operate than the devices that IBM, Honeywell and Rigetti are working on, which are called gate-model quantum computers. This is why D-Wave's team has already hit much higher numbers of qubits. However, quantum annealing is only suited to specific optimisation problems, and experts argue that the technology will be comparatively limited when gate-model quantum computers reach maturity.

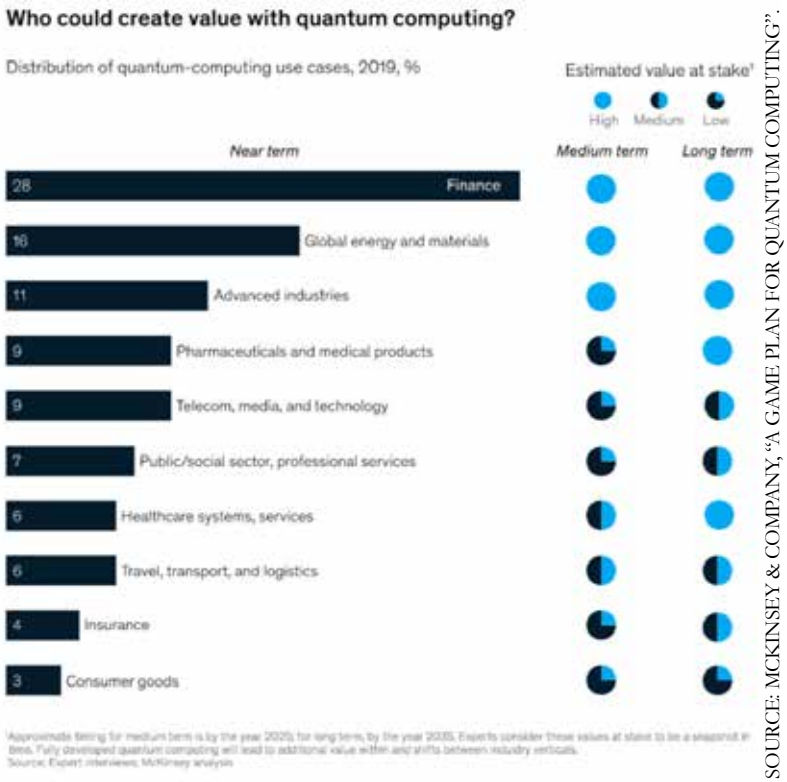
The suppliers of quantum processing power are increasingly surrounded by third-party companies that act as intermediaries with customers. Zapata, QC Ware or 1QBit, for example, provide tools ranging from software stacks to training, to help business leaders get started with quantum experiments.

In other words, the quantum ecosystem is buzzing with activity, and is growing fast. "Companies in the industries where quantum will have the greatest potential for complete disruption should get involved in quantum right now," says Ostojic.

And the exponential compute power of quantum technologies, according to the analyst, will be a game-changer in many fields. Qubits, with their unprecedented ability to solve optimisation problems, will benefit any organisation with a supply chain and distribution route, while shaking up the finance industry by maximising gains from portfolios. Quantum-infused artificial intelligence also holds huge promise, with models expected to benefit from better training on bigger datasets.

One example: by simulating molecular interactions that are too complex for classical computers to handle, qubits will let biotech companies fast-track the discovery of new drugs and materials. Microsoft, for example, has already demonstrated how quantum computers can help manufacture fertilizers with better yields. This could have huge implications for the agricultural sector, as it faces the colossal task of sustainably feeding the growing global population in years to come.

Chemistry, oil and gas, transportation, logistics, banking and cybersecurity are often cited as sectors that quantum technology could significantly transform. "In principle, quantum will be relevant for all CIOs as it will accelerate solutions to a large range of problems," says Ostojic. "Those companies need to become owners of quantum capability."



SOURCE: MCKINSEY & COMPANY, "A GAME PLAN FOR QUANTUM COMPUTING".

Chemistry, oil and gas, transportation, logistics, banking or cybersecurity are among the industries that are often pointed to as examples of the fields that quantum technology could transform.

There is a caveat. No CIO should expect to achieve too much short-term value from quantum computing in its current form. However fast-growing the quantum industry is, the field remains defined by the stubborn instability of qubits, which still significantly limits the capability of quantum computers.

"Right now, there is no problem that a quantum computer can solve faster than a classical computer, which is of value to a CIO," insists Heike Riel, head of science and technology at IBM Research Quantum Europe. "But you have to be very careful, because the technology is evolving fast. Suddenly, there might be enough qubits to solve a problem that is of high value to a business with a quantum computer."

And when that day comes, there will be a divide between the companies that prepared for quantum compute power, and those that did not. This is what's at stake for business leaders who are already playing around with quantum, explains Riel. Although no CIO expects quantum to deliver value for the next five to ten years, the most forward-thinking businesses are already anticipating the wave of innovation that the technology will bring about eventually -- so that when it does, they will be the first to benefit from it.

This means planning staffing, skills and projects, and building an understanding of how quantum computing can help solve actual business problems. "This is where a lot of work is going on in different industries, to figure out what the true problems are, which can be solved with a quantum computer and not a classical computer, and which would make a big difference in terms of value," says Riel.

Riel points to the example of quantum simulation for battery development, which companies like car manufacturer Daimler are investigating in partnership with IBM. To increase the capacity and speed-of-charging of batteries for electric vehicles, Daimler's researchers are working on next-generation lithium-sulfur batteries, which require the alignment of various compounds in the most stable configuration possible. To find the best placement of molecules, all the possible interactions between the particles that make up the compound's molecules must be simulated.

This task can be carried out by current supercomputers for simple molecules, but a large-scale quantum solution could one day break new ground in developing the more complex compounds that are required for better batteries.

"Of course, right now the molecules we are simulating with quantum are small in size because of the limited size of the quantum computer," says Riel. "But when we scale the next generation of quantum computers, then we can solve the problem despite the complexity of the molecules."

Similar thinking led oil and gas giant ExxonMobil to join the network of companies that are currently using IBM's cloud-based quantum processors. ExxonMobil started collaborating with IBM in 2019, with the objective of one day using quantum to design new chemicals for low energy processing and carbon capture.

The company's director of corporate strategic research Amy Herhold explains that for the past year, ExxonMobil's scientists have been tapping IBM's quantum capabilities to simulate macroscopic material properties such as heat capacity. The team has focused so far on the smallest of molecules, hydrogen gas, and is now working on ways to scale the method up to larger molecules as the hardware evolves.

A number of milestones still need to be achieved before quantum computing translates into an observable business impact, according to Herhold. Companies will need to have access to much larger quantum computers with low error rates, as well as to appropriate quantum algorithms that address key problems.

"While today's quantum computers cannot solve business-relevant problems -- they are too small and the qubits are too noisy -- the field is rapidly advancing," Herhold tells ZDNet. "We know that research and development is critical on both the hardware and the algorithm front, and given how different this is from classical computing, we knew it would take time to build up our internal capabilities. This is why we decided to get going."

Herhold anticipates that quantum hardware will grow at a fast pace in the next five years. The message is clear: when it does, ExxonMobil's research team will be ready.

One industry that has shown an eager interest in quantum technology is the financial sector. From JP Morgan Chase's partnerships with IBM and Honeywell, to BBVA's use of Zapata's services, banks are actively exploring the potential of qubits, and with good reason. Quantum computers, by accounting for exponentially high

numbers of factors and variables, could generate much better predictions of financial risk and uncertainty, and boost the efficiency of key operations such as investment portfolio optimisation or options pricing.

Similar to other fields, most of the research is dedicated to exploring proof-of-concepts for the financial industry. In fact, when solving smaller problems, scientists still run quantum algorithms alongside classical computers to validate the results.

"The classical simulator has an exact answer, so you can check if you're getting this exact answer with the quantum computer," explains Tony Uttley, president of Honeywell Quantum Solutions, as he describes the process of quantum options pricing in finance.

"And you better be, because as soon as we cross that boundary, where we won't be able to classically simulate anymore, you better be convinced that your quantum computer is giving you the right answer. Because that's what you'll be taking into your business processes."

Companies that are currently working on quantum solutions are focusing on what Uttley calls the "path to value creation". In other words, they are using quantum capabilities as they stand to run small-scale problems, building trust in the technology as they do so, while they wait for capabilities to grow and enable bigger problems to be solved.

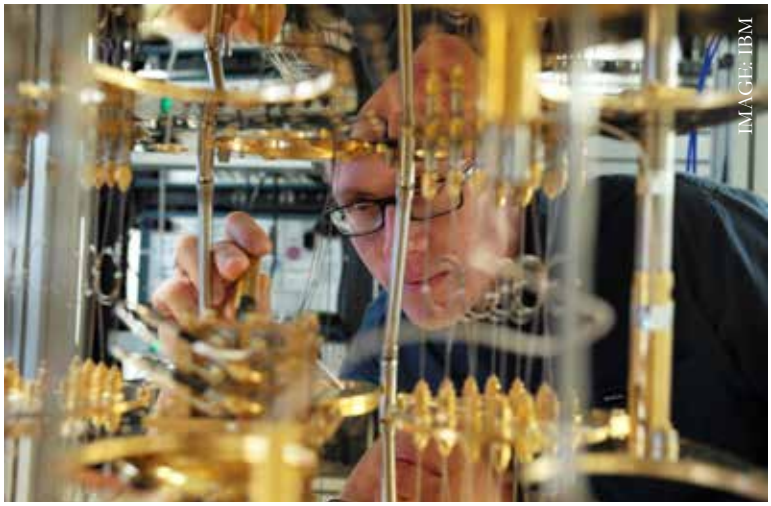


IMAGE: IBM

In many fields, most of the research is dedicated to exploring proof-of-concepts for quantum computing in industry.

Tempting as it might be for CIOs to hope for short-term value from quantum services, it's much more realistic to look at longer timescales, maintains Uttley. "Imagine you have a hammer, and somebody tells you they want to build a university campus with it," he says. "Well, looking at your hammer, you should ask yourself how long it's going to take to build that."

Quantum computing holds the promise that the hammer might, in the next few years, evolve into a drill and then a tower crane. The challenge, for CIOs, is to plan now for the time that the tools at their disposal get the dramatic boost that's expected by scientists and industry players alike.

It is hard to tell exactly when that boost will come. IBM's roadmap announces that the company will reach 1,000 qubits in 2023, which could mark the start of early value creation in pharmaceuticals and chemicals,

thanks to the simulation of small molecules. But although the exact timeline is uncertain, Uttley is adamant that it's never too early to get involved.

"Companies that are forward-leaning already have teams focused on this and preparing their organisations to take advantage of it once we cross the threshold to value creation," he says. "So what I tend to say is: engage now. The capacity is scarce, and if you're not already at the front of the line, it may be quite a while before you get in."

Creating business value is a priority for every CIO. At the same time, the barrier to entry for quantum computing is lowering every time a new startup emerges to simplify the software infrastructure and assist non-experts in kickstarting their use of the technology. So there's no time to lose in embracing the technology. Securing a first-class spot in the quantum revolution, when it comes, is likely to be worth it.

RESEARCH: QUANTUM COMPUTING WILL IMPACT THE ENTERPRISE, DESPITE BEING MISUNDERSTOOD

58% of survey respondents said quantum computing will have a significant or somewhat of an impact on the enterprise, even though 90% reported having little or no understanding of the technology.

BY MELANIE WOLKOFF WACHSMAN/TECHREPUBLIC

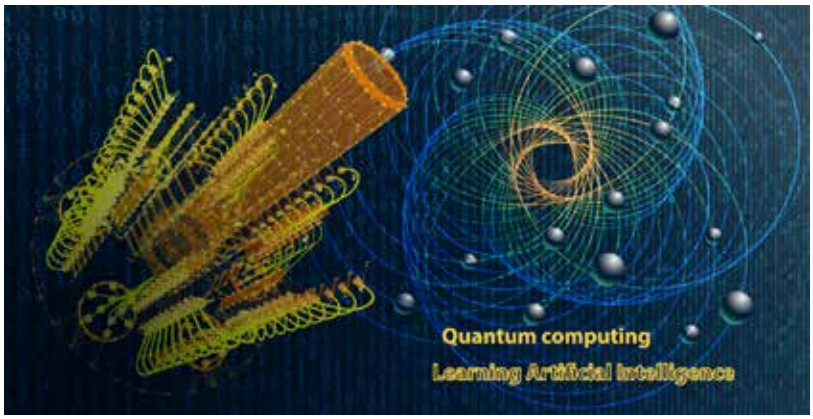


IMAGE: ISTOCKPHOTO/ANADMIST

Nanotechnology, transportation, cybersecurity, and data analytics are just a small sampling of the fields that quantum computing is predicted to impact. However, while the use cases for quantum computing may seem endless, enterprises are still deciding if this new level of compute power is all just a pipe dream or a future reality.

ZDNet's sister site TechRepublic Premium wanted to discover exactly what the enterprise thinks about quantum computing. So it conducted a survey asking professionals what they know about quantum computing, and what they don't.

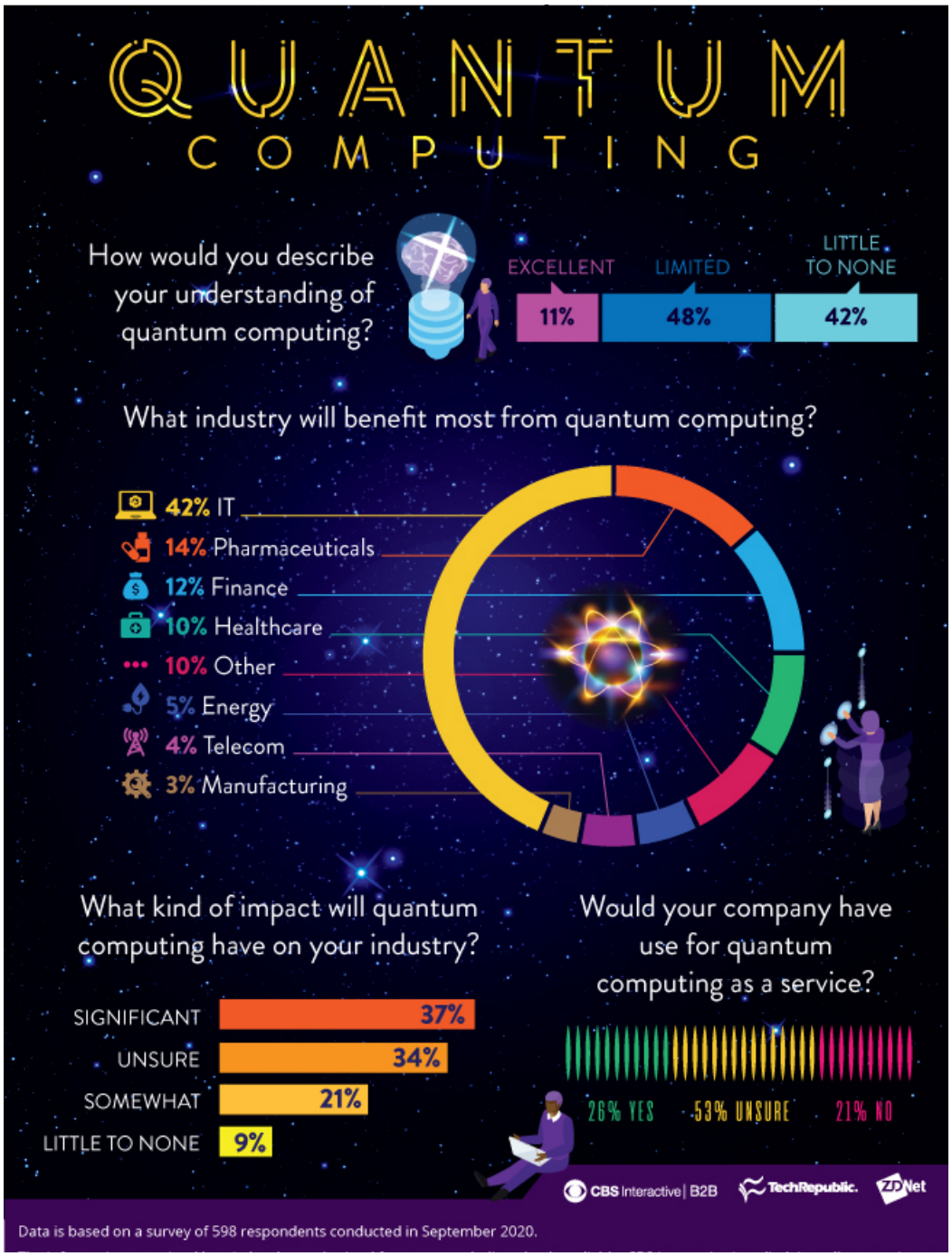
Overall, quantum computing remains an enigma for the majority of survey respondents, with 90% reporting that they had little to no understanding of the topic. Only 11% of the 598 respondents said they had an 'excellent' understanding of quantum computing.

In terms of industry impact, more than half of the respondents (58%) said quantum computing will have either a significant or somewhat of an impact on the enterprise. Exactly where that impact will be seen was less clear. According to 42% of survey respondents, the IT sector will benefit most, followed by the pharmaceutical and finance sectors at 14% and 12% respectively. Other cited industries included healthcare, energy, telecom, and manufacturing.

Because this new level of compute power allows data to be consumed and processed faster while using less energy, all industries could potentially reap benefits from quantum computing. However, when asked "would your company have a use for quantum computing as a service?", 53% felt unclear about the promise of this

technology. Twenty-six percent of respondents said they do see a use for quantum computing as a service, while almost a quarter (21%) did not.

This infographic contains more details from the research. For all the findings, download the full report Research: Quantum computing in the enterprise; key vendors, anticipated benefits, and impact (available free to TechRepublic Premium subscribers).



WHAT IS QUANTUM COMPUTING? UNDERSTANDING THE HOW, WHY AND WHEN OF QUANTUM COMPUTERS

There are working machines today that perform some small part of what a full quantum computer may eventually do. But what are the real-world applications for quantum computing?

BY SCOTT FULTON III/ZDNET CONTRIBUTOR

A quantum computer is -- or, perhaps more accurately phrased, would be -- a wholly different order of mechanism than anything the human species has ever constructed. Today, there are working machines that perform some small part of what a full quantum computer may eventually do. Depending upon whom you ask, these are either quantum computing prototypes or "prologues" -- stepping stones toward the real thing.

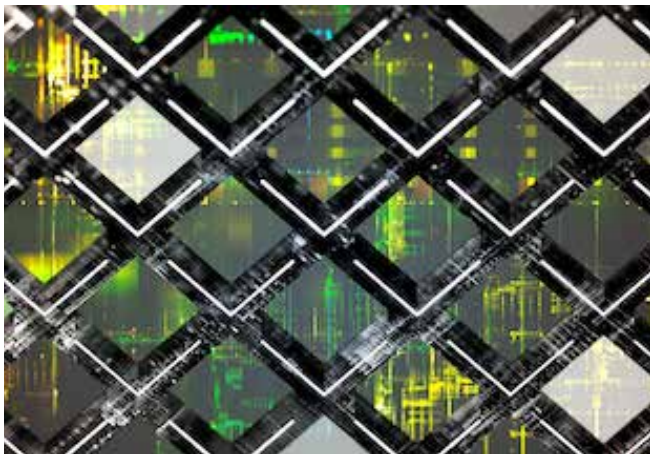


IMAGE: ISTOCKPHOTO/NIPLOT

The goal of quantum computing research is to discover a means of expediting the execution of long waves of instructions. Such a means would exploit an observed phenomenon of quantum mechanics that, when you write it down on paper, doesn't appear to make sense.

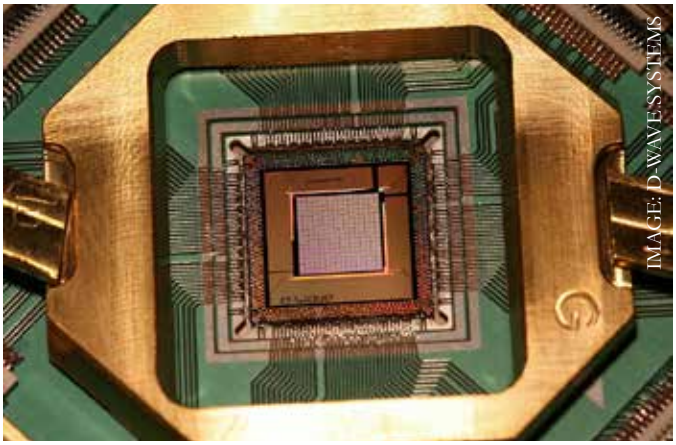


IMAGE: D-WAVE SYSTEMS

D-Wave's 2000Q quantum annealing device.

WHY QUANTUM?

If this goal is achieved -- if everything that physicists are certain works theoretically, ends up working in the real world -- then mathematical problems that require days' worth of calculation even on today's supercomputers, and some that are not solvable even now, may be solved instantaneously. Climate change models, estimates of the likelihood of Earth-type planets in the observable galaxy, models of the immune system's capability to destroy cancer cells -- the most

difficult and challenging problems we face today may suddenly yield results within no longer than an hour after launching the program.

Granted, these results may not come in the form of a complete solution, but instead a probability table pointing to the most likely solutions. But even such probabilities, up to now, have been unattainable even with the highest-performing supercomputers on the planet.

WHAT QUANTUM COMPUTING WOULD ACCOMPLISH

If you've ever programmed an Excel macro, you've personally experienced the following: You add input rows to the bottom of a worksheet whose columns serve as inputs for a long formula. Each time the formula recalculates, the time consumed is longer and longer. If you're on a slow enough computer, you can witness this phenomenon for yourself: As the number of input rows grows linearly, the time consumed by the macro grows exponentially.

If you've ever written a program for a supercomputer, you've witnessed exactly the same phenomenon. The scale may be different, but the effect is the same. And if you read through the supercomputer's logs, you can verify this observation personally. There's a point in time in which every algorithm, no matter how simple, simply becomes unworkable on account of the overwhelming weight of its input data.

This is the phenomenon that quantum computing would eliminate. A fully-functional quantum computer would become more capable exponentially by scaling its computing capacity linearly. As a result, for each increase in the number of steps in a quantum algorithm, the amount of time consumed during execution increases by a smaller amount, until eventually the time gap between exponentially different workloads becomes so small as to be immeasurable.

"What it means is that the difference between hard and easy problems," explained John Preskill, the Feynman Professor of Theoretical Physics at Caltech, during a 2017 speech, "the difference between problems we'll be able to solve someday with advanced technologies, and the problems that we'll never be able to solve because they're just too hard -- that boundary between 'hard' and 'easy' is different than it otherwise would be, because this is a quantum world, not a classical world."

Prof. John Preskill, Caltech

The quantum tradeoffs

To be very clear: It would be inaccurate to say that a quantum computer runs programs faster than a PC or an x86 server. A 'program' for a quantum computer is a very different order of beast than anything ever produced for a binary processor. The translation between a mathematical problem intelligible by college professors into a binary program, and the translation between the same problem into a quantum computer program, are as different from one another as '20 Questions' is from billiards.

There are several fundamental compromises when you move into the realm of quantum computing. Here's one that's daunting just by itself: Solutions will rarely be exact or definitive. A quantum computer is not a deterministic machine; in other words, there is no singular solution for which any other result would be an error. Instead, a quantum computer will tend to render sets of answers with their respective probabilities.

If that doesn't discourage you, get prepared for this: The atom-level device that actually performs the quantum calculations will, as a result of its work and as is its nature, self-destruct when it's done. A quantum computing mechanism would actually be a machine that automatically builds the computing device out of atoms (calcium atoms are good candidates), sustains the operating conditions of that device for the duration of its program, applies the program, allows it to execute, looks the other way (because quantum logic gates are shy and will explode if anyone sees them), interprets the final state of its registers as the final probability table of results, then resets itself to rebuild another mechanism all over again.

Imagine if Alan Turing's incredible machine that cracked the Nazi 'Enigma' code, was guaranteed to explode after every run (quantum computing engineers prefer the term 'collapse', but let's call it what it is -- explode.) And imagine if Turing, an ingenious engineer, devised an automated manufacturing operation that rebuilt that machine out of new parts, each and every day. Every quantum computer engineer has done more than imagine such a scheme; they have built a plan for such a device on the quantum scale. Indeed, such hypothetical 'on paper' schemes are called 'Turing machines'. Quantum engineers believe their computers can and will work, because their Turing machine experiments give them cause for faith.

WHAT A QUANTUM COMPUTER MAY BE GOOD FOR

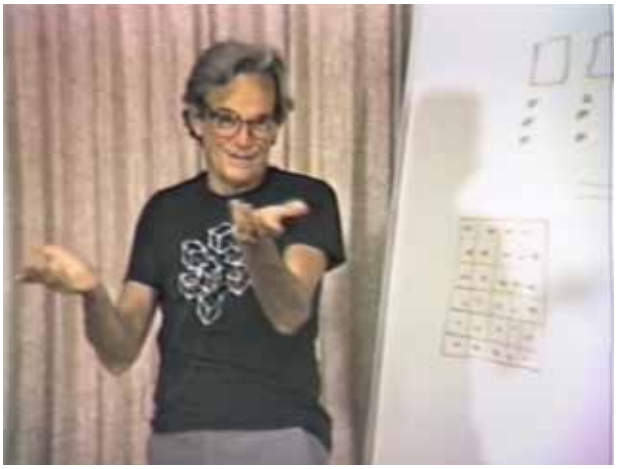
Are there real-world applications of quantum computing technology, or some derivative of it, that people are putting to good use right now? Put another way, what does quantum actually do, and whom does it directly serve?

- **Navigation:** A GPS system cannot work everywhere on the planet, particularly underwater. A quantum computer requires atoms to be supercooled and suspended in a state that renders them particularly sensitive. In an effort to capitalize on this, competing teams of scientists are racing to develop a kind of quantum accelerometer that could yield very precise movement data. One promising effort to that end

comes from France's Laboratoire de Photonique Numérique et Nanosciences: An effort to build a hybrid component that pairs a quantum accelerometer with a classical one, then uses a high-pass filter to subtract the classical data from the quantum data. The result, if realized, would be an extremely precise quantum compass that would eliminate the bias and scale factor drifts commonly associated with gyroscopic components.

- **Seismology:** That same extreme sensitivity may also be exploited to detect the presence of oil and gas deposits, as well as potential seismic activity, in places where conventional sensors have to date been unable to explore. This is according to QuantIC, the quantum imaging technology hub led by the University of Glasgow. In July 2017, working with commercial photonics tools provider M Squared, QuantIC demonstrated how a quantum gravimeter detects the presence of deeply hidden objects by measuring disturbances in the gravitational field. If such a device becomes not only practical but portable, the team believes it could become invaluable in an early warning system for predicting seismic events and tsunamis.
- **Pharmaceuticals:** At the leading edge of research into tackling diseases such as Alzheimer's and multiple sclerosis, scientists have been utilizing software that models the behavior of artificial antibodies at the molecular level. Neuroscience firm Biogen has been partnering with IT consultancy Accenture and quantum computing research firm 1QBit to frame a new molecular simulation model in such a way that it can be executed on classical platforms, as well as present and future quantum platforms. One methodology developed by 1QBit's researchers involves translating traditional molecular diagrams into graphs full of dots, lines, and curves that, while seemingly more confusing on the surface, map more directly to a quantum model of vectors and relationships.

Now to the more controversial question: Assume someone built a mechanism that successfully leaps over the hurdles imposed by quantum physics, producing a full quantum computer capable of performing all the tasks currently relegated to the realm of theory and simulation. What do experts in this field think a quantum computer should be able to do, assuming every phenomenon that physicists have theorized and that scientists have observed and verified, is ultimately exploitable?



Prof. Richard Feynman, Caltech, approx. 1983

- **Physics:** This one should be obvious enough. It's actually the reason for the concept's very existence. During a 1981 speech at Caltech, Prof. Richard Feynman, the father of quantum electrodynamics (QED), suggested that the only way to build a

successful simulation of the physical world at the quantum level would be with a machine that obeyed the laws of quantum mechanics. It was during that speech that Prof. Feynman explained, and the rest of the world came to realize, that it would not be enough for a computer to generate a probability table and, as it were, roll dice. Moreover, it would take a mechanism that behaved along the same lines as the behavior it would purport to simulate, to produce results that physicists themselves wouldn't dismiss as apocryphal.

- **Machine learning:** If and when quantum computers ever become stable enough to support thousands of qubits, algorithms for machine learning are standing by, having been thoroughly tested on paper and in simulators. The basic theory among proponents is that quantum systems may be geared to 'learn' patterns of states in huge, concurrent waves rather than successive, sequential scans. If you were awake for the preceding paragraph, you already know what the problem is here: Paper, like electronic computers, is a classical system. Conventional mathematics can circumscribe a set of probable quantum outcomes, as vectors in a wildly configurational space. Yet it cannot -- as Richard Feynman made clear from the very beginning -- simulate how those outcomes may be attained. The first signs of general doubt among experts that quantum machine learning may even be possible were gently seeded into a report from MIT in October 2018 on a panel convened with IBM, where experts admitted that even after quantum computers become reality, several more years may pass before enough stable qubits make quantum machine learning feasible.
- **Decryption:** Here, at last, is the breakthrough that cast the first bright spotlight on quantum computing. What makes encryption codes so difficult even for modern classical computers to break is the fact that they're based on factors of extremely large numbers, requiring inordinate amounts of time to isolate by 'brute force'. An operational quantum computer should isolate and identify such factors in mere moments, rendering the RSA system of encoding effectively obsolete. In 1994, MIT Professor Peter Shor devised a quantum algorithm for factoring values, which experimenters building low-qubit quantum systems have already tested successfully, albeit with rather small quantities. When large-qubit quantum computers are successfully built, few doubt the power of Shor's Algorithm to knock down all current public key cryptography.
- **Encryption:** But herein, some say, lies an opportunity: A concept called quantum key distribution (QKD) holds out the theoretical hope that the kinds of public and private keys we use today to encrypt communications may be replaced with quantum keys that are subject to the effects of entanglement. Theoretically, any third party breaking the key and attempting to read the message would immediately destroy the message for everyone. Granted, that may be enough mischief right there. But the theory of QKD is based on a huge assumption which has yet to be tested in the real world: That values produced with entangled qubits are themselves entangled and subject to quantum effects wherever they go.

WHO IS IN THE RACE TO BUILD QUANTUM COMPUTERS?

Despite certain people's best efforts, the modern economy remains global. The laboratories, universities, and manufacturers with an interest in quantum have their own interests across the globe. So there is no genuine country-versus-country 'arms race' to build the first complete quantum computer.

One private firm with real contracts, including with US Government agencies, that produces devices that perform one form of quantum computing, called quantum annealing, is D-Wave Systems Inc. D-Wave produces a commercial system which it claims is capable of sustaining over 5,000 qubits -- substantially greater than other researchers claim thus far. While some continue to openly dispute this claim (specifically, they cast doubt on the 'quantum-ness' of its results), it's worth noting that D-Wave's partners in the Quantum Artificial Intelligence Laboratory (QuAIL) are NASA and Google; and its partners in the Quantum Computation Center (QCC) are Lockheed Martin and the University of Southern California.

Microsoft participates in quantum research laboratories worldwide, including areas in which you wouldn't think Microsoft would have an interest, such as materials for quantum computer substrates. The company funds and actively supports quantum computing research, and to promote the concepts of quantum algorithms, in December 2017, Microsoft released a quantum simulator and development kit, complete with a domain-specific programming language called Q#, all of which are freely downloadable and may be integrated with Visual Studio or VS Code.

IBM's Think Q team working at its Watson Research Lab in New York.

IBM lays a valid claim to having built several functional quantum processing devices, though currently limited to a 65-qubit array at best. Like Microsoft, IBM offers an open source developers' kit called Qiskit, and invites individuals to experiment with producing quantum algorithms using its 32-qubit simulator. IBM's quantum computing roadmap includes a 127-qubit Eagle processor in 2021, a 433-qubit Osprey system in 2022, and a 1,121-qubit Condor processor in 2023. The ultimate goal, some unspecified time in the future, is a million-plus qubit device.

Intel has been working on quantum computing devices like the 17-qubit prototype at left, using processes that are not significantly different from fabricating conventional superconductors. The catch is that Intel seeks to replace the conventional model of the qubit, which is superconductive and thus requires supercooling, with a more temperature-tolerant alternative it calls a spin qubit. In June 2018, at the company's D1D fabrication facility just outside of Portland, Oregon, Intel produced a test chip claimed to be capable of sustaining qubits at the 'milder' temperature of one degree kelvin. Such a chip cannot yet, however, be considered a full quantum processor. Intel's current 3rd generation Tangle Lake quantum processor has 49 superconducting qubits.

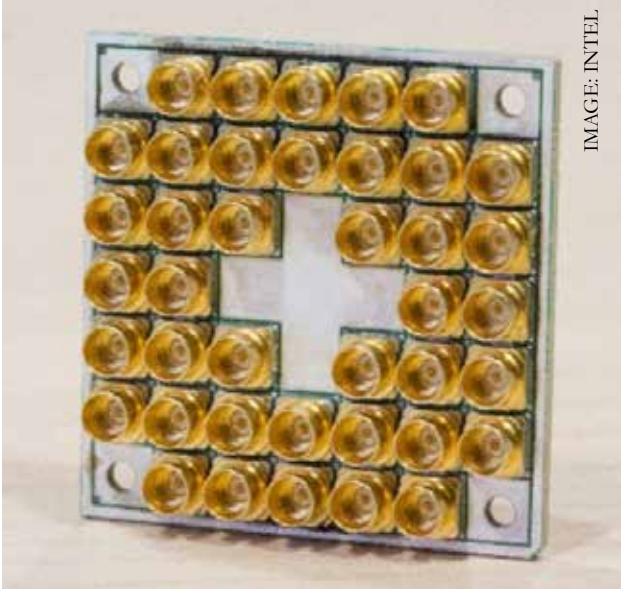


IMAGE: INTEL

The socket end of an Intel prototype quantum computing chip.

In April 2016, the European Union launched a project it calls Quantum Technologies Flagship, with the aim of boosting quantum computing research and development throughout Europe. In October 2018, as part of this effort, the Flagship announced the start of some 20 related projects for this effort, including one called the Quantum Internet Alliance (QIA). Its goal is no less than the conceptualization of a fully entangled global network, theoretically enabling the instantaneous transmission of qubits between repeating stations.

WHAT A QUANTUM COMPUTER PROBABLY IS

The word 'computer' here has a very basic context -- not a handheld device or a cooled server with a processor and memory. Think of a computer the way Charles Babbage or John von Neumann considered it: As a mechanism guaranteed to deliver a certain output given a specific set of inputs and a defined configuration. At the deepest microscopic levels of a modern microprocessor, one logic unit is what these fellows would have called a computer.

Bits and qubits

Every classical electronic computer exploits the natural behavior of electrons to produce results in accordance with Boolean logic (for any two specific input states, one certain output state). Here, the basic unit of transaction is the binary digit ('bit'), whose state is either 0 or 1. In a conventional semiconductor, these two states are represented by low and high voltage levels within transistors.

In a quantum computer, the structure is radically different. Its basic unit of registering state is the qubit, which at one level also stores a 0 or 1 state (actually 0 and/or 1, which I'll confuse you with in a moment). Instead of transistors, a quantum computer obtains its qubits by bombarding atoms with electrical fields at perpendicular angles to one another, the result being to line up the ions, but also keep them conveniently and equivalently separated. When these ions are separated by just enough space, their orbiting electrons become the home addresses, if you will, for qubits.

Spin, one way or the other

While a conventional computer focuses on voltage, a quantum system is (passively) concerned with one aspect of electrons at the quantum level, called spin. Yes, this has to do with the electron's angular momentum. The reason we use the term 'quantum' at the subatomic level of physics is because of the indivisibility of what we may observe, such as the amount of energy in a photon (a particle of light). Spin is one of these delightfully indivisible components, representing the angular momentum of an electron as it orbits the nucleus of an atom. The spin of an electron is always, as physicists calculate it, 1/2; the only difference here is polarity, which very simply may be either 'up' or 'down'.

It's the 'up' or 'down' state of electron spin that corresponds to the '1' and '0' of the typical binary digit. Yet it's here where quantum computing makes a sharp turn into a logical black hole, through a tunnel of white noise, and jettisons us helplessly into a whimsically devious universe whose laws and principles seem concocted by the University of Toontown.

Superposition and why you can't see it

A qubit maintains the quantum state for one electron. When no-one is looking at it, it can attain the '1' and '0' state simultaneously. If you look at it, you won't see this happen, and if it was happening before, it immediately stops. (This is literally true.) Yet the fact that the qubit's electron was spinning both directions at once, is verifiable after the fact. Quantum mechanics calls this simultaneous state of both here and there 'superposition'. It is impossible to witness an electron in a state of superposition because witnessing requires the very exchange of photons that causes such a superposition to collapse.

As one Fordham University lecturer put it, "We don't understand this, but get used to it."

There are multiple possible states of superposition. Here is why each additional qubit in a quantum system is more influential than the last: In a system with n qubits, the number of possible superposition states for each qubit is 2 to the power n. If you remember the history of binary computers, when 16-bit processors were first replaced with 32-bit processors, suddenly a byte's maximum unsigned value was no longer 65,535 but 4,294,967,295. In a quantum system, each qubit in a 32-unit rack of atoms would have 4,294,967,296 possible superposition states.

Why does this matter, if the final state only collapses to 0 or 1 anyway when someone or something takes the bold step of just looking at the thing? Because before that collapse takes place, each of these states is a valid, possible value. (This is why you don't hear a lot about quantum computers needing much memory.) During that strange, black-box period where it can work unobserved and undisturbed, a quantum processor is capable of performing real algorithmic functions on units that are much less like binary digits than they are like wheels in one of Charles Babbage's difference engines -- except with billions of settings rather than just 10.

Instead of giant wheels, quantum engineers have chosen a better way of representing qubits' spin states. More specifically, they borrowed it from a Swiss emigrant physicist to the US, Felix Bloch, who shared the 1952 Nobel Prize in physics for discovering the principle of nuclear magnetic resonance. If you can imagine a billiard ball with one dot, and an imaginary line from the core of the ball through the center of the dot and outward as a vector, then you can picture a Bloch sphere like the one shown at right. Each superposition state a qubit may take may be represented by a vector in a Bloch sphere, which you can think of in terms of angles along the x and y axes of the sphere. Using ordinary geometry, the vector may be expressed as a function of the cosine of that angle to the z axis, added to the sine of that angle to the z axis.

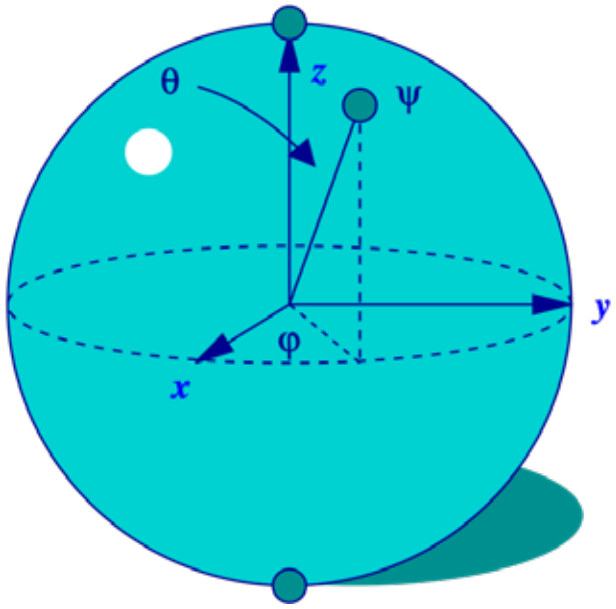


IMAGE: LICENSED UNDER CREATIVE COMMONS

WHAT THE FIRST QUANTUM PROGRAMS WILL LOOK LIKE

The trick in writing a quantum algorithm is to imagine that you could actually see, or measure, qubits in their superposition states, so that you can instruct them as to what happens next and cause adjustments to those states. In reality, the very act of attempting to witness superposition results in decoherence -- the reversion of qubits to their classical 0 or 1 states. Decoherence always happens eventually to a quantum system, often after a few minutes, or if you're lucky, in under an hour.

The whole point of a quantum program becomes to take full advantage of the ability to manipulate which way all these billiard balls are pointing while no-one is looking, prior to their decoherence. There are two types of quantum programs, which function very differently from one another:

- A program using **quantum gates** follows Richard Feynman's original suggestion: That there are other forms of logic within the quantum space. With a binary computer, an AND or an OR gate would take

two discrete voltage inputs as bits and yield one certain output. With gates in a quantum circuit -- the quantum counterpart of a classical electrical circuit -- several qubits may be used as inputs, and the result may be some form of a superposition state, which the Bloch sphere representation breaks down into mathematical values -- including, quite likely, complex numbers.

- A **quantum annealing** system, such as the kind D-Wave currently produces, takes a very different route. Instead of establishing a quantum circuit, an annealer translates formulas (called 'Hamiltonians') that describe the physical state of the quantum system, into actual physical states. While any quantum computer may use one Hamiltonian to describe the initial state, an annealer uses successive Hamiltonians to represent minute changes in the desired state of the system, in very incremental steps along the way to the final desired state. Each step knocks the qubits around, in such a way that their state at the final step represents the set of probabilities that form the final solution. (One researcher likened this to shaking marbles around in an egg crate, with each shake perfectly programmed.) Skeptics of this process are wont to point out that this is not the system Feynman first proposed, and thus either directly assert that an annealing system is not a true quantum computer, or indirectly suggest that no real quantum computer presently exists. It's fair to assume such skeptics do not presently have contracts with NASA, Google, or Lockheed Martin.

THE REAL PROSPECTS FOR A QUANTUM ECOSYSTEM

If every 'revolutionary' technology were guaranteed financial or market success, you'd be holding in your hand today a voice-controlled edge processor with 3D transistors powered by a dime-sized superconductor with a half-century lifespan, rather than whatever it is you're using now.

Quantum computing will not truly succeed, even when it does completely exist, unless there's a viable business model for it. It's often presented with enough bombast that you might think customers would form queues around city blocks waiting for it to arrive. But because a full quantum computer is not, nor ever will be, portable (unlike a quantum compass, where detecting disturbances is the actual goal), the only way to make it commercial is by offering it as a service, similar to how laboratories and universities offer supercomputer services today.

It would not be a 'quantum cloud'. Cloud computing implies some kind of tenancy, a leasing of virtual computing capacity or, in the case of so-called serverless technology, the use of a solution. There is no division of tenancy in the quantum space; it sets up the Hamiltonian situation, runs the algorithm or the annealing pattern, lets the system blow up, and renders the results as likelihoods. Time is not a factor; a harder problem may not take measurably longer than a simpler one -- so leasing on a per-minute basis is pointless.

Which leaves the per-solution option, similar to serverless. But since solutions are probabilities rather than certainties, and subject to variations, inevitably customers will question the value of the solutions they're getting. If they have to pay by the solution, they're not looking for a deal like 'Bertie Bott's Every Flavor Beans' where one flavor may be blueberry and the next earwax. At some point, quality of service will inevitably enter the discussion.

It would appear that quantum computing's early adopters would probably include all those folks looking to demolish RSA-based cryptography at the first opportunity. But for the makers of quantum computers to start profiting from them, they'll want a more stable customer base than just wannabe hackers or former superpower countries with unresolved grief issues. They'll need to foster communities of scientific and educational developers willing to learn the rules and practices of a completely new universe, so they can contribute solutions to the previously unfathomable problems facing our own world.

QUANTUM COMPUTING HAS ARRIVED, BUT WE STILL DON'T REALLY KNOW WHAT TO DO WITH IT

Even for a technology that makes a virtue of uncertainty, where quantum goes next is something of a mystery.

BY DAPHNE LEPRINCE-RINGUET/ZDNET

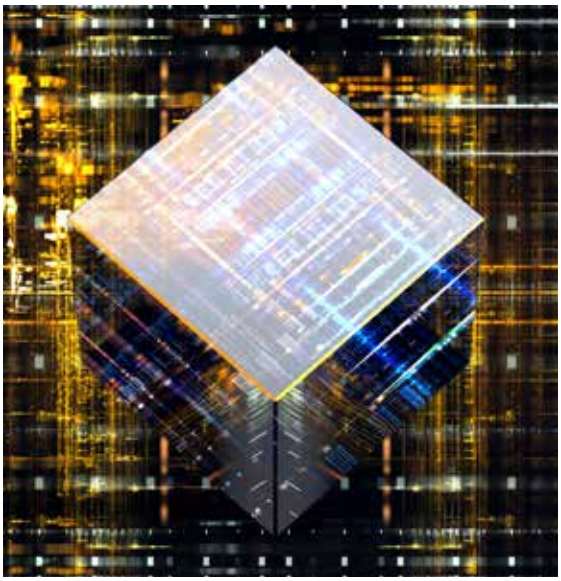


IMAGE: ISTOCKPHOTO/NIPLOT

As of 2020, the UK is over half-way through a ten-year national programme designed to boost quantum technologies, which has so far benefited from a combined £1 billion investment from government and industry. The verdict? Quantum has a lot of potential -- but we're not sure what for.

Speaking at a conference in London, Claire Cramer, from the US Department of Energy, said: "There is a lot of promise in quantum, but we don't have a transformative solution yet. In reality, we don't know what impact the technology will have."

That's not to say, of course, that the past six years have been a failure. Quite the opposite: researchers around the world can now effectively trial and test quantum technology, because the hardware has been developed. In other words, quantum computers are no longer a feat of the imagination. The devices exist, and that in itself is a milestone.

At the Consumer Electronics Show in January 2020, IBM went to great lengths to remind the public that the IBM Q System One -- a 20-qubit quantum computer that the company says is capable of performing reliable quantum computations -- is gaining more momentum among researchers.

The Q System One has been deployed to 15 companies and laboratories so far, as a prototype that research teams can run to work out how quantum computers may be used to solve problems in the future.

Finding out what those problems might be is quantum's next challenge. Liam Blackwell, deputy director at the Engineering and Physical Sciences Research Council (EPSRC), said: "A lot of money has been invested, and we need to start seeing actual outcomes that will benefit the UK. The challenge now, really, is that we have to deliver."

Research teams are not leaping into the unknown: there are already a few potential applications of quantum technology that have been put forward, ranging from enhancing security with quantum cryptography to improving the accuracy of GPS.

Pharmaceuticals and drug discovery have also been identified as fields that could hugely benefit from the new technology. In 2018, for example, neuroscience firm Biogen partnered with quantum computing research firm 1QBit to better tackle diseases like Alzheimer's and multiple sclerosis.

For Cramer, though, this is only scratching the surface. "Look at laser technology, for example," she said. "Seventy years ago, people didn't think lasers could even exist, and now you wouldn't think twice about holding a laser pointer in your hand.

"It's the same thing with quantum. We can't imagine what the transformative applications will be yet; so we need to maintain a culture of discovery."

There is only one secret to achieve a successful "culture of discovery", Cramer continued: research, research, and more research. In the US, for example, the Department of Commerce created the Quantum Economic Development Consortium (QEDC) in 2018. Its objectives? To "identify technology solutions" and "highlight use cases and grand challenges to accelerate development efforts".

But it's not enough to pump money into labs. Once blue-sky research has come up with an unexplored application of quantum, the idea must still be commercialised -- and bridging between labs and industry can be easier said than done.

In the UK, the issue is not confined to quantum technology. A report by VC company Octopus Ventures showed that trillions of pounds are lost every year because of the difficulty of taking new ideas from university labs to the stock exchange.

In contrast, in the US, over 26,000 companies started in research teams from the Massachusetts Institute of Technology (MIT). Combined, these businesses have an annual turnaround of over $2 trillion (£1.5 trillion).

"The UK has a very strong lead on research in quantum, but we have lessons to learn from the US," said Elham Kashefi, professor of computer science at the University of Edinburgh. "We need to push research to the next level, to connect it to industry."

The UK Research and Innovation (UKRI), an organisation that directs innovation funding through the budget of the Department for Business, Energy and Industrial Strategy, has stressed that commercialising quantum technology would be a priority.

UKRI invested £20 million in "pioneer funding" for start-ups leveraging quantum technology to develop "products of the future". Four projects benefited from the award to develop prototypes ranging from quantum sensors that can detect objects underground, to encryption tools that keep data safe.

UKRI is now investing another £153 million in new projects, alongside a £205 million investment from industry. Presenting the organisation's plans for the future, UKRI's director for quantum technologies, Roger McKinlay, said: "I don't know what's coming next, but I hope that we can continue to support what I believe is by far the most interesting emerging technology at the moment."

Quantum uncertainty may not be resolved anytime soon -- but it's certainly worth watching

CIO JURY: HOW QUANTUM COMPUTING WILL AFFECT THE ENTERPRISE

The impact of quantum computing is a popular topic. Some industries expect to see more changes from it than others.

BY TEENA MADDOX/TECHREPUBLIC

Quantum computing allows companies to take a new approach to analyzing information. It offers the enterprise an opportunity to process data and solve problems never before possible. Because of the incredible possibilities of quantum computing, vendors such as IBM, Microsoft, Google, Rigetti Computing and IonQ are among those in a race for quantum supremacy.

IMAGE: GETTY IMAGES/ISTOCKPHOTO

This month, our CIO Jury was asked, "Do you expect quantum computing to have a significant impact on your industry in the next five years?" Four out of six tech leaders, or 67%, said no, while two, or 33%, said yes.

Kent Blackwell, threat and vulnerability assessment manager, Schellman & Company, LLC, expects quantum to have an impact on his industry, particularly since it's already commercially available in the cloud.

Blackwell said, "Quantum computing promises to solve problems and drive simulations that have been computationally or physically intractable with conventional hardware, such as simulating the interactions of a novel pharmaceutical in vivo, creating secret messages that destroy themselves when read, or covertly monitoring remote systems without the need for an internet connection. This may all sound well and good, except for the fact that internet security is, for the most part, predicated on the following assumption: It is hard to factor large numbers into their prime components."

A "yes" vote came from Fortinet CISO Phil Quade. He said, "Quantum computers themselves will have little or no significant impact in the next five years. But the preparations for their eventuality are hugely important now. Here's why: Viable, operational quantum computers, that have both a sufficient number of qubit computational capability and a reliable, sustainable power and environmental infrastructures, are still several years

away. But even so, users of security products are already late-to-need in preparing for their eventuality, because of the time and complexity of replacing crypto algorithms. Quantum computers will render breakable an important type of encryption (called asymmetric cryptography) that is used worldwide to establish confidentiality keys and do integrity checks, on which our whole economy and society depends. We need to implement crypto agility now—as part of a broader strategy that embraces security agility – so that quantum-resistant algorithms can be quickly deployed in crypto-agile systems when those algorithms become available."

Quantum won't have a big impact on the banking industry, according to John Gracyalny, vice president of digital member services for Coast Central Credit Union.

Gracyalny said, "Banking tends to be very conservative in adopting new technology, one good example being blockchain, which is still in the 'talk about' stage. And I don't think quantum computing will be ready to have a viable fintech product based on it for maybe 10 years. As with blockchain, one potential attraction of quantum computing is that it is supposedly unhackable.

"The sad reality is that the vast preponderance of banking related data breaches that make the news are caused by the human element being careless, clueless, complacent, complicit, or coerced. And technology won't help you there," Gracyalny said.

Here are this month's CIO Jury participants:

- *John Gracyalny, vice president of digital member services, Coast Central Credit Union*
- *Randy Krzyston, senior manager, IT security and compliance, Brinks Home Security*
- *Phil Quade, CISO, Fortinet*
- *Michael Hanken, vice president of IT, Multiquip*
- *Cory Wilburn, CIO, Texas General Land Office*
- *Kent Blackwell, threat and vulnerability assessment manager, Schellman & Company, LLC*

QUANTUM COMPUTING: FIVE WAYS YOU CAN GET INVOLVED

Getting involved in quantum might seem like a daunting prospect for CIOs. Here are five expert tips to kickstart the process.

BY DAPHNE LEPRINCE-RINGUET/ZDNET

Any modern-day CIO who has been keeping an alert eye on the latest trends will, at one point, have come across quantum technologies.

And while grasping the peculiarities of qubit behavior might be out of reach for some, a PhD in quantum mechanics isn't necessary to understand that this technology could disrupt entire industries during the next decade thanks to the building of unprecedented quantum compute power.

From financial services to agriculture, the extraordinary properties of quantum computing are set to improve efficiencies and boost productivity, to save time and cut costs, solving in minutes the problems that classical computers are incapable of harnessing.

IMAGE: ISTOCKPHOTO/NIPLOT

The pitch certainly sounds promising, and the benefits that could be reaped from quantum can easily seem marvellous. In other words, there is little reason to not want to get involved.

But getting started with quantum computing is no easy thing. Here are the first steps that decision makers can take now to kick-start their business's quantum experiment.

1. Work out the relevant use cases for your business

It might seem obvious, but the first place to start is to discover what problems quantum technology might be able to solve. Business leaders need to develop a roadmap of potential use cases that reflect how value can be captured both in the short and the long term.

"The nearest-term use case to consider is machine learning," Christopher Savoie, CEO of quantum software company Zapata, tells ZDNet. "Quantum computing could massively accelerate capabilities in this area. If your company has an artificial intelligence or a machine-learning strategy, that strategy should include quantum computing."

A good idea is to identify spaces that currently require a lot of high-performance and complex computing, and lay out the tasks that might benefit from quantum capabilities. As Savoie explains, these spaces are likely to include quantum-enhanced databases for AI; but it is also worth paying attention to the optimization of supply-chains, or molecular developments in chemistry and pharmaceuticals.

2. Start building your quantum workforce

One of the keys to deploying quantum technology is access to quantum-trained staff. "You need to understand the level of knowledge and expertise in the company," says Heike Riel, head of science and technology at IBM Research Quantum Europe. "We are going into a future where, as quantum computing becomes more important, it'll be crucial to develop quantum expertise in your own company."

Qualified talent will be essential to identify and execute the right use cases for the technology. And since quantum-capable employees aren't exactly in the mainstream yet, securing and retaining talent should be a priority. This can be done, for example, via partnerships with universities and specialized consultancies, but also by upskilling existing staff.

3. Know your way around the quantum ecosystem

The quantum space is growing increasingly crowded with companies small and big, which are all offering different services. It is easy to get lost between abstract concepts such as quantum volume, annealing processors, emulators and simulators, not to mention trapped-ions, gate-model systems and quantum algorithms.

Zapata's Savoie tells ZDNet: "Against this background of uncertainty, it can be hard to answer questions like: which hardware is best? Which software works best with which hardware? Which problems should I pursue first for my business? Finally, if I do invest, who is going to do the actual work?"

CIOs have to ask those questions and do the research to make sure that they know, even before they start browsing, what technology stack and capabilities they will need to solve industry problems. From there, it will be easier to figure out who the right partners are and how those partners can make sure that experiments move at speed and scale.

4. Adopt a flexible set of tools and technologies

It is unlikely that many organizations will want, or be able, to invest in pure quantum hardware from the get-go. The technical infrastructure, at least to start with, will probably be a hybrid of cloud-based quantum hardware and classical computers.

Since multiple options already exist, it might also be a good idea to diversify the sources of hardware, while always keeping an eye on emerging players in the field that might come up with innovative solutions. Recent

months, for example, have seen promising silicon-based photonic developers looking at brand-new ways of manufacturing universal quantum computers.

"The fact that quantum computing technology is still evolving can make it challenging," says Savoie. "There's a lot to consider and no one wants to get locked into a single vendor framework or invest in a particular technology that turns out to be a dead end."

5. Don't set the bar too high

Quantum computing will not deliver business value in the near-term, because quantum computers are not powerful enough yet. Rather, businesses should engage with the technology with an eye to being first in line to reap benefits when a large-scale quantum computer is ready.

Honeywell quantum solutions' president Tony Uttley suggests starting with small-scale problems that classical computers can already solve in order to test and validate the usefulness of quantum for those specific use cases.

As capabilities increase, so will the size of the problem that the quantum computer can solve – until qubits start running applications that classical computers cannot. "You can plot out when quantum is going to have a meaningful impact on your business," Uttley tells ZDNet. "And by planning it now, you are able to integrate it into your infrastructure. The proof-of-concept algorithms being run today will become meaningful executive-level business decisions."

That is the point that businesses should be working towards now. Uttley believes that the next 18 to 24 months could bring very early results. The quantum race is on.

QUANTUM COMPUTERS COULD SOON REVEAL ALL OF OUR SECRETS. THE RACE IS ON TO STOP THAT HAPPENING

Although the threat is at least ten years off, governments and businesses are gearing up security to prepare for the quantum age.

BY DAPHNE LEPRINCE-RINGUET/ZDNET

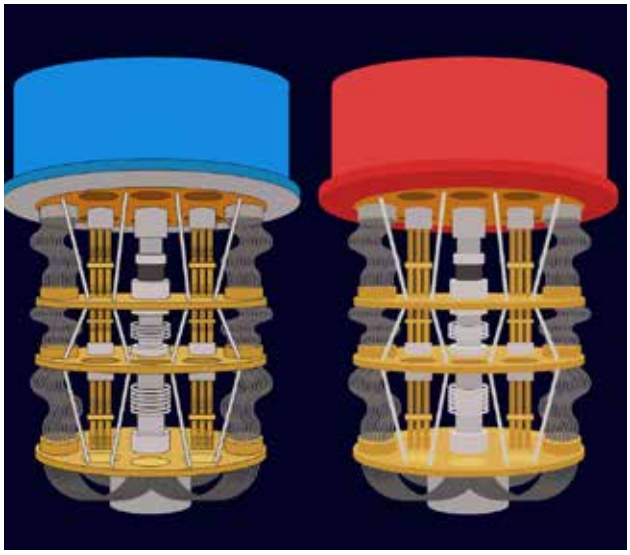


IMAGE: ISTOCKPHOTO/ADAPTROGRAPHICS

A fully-fledged quantum computer that can be used to solve real-world problems: for many computer scientists, the arrival of such a device would be their version of the Moon landings; the final achievement after many decades of research – and the start of a new era.

For companies, the development could unlock huge amounts of wealth, as business problems previously intractable for classical computers are resolved in minutes. For scientists in the lab, it could expedite research into the design of life-saving drugs.

But for cryptographers, that same day will be a deadline – and a rather scary one. With the compute power that they will be capable of, large-scale quantum devices effectively pose an existential threat to the security protocols that currently protect most of our data, from private voice notes all the way to government secrets.

The encryption methods that are used today to transform data into an unreadable mush for anyone but the intended recipients are essentially a huge maths problem. Classical computers aren't capable of solving the equation in any useful time frame; add some quantum compute power, though, and all of this carefully encoded data could turn into crystal-clear, readable information.

At the heart of the problem is public key encryption – the protocol that is used to encode a piece of data when it is sent from one person to another, in a way that only the person on the receiving end of the message can decode. In this system, each person has a private cryptography key as well as a public one, both of which are generated by the same algorithm and inextricably tied to each other.

The publicly-available key can be used by any sender to encrypt the data that they would like to transmit. Once

the message has arrived, the owner of the key can then use their private key to decrypt the encoded information. The security of the system is based on the difficulty of figuring out a person's private key based on their public one, because solving that problem involves factoring huge amounts of numbers.

Inconveniently, if there is one thing that quantum computers will be good at, it is crunching numbers. Leveraging the quasi-supernatural behavior of particles when taken in their smallest state, quantum devices are expected to one day breeze through problems that would take current supercomputers years to resolve.


IMAGE: IBM

Researchers have developed quantum algorithms that can, in theory, break public-key cryptography systems.

That's bad news for the security systems that rely on presumably difficult mathematics. "The underlying security assumptions in classical public-key cryptography systems are not, in general, quantum-secure," says Niraj Kumar, a researcher in secure communications from the school of informatics at the University of Edinburgh.

"It has been shown, based on attacks to these keys, that if there is quantum access to these devices, then these systems no longer remain secure and they are broken."

But as worrying as it sounds, explains Kumar, the idea that all of our data might be at risk from quantum attacks is still very much theoretical. Researchers have developed quantum algorithms that can, in theory, break public-key cryptography systems, such as Shor's algorithm, but they are subject to no small condition: that the algorithms operate in a quantum computer with a sufficient number of qubits, without falling to noise or decoherence.

In other words, a quantum attack on public-key cryptography systems requires a powerful quantum computer, and such a device is not on any researcher's near-term horizon. Companies involved in the field are currently sitting on computers of the order of less than 100 qubits; in comparison, recent studies have shown that it would take about 20 million qubits to break the algorithms behind public-key cryptography.

Kumar, like most researchers in the field, doesn't expect a quantum device to reach a meaningful number of qubits before the next ten or 20 years. "The general consensus is that it is still very much a thing of the future," he says. "We're talking about it probably being decades away. So any classical public-key cryptography scheme used for secure message transmission is not under imminent threat."

NIST, the US National Institute of Standards and Technology, for its part estimates that the first quantum computer that could pose a threat to the algorithms that are currently used to produce encryption keys could be built by 2030.

Don't let the timeline fool you, however: as long as a decade sounds, quantum-safe cryptography is not a problem that can be relegated to future generations. Some of the systems that are being deployed now will effectively protect data that will still need to be safe in ten years. The most obvious example is ultra-secret government communications, which will need to remain confidential for the next few decades.

This type of data needs to be protected now with protocols that will withstand quantum attacks when they become a reality. Governments around the world, in fact, are already acting on the quantum imperative: in the UK, for example, the National Cyber Security Centre (NCSC) has established for several years now that it is necessary to end reliance on current cryptography protocols, and to start the transition to what is known as "quantum-safe cryptography".

Similarly, the US National Security Agency (NSA), which currently uses a set of algorithms called Suite B to protect top secret information, has determined since 2015 that it was time to start planning the transition towards quantum-resistant algorithms.

As a direct result of the NSA's announcement five years ago, a global research effort into new quantum-safe cryptography protocols started in 2016, largely led by NIST in the US. The goal? To make classical public-key cryptography too difficult a problem to solve, even for a quantum computer – an active research field now called post-quantum cryptography.

NIST launched a call for help to the public, asking researchers to submit ideas for new algorithms that would be less susceptible to a quantum computer's attack. Of the 69 submissions that the organization received at the time, a group of 15 was recently selected by NIST as showing the most promise.

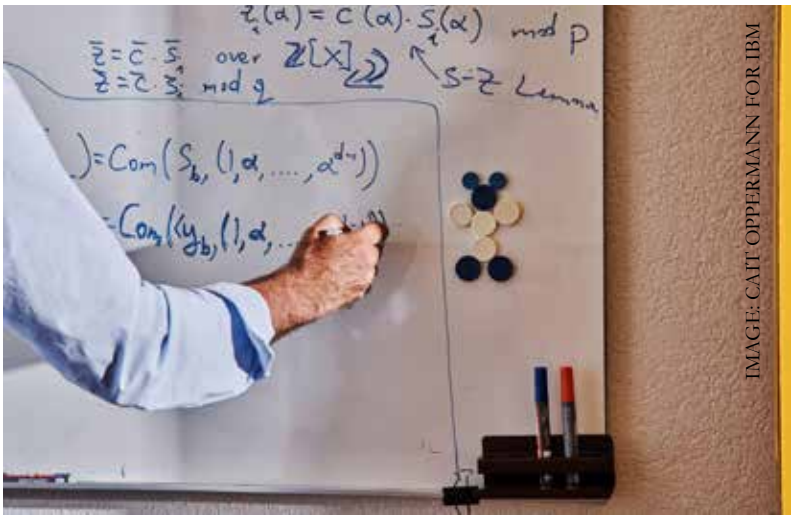
There are various mathematical approaches to post-quantum cryptography, which in essence consist of making the problem harder to crack at different points in the encryption and decryption processes. Some post-quantum algorithms are designed to safeguard the key agreement process, for example, while others ensure quantum-safe authentication thanks to digital signatures.

The technologies form an array of bizarrely named methods, including lattices, polynomials, hashes, isogenies, or elliptic curves, but they share a similar gist: to build algorithms robust enough that they will be quantum-proof.

The 15 algorithms selected by NIST this year are set to go through another round of review, after which the organization hopes to standardize some of the proposals. Before 2024, NIST plans to have set up the core of the first post-quantum cryptography standards.

The UK's NCSC and the US's NSA have both made it clear that they will start transitioning to post-quantum cryptography protocols as soon as such standards are in place. But government agencies are not the only organizations showing interest in the field. Vadim Lyubashevsky, from IBM Research's security group, explains that many players in different industries are also patiently waiting for post-quantum cryptography standards to emerge.

"This is becoming a big thing, and I would say certainly that everyone in the relevant industries is aware of it," says Lyubashevsky. "If you're a car manufacturer, for example, you're making plans now for a product that will be built in five years and will be on the road for the next ten years. You have to think 15 years ahead of time, so now you're a bit concerned about what goes in your car."



For IBM's Vadim Lyubashevsky, many players in different industries are patiently waiting for post-quantum cryptography standards to emerge.

Any product that might still be in the market in the next couple of decades is likely to require protection against quantum attacks – think aeroplanes, autonomous vehicles and trains, but also nuclear plants, IoT devices, banking systems or critical telecommunications infrastructure.

Businesses, in general, have remained quiet about their own efforts to develop post-quantum cryptography processes, but Lyubashevsky is positive that concern is mounting among those most likely to be affected. JP Morgan Chase, for example, recently joined research hub the Chicago Quantum Exchange, mentioning as it did that the bank's research team is "actively working" in the area of post-quantum cryptography.

That is not to say that quantum-safe algorithms should be top-of-mind for every company that deals with potentially sensitive data. "What people are saying right now is that threat could be 20 years away," says Lyubashevsky. "Some information, like my credit card data for example – I don't really care if it becomes public in 20 years. There isn't a burning rush to switch to post-quantum cryptography, which is why some people aren't pressed to do so right now."

Of course, things might change quickly. Tech giants like IBM are publishing ambitious roadmaps to scale up their quantum-computing capabilities, and the quantum ecosystem is growing at pace. If milestones are achieved accordingly, predicts Lyubashevsky, the next few years might act as a wake-up call for decision makers.

Consultancies like security company ISARA are already popping up to provide businesses with advice on

the best course of action when it comes to post-quantum cryptography. In a more pessimistic perspective, however, Lyubashevsky points out that it might, in some cases, already be too late.

"It's a very negative point of view," says the researcher, "but in a way, you could argue we've already been hacked. Attackers could be intercepting all of our data and storing it all, waiting for a quantum computer to come along. We could've already been broken – the attacker just hasn't used the data yet."

Lyubashevsky is far from being the only expert to discuss this possibility, and the method even has a name: "harvest and decrypt". The practise is essentially an espionage technique, and as such mostly concerns government secrets. Lyubashevsky, for one, is convinced that state-sponsored attackers are already harvesting confidential encrypted information about other nations, and sitting on it in anticipation of a future quantum computer that would crack the data open.

For the researcher, there is no doubt that governments around the world are already preparing against harvest-and-decrypt attacks – and as reassuring as it would be to think so, there won't be a way to find out for at least the next ten years. One thing is for certain, however: for unaware businesses and organizations, the quantum revolution might come with some nasty security surprises.

8 COMPANIES LEADING IN QUANTUM COMPUTING ENDEAVORS IN 2020

Organizations investing in quantum cite improved AI capabilities, accelerated business intelligence, and increased productivity and efficiency, according to IDC.

BY ESTHER SHEIN/TECHREPUBLIC CONTRIBUTOR

Use of quantum computers has grown over the past several months as researchers have relied on these systems to make sense of the massive amounts of data related to the COVID-19 virus.

IMAGE: ISTOCKPHOTO/NOBI_PRIZUE

Quantum computers are based on qubits, a unit that can hold more data than classic binary bits, said Heather West, a senior research analyst at IDC.

Besides better understanding of the virus, manufacturers have been using quantum systems to determine supply and demand on products—like toilet paper—so they can make estimates based on trends, such as how much is being sold in certain geographic areas, she said.

"Quantum computers can help better determine demand and supply, and it allows manufacturers to better push out supplies in a more scientific way," West said. "If there is that push in demand it can also help optimize the manufacturing process and accelerate it and actually modernize it by identifying breakdowns and bottlenecks."

QUANTUM COMPUTING GAINS MOMENTUM

Quantum has gained momentum this year because it has moved from the academic realm to "more commercially evolving ecosystems," West said.

In late 2019, Google claimed that it had reached quantum supremacy, observed Carmen Fontana, an emerging tech practice lead at Centric Consulting. "While there was pushback on this announcement by other leaders in tech, one thing was certain—it garnered many headlines."

Echoing West, Fontana said that until then, "quantum computing had felt to many as largely an academic

exercise with far-off implications. After the announcement, sentiment seemed to shift to 'Quantum computing is real and happening sooner than later.'"

In 2020, there have been more tangible timelines and applications for quantum computing, indicating that the space is rapidly advancing and maturing, Fontana said.

"For instance, IBM announced plans to go from their present 65-qubit computer to a 1,000-qubit computer over the next three years," he said. "Google conducted a large-scale chemical simulation on a quantum computer, demonstrating the practicality of the technology in solving real-world problems."

Improved artificial intelligence (AI) capabilities, accelerated business intelligence, and increased productivity and efficiency were the top expectations cited by organizations currently investing in cloud-based quantum computing technologies, according to a survey IDC conducted earlier this year.

"Initial survey findings indicate that while cloud-based quantum computing is a young market, and allocated funds for quantum computing initiatives are limited (0-2% of IT budgets), end users are optimistic that early investment will result in a competitive advantage," IDC said.

Manufacturing, financial services, and security industries are currently leading the way by experimenting with more potential use cases, developing advanced prototypes, and being further along in their implementation status, according to IDC.

CHALLENGES OF QUANTUM CHALLENGES

Quantum is not without its challenges, though. The biggest one West sees is decoherence, which happens when qubits are exposed to "environmental factors" or too many try to work together at once. Because they are "very, very sensitive," they can lose their power and ability to function, and as result, cause errors in a calculation, she said.

"Right now, that is what many of the vendors are looking to solve with their qubit solutions," West said.

Another issue preventing quantum from becoming more of a mainstream technology right now is the ability to manage the quantum systems. "In order to keep qubits stable, they have to be kept at very cold, subzero temps, and that makes it really difficult for a lot of people to work with them," West said.

Nevertheless, With the time horizon of accessible quantum computing now shrinking to a decade or less, Fontana believes we can expect to see "an explosion of start-ups looking to be first movers in the quantum applications space. These companies will seek to apply quantum's powerful compute power to solve existing problems in novel ways."

COMPANIES FOCUSED ON QUANTUM COMPUTING

Here are eight companies that are already focused on quantum computing.

1. Atom Computing

Atom Computing is a hardware, quantum computing company specializing in neutral atom quantum computers. While it is currently prototyping its first offerings, Atom Computing said it will provide cloud access "to large numbers of very coherent qubits by optically trapping and addressing individual atoms," said Ben Bloom, founder and CEO.

The company also builds and creates "complicated hardware control systems for use in the academic community," Bloom said.

2. Xanadu

Xanadu is a Canadian quantum technology company with the mission to build quantum computers that are useful and available to people everywhere. Founded in 2016, Xanadu is building toward a universal quantum computer using silicon photonic hardware, according to Sepehr Taghavi, corporate development manager.

The company also provides users access to near-term quantum devices through its Xanadu Quantum Cloud (XQC) service. The company also leads the development of PennyLane, an open-source software library for quantum machine learning and application development, Taghavi said.

3. IBM

In 2016, IBM was the first company to put a quantum computer on the cloud. The company has since built up an active community of more than 260,000 registered users, who run more than one billion every day on real hardware and simulators.

In 2017, IBM was the first company to offer universal quantum computing systems via the IBM Q Network. The network now includes more than 125 organization, including Fortune 500s, startups, research labs, and education institutions. Partners include Daimler AG, JPMorgan Chase, and ExxonMobil. All use IBM's most-advanced quantum computers to simulate new materials for batteries, model portfolios and financial risk, and simulate chemistry for new energy technologies, the company said.

By 2023, IBM scientists will deliver a quantum computer with a 1,121-qubit processor, inside a 10-foot tall "super-fridge," that will be online and capable of delivering a Quantum Advantage–the point where certain information processing tasks can be performed more efficiently or cost effectively on a quantum computer, versus a classical one, according to the company.

4. ColdQuanta

ColdQuanta commercializes quantum atomics, which it said is "the next wave of the information age." The company's Quantum Core technology is based on ultra-cold atoms cooled to a temperature of nearly absolute zero; lasers manipulate and control the atoms with extreme precision.

The company manufactures components, instruments, and turnkey systems that address a broad spectrum of applications: Quantum computing, timekeeping, navigation, radiofrequency sensors, and quantum communications. It also develops interface software.

ColdQuanta's global customers include major commercial and defense companies; all branches of the US Department of Defense; national labs operated by the Department of Energy; NASA; NIST; and major universities, the company said.

In April 2020, ColdQuanta was selected by the Defense Advanced Research Projects Agency (DARPA) to develop a scalable, cold-atom-based quantum computing hardware and software platform that can demonstrate quantum advantage on real-world problems.

5. Zapata Computing

Zapata Computing empowers enterprise teams to accelerate quantum solutions and capabilities. It introduced Orquestra, an end-to-end, workflow-based toolset for quantum computing. In addition to previously available backends that include a full range of simulators and classical resources, Orquestra now integrates with Qiskit and IBM Quantum's open quantum systems, Honeywell's System Model HØ, and Amazon Braket, the company said.

The Orquestra workflow platform provides access to Honeywell's HØ, and was designed to enable teams to compose, run, and analyze complex, quantum-enabled workflows and challenging computational solutions at scale, Zapata said. Orquestra is purpose-built for quantum machine learning, optimization, and simulation problems across industries.

6. Azure Quantum

Recently introduced Azure Quantum provides a "one-stop-shop" to create a path to scalable quantum computing, Microsoft said. It is available in preview to select customers and partners through Azure.

For developers, Azure Quantum offers:

- An open ecosystem that enables access to diverse quantum software, hardware, and offerings from Microsoft and it partners: 1QBit, Honeywell, IonQ, and QCI.
- A scalable, and secure platform that will continue to adapt to our rapidly evolving quantum future.

- An ability to have quantum impact today with pre-built applications that run on classical computers--that Microsoft refers to as "quantum-inspired solutions."

7. D-Wave

Founded in 1999, D-Wave claims to be the first company to sell a commercial quantum computer in 2011 and the first to give developers real-time cloud access to quantum processors with Leap, its quantum cloud service.

D-Wave's approach to quantum computing, known as quantum annealing, is best suited to optimization tasks in fields such as AI, logistics, cybersecurity, financial modeling, fault detection, materials sciences, and more. More than 250 early quantum applications have been built to-date using D-Wave's technology, the company said.

The company has seen a lot of momentum in 2020. In February, D-Wave announced the launch of Leap 2, which introduced new tools and features designed to make it easier for developers to build bigger applications. In July, D-Wave expanded access to Leap to India and Australia. In March, D-Wave opened free access to Leap for researchers working on responses to the COVID-19 pandemic. In September, D-Wave launched Advantage, a quantum system designed for business. Advantage has more than 5,000 qubits, 15-way qubit connectivity, and an expanded hybrid solver service to run problems with up to one million variables, the company said. Advantage is accessible through Leap.

8. Strangeworks

Strangeworks, a startup based in Austin, Texas, claims to be lowering the barrier to entry into quantum computing by providing tools for development on all quantum hardware and software platforms. Strangeworks launched in March 2018, and one year later, deployed a beta version of its software platform to users from more than 140 different organizations. Strangeworks will open its initial offering of the platform in Q1 2021, and the enterprise edition is coming in late 2021, according to Steve Gibson, chief strategy officer.

The Strangeworks Quantum Computing platform provides tools to access and program quantum computing devices. The Strangeworks IDE is platform-agnostic, and integrates all hardware, software frameworks, and supporting languages, the company said. To facilitate this goal, Strangeworks manages assembly, integrations, and product updates. Users may share their work privately with collaborators, or publicly. Users' work belongs to them and open sourcing is not required to utilize the Strangeworks platform.

WHAT CLASSIC SOFTWARE DEVELOPERS NEED TO KNOW ABOUT QUANTUM COMPUTING

BM's Quantum Challenge is designed to help classic software programmers become quantum ready developers.

BY BILL DETWILER/TECHREPUBLIC

IBM, Intel, Google, D-Wave and others have made significant advancements in the field of Quantum computing over the past few years, but many hurdles (not all of them technical) exist before the technology can become a practical alternative for businesses. For example, software developers will need to learn new ways of writing programs for quantum computers.

In May this year, IBM hosted its fourth annual Quantum Challenge. The four-day event consisted of four exercises designed to help classic software developers, researchers, and even business users better understand how quantum programming works. Participants were able to use the 18 IBM Quantum systems on the IBM Cloud to complete the exercises and according to IBM during the event the total use of these system "exceeded 1 billion circuits a day." Over 1,745 people from 45 countries participated in the challenge and 574 people actually completed all four exercises

In this installment of Dynamic Developer, I talked with one of the IBM team members who helped put the challenge together. In our conversation, Abe Asfaw, Global Lead, Quantum Education and Open Science at IBM, explain the 2020 Quantum Challenge and the challenges developers face when trying to write programs for quantum computers.

Bill Detwiler: So let's start with what the IBM Quantum Challenge is. Give everybody a breakdown of how it works, how long it's been around, and you know what people do when they participate in it.

Abe Asfaw: Yeah. So the IBM Quantum Challenge is one of our many attempts to make sure that everyone becomes quantum ready, everyone can do quantum computing, can program a quantum computer. So it's a set of four exercises that they can take with their families. And at the end of the day, what we hope to achieve from this process is that everyone is equipped to be able to program a quantum computer.

Bill Detwiler: Yeah. So let's talk about those exercises. What's the first one about?

Abe Asfaw: Sure. So every time you talk about programming a quantum computer, really what you're doing is building a quantum circuit and then running that quantum circuit on the quantum computer. So in the first exercise, what we thought we would do is walk people through this model of computation where we show

what it takes to build a quantum circuit. When you build a quantum circuit, you're putting on quantum gates on different cubits. So we show what each quantum gate does to each qubit and we build up from there.


IMAGE: IBM

Abe Asfaw, Quantum Education Lead, IBM Quantum

Bill Detwiler: Okay. And maybe before we go any further, I guess it would be helpful for folks to know what is it that... how did they get that foundation of knowledge so that they understand the language. Whether you're a seasoned developer trying to learn a new language, whether you're new to programming or new to quantum computers. Is there a way for people to understand, "Okay, so I know what a circuit is. I know what gate means. I understand the terminology in the process."

Abe Asfaw: Yeah. So we have several tools to be able to get you from knowing classical computing to being a quantum ready developer. So one of the things that we do is make an open source textbook available online, and several people have been looking through this textbook. So for this challenge, what we did is take snippets of the textbook and put them in with exercises that walk people through the material, solve a problem, walk through more materials, solve the problem, and gradually you develop that terminology that you mentioned where you go from classical development to quantum development.

BEYOND THE BASICS OF QUANTUM COMPUTING: QUANTUM NOISE, UNDERSTANDING SUPERPOSITION AND QUANTUM KEY DISTRIBUTION

Bill Detwiler: Okay, cool. So you've gone through that first exercise, which helps you understand some of the basics of quantum computing. What's the second exercise that people move to after that?

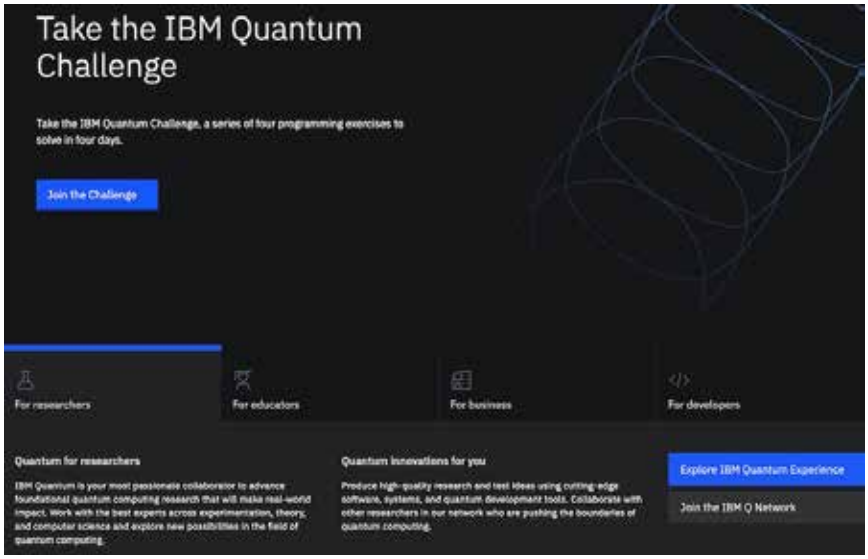
Abe Asfaw: The second exercise is, in my mind, one of the more exciting ones where you go from knowing what a quantum circuit is to then running it on a real quantum computer. So, everyone gets experience running the quantum circuits that they built in the first exercise and the second one. And really the kind of experience that you get from doing that is valuable. Because today's quantum computers are still under development, right? We have things like quantum noise in our systems that we need to learn how to work with. So people get a taste of what it looks like to be able to do things like readout error mitigation. So as you're getting the results back from the quantum computers, how you take those results and interpret them when you have some noise in the quantum system.

Bill Detwiler: What's the best way to think about quantum noise? When people ask you, what does that mean or how does that relate to the regular type of error mitigation that you're doing and programming? How does quantum noise relate to that?

Abe Asfaw: So let me give you an example of a standard error mitigation technique. If you and I are communicating right now and we have a very noisy channel between us, so you kind of hear what I say and maybe there's some blurriness to it. One easy protocol that you and I can take right now is to repeat the communication multiple times. And every time I repeat it, you can measure it and then take a majority vote. It sounds like multiple times I heard him say this, so I'll just assume this is what he said. So that's a standard classical mitigation technique. In quantum mechanics you can't play that game because measuring a quantum state to understand what it was effectively destroys the quantum information and gives you one particular outcome instead of the large superposition of states that would be accessible with a quantum state. So the rules are different now and do you need to employ different error mitigation techniques and we walk people through one of them in this exercise.

Bill Detwiler: Okay, cool. And I would imagine there are a lot of things like that that people new to quantum computing need to wrap their heads around when they start trying to code for quantum computers.

Abe Asfaw: Exactly. So the rules that change now are the things that we're trying to get people used to. As you're doing quantum programming, the two hardest parts to get used to are one, that you simply can't do measurements like you used to be able to do on a real system. And secondly, the rules of quantum mechanics are just so different. Here, instead of using classical computing techniques, what you're doing is taking advantage of superposition, which is the ability to take a quantum state and have it become a combination of different basis states to have interference between quantum states and to have entanglement between quantum systems. So these three rules are very unfamiliar to a classical developer and that's what you have to take advantage of to build quantum algorithms.



IBM Quantum Challenge

Bill Detwiler: So I think that's a great segue. As we talk about entanglement, as we talk about communication moving to exercise three, because that's where you get into one of the big areas where people think quantum computers will play a role in the future, which is cryptography.

Abe Asfaw: Exactly. And in exercise three we walk people through what's called quantum key distribution. And one of the earliest protocols for quantum key distribution is something called BB84. B and B stand for Bennett and Brassard who are the people who came up with this protocol back in 1984. Charlie Bennett still works at IBM and to this day is making a significant impact in the field. So there's a lot of history in this protocol. What we're trying to do here is show as information goes from point a to point b, we call these personalities Alice and Bob, if there's an eavesdropper in the middle who we call Eve, the question is how do you take advantage of quantum mechanics to find out if there was any sort of interference in that communication or if there wasn't. And the key point here is, as I mentioned before, as you're working with quantum states, measuring them drastically affects the quantum states. So you can use this to make sure that your quantum communication is secure.

Bill Detwiler: Right, because the theory would be, and correct me if I'm wrong, that if someone observed those states, you would be able to tell that that had happened and you would know that the communication was not secure.

Abe Asfaw: Exactly. So it's a modification of the classical protocol that you and I discussed earlier about taking a majority vote by doing something repeatedly, except now you add a flavor of quantum mechanics to it, where you say, "If there was a measurement, I know that there was some sort of interference."

Bill Detwiler: And these are some of the news announcements that we saw maybe come out in the last few years. Various agencies talking about being able to create secure communication channels between the earth and satellites, things like that, being able to use quantum computing to try to do that, right?

Abe Asfaw: That's right. So there are many different parts of quantum that are exciting to study. One is quantum computing using quantum to do any sort of information processing, the other is communication itself. And maybe the third part that doesn't get as much media attention but should is sensing, using quantum computers to sense things much more sensitively than you would classically. So think about sensing very small magnetic fields for example. So the communication aspect of it is just as important because at the end of the day it's important to have secure communication between your quantum computers as well. So this is something exciting to look forward to.

Bill Detwiler: Okay, so let's talk about the fourth exercise because that's where I guess you really ramp things up a little bit. Give us a break down of what's involved in that one.

Abe Asfaw: Okay. So this has been the most rewarding part of designing this challenge to see how people are coming up with clever solutions to the following problem. So the problem is if I give you a quantum circuit, effectively what you're doing is taking a series of operations and applying them on some qubits in your quantum computer. To each circuit there is a matrix that corresponds to the series of operations that are applied. So every time you give me a circuit, I can tell you the unitary part of that circuit, which is just the set of quantum operations, looks like the following matrix.

Now the question is, if I gave you the matrix instead, can you do the reverse? Can you tell me what circuit generated that matrix? This is a hard problem in general and it's really exciting. So we gave people a very small matrix. It's not that big of a matrix and we set it up so that we can see different creative ways that people go back from the matrix to the circuit that generated it. And I'm seeing so many creative ways of solving this problem, Bill. It's really rewarding to see this after having made the challenge.

Bill Detwiler: And is that something that you maybe find is maybe most, like you said, very rewarding is most interesting about the challenge is that you get to see people that are using novel ways to solve problems that even you didn't think of that you didn't think about. You're seeing the unexpected inventions come out of this, right? You're seeing new ways that people were like, "Oh yeah, that could work. We have practical applications for that."

Abe Asfaw: That's right. And people are coming up with clever ways that we didn't think about, but more importantly, taking this problem really requires understanding things deeply. Being able to go from the matrix to the circuit requires for some people writing down equations and solving those equations on paper and then writing down a quick script to solve it. For other people that requires writing different circuits and trying out what did this small change that I did to a circuit do to the matrix and trying to go back and forth between the two. The rewarding part of all of this is seeing the amount of learning that's happening. People going from exercise one, starting with no quantum background and finishing all the way through exercise four, I think that's a huge, huge step for someone to make and it's really exciting to see that many people learning.

Bill Detwiler: Do you have a sense from the people who participate in the challenge, and I don't know whether you collect data about the people that participate, but do you get a sense that there are people with a previous engineering background like yourself or are they people with a coding background or are they people with an IT background or are they people who are just interested in this? Who do you find participates in the challenge?

Abe Asfaw: You'll find that traditionally the field has been dominated by PhDs in physics and electrical engineering. So when you talk about quantum computing, if you look at any of the research labs today, you'll find that most people have that kind of background. The work that I'm doing with all the quantum education

effort within our team is to make sure the barrier to entry is lowered to the college level. So anyone with any sort of programming experience and a little bit of linear algebra, so the kind of math that you take in freshman year, freshman year of college can attack these problems. So if you look at the kinds of people who are taking this challenge, you'll see various STEM, so Science, Technology, Engineering and Math people with that kind of background. But what we're starting to see is people crossing over from other fields.

Finance is one of the ones where we see a lot of people coming from and that's for good reason. There are some quantum algorithms where we expect to see some advantage from quantum computers. We're seeing a lot of people from data science because there seems to be a very good motivation to study quantum machine learning. So these are the kinds of backgrounds that we're seeing overall. The most rewarding thing for me to see is not just college students, but people from high school and middle school attacking these problems. You can see their responses on Twitter. When you ask how did you solve this that they're so excited about quantum computing and they're learning every day and consume any material that we put out.

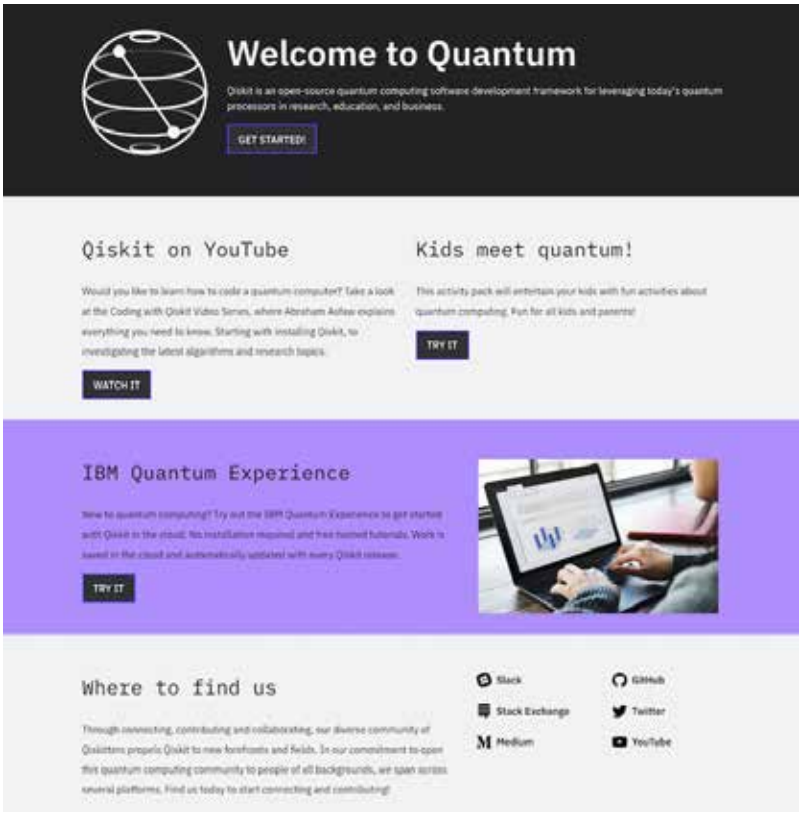
QISKIT: IBM'S OPEN-SOURCE TOOLS FOR WRITING QUANTUM COMPUTER CODE

Bill Detwiler: Yeah, that's really cool. Let's talk about the tools. We talked about people who are interested in the challenge and taking the challenge. What are the tools that people need from, a software, an online or a hardware [perspective that] they need to kind of start with quantum computing. Where can they get the tools as part of the challenge or how do people just physically go to actually, "Oh, here's how I build a circuit. Here's how I run the circuit."

Abe Asfaw: So the first tool that you need, and one of the most important tools is the one that gives you access to the quantum computers. So if you go to quantum-computing.ibm.com and create an account there, we give you immediate access to several quantum computers, which first of all, every time I say, this just blows my mind because four years ago this wasn't a thing. You couldn't go online and access a quantum computer. I was in grad school because I wanted to do quantum research and needed access to a lab to do this work. But now you can just log into a website and immediately get access to quantum computers.

To help with using these quantum computers we have open software called Qiskit, that's Q-I-S-K-I-T. So qiskit.org is where you'd find access to the software. So in my work, one of the things I do is make sure that people have all the right tools to get started with quantum computing. So you'll find an open source online textbook at qiskit.org/textbook and having the textbook open and the quantum computing website that I mentioned open, you can be looking at snippets of code and writing the code and testing it yourself on a real quantum computer.

Bill Detwiler: And I think what is striking for me too, been in technology for longer than I care to admit to, but that you're actually by accessing IBM's quantum computers, you're actually going to run this not on a virtualized quantum computer or an emulator type set up on local machine, but you're actually going to be able to run this on real hardware somewhere, it reminds me of the old supercomputer days, where you would write your code and then you would submit it up to the computer and then you would, "Okay, when am I going to get time to run this thing? When am I going to get my simulation back? Okay, it's going to be two days. It's going to be tomorrow. Okay, well I'll wait here. Wait to get the data back. Oh your batch ran. You got your data back."



IBM Qiskit

Abe Asfaw: So let me tell you about how confusingly good the progress is here. So four years ago, no quantum computers available. Right? All right, so now quantum computers become available. Everyone gets excited and wants to access the one quantum computer that we have online. Which means now you need to think about exactly what you said, "Which is how do I get time on this thing?" There's, there's a public queue, we all want to access this device, so now you have to wait a long time. And gradually we've been increasing the number of quantum computers that we have online. We have 18 of them now, which again is another confusing number. It's not one or two quantum computers, 18 quantum computers, which means now when you send your job, you don't need to wait as long as you used to a few years back to do this. So we're going from the timeframe when you needed to think about, "How do I get time on a quantum computer?" More to the question of what kinds of interesting things can I try on a quantum computer because it is available and readily accessible right now.

Bill Detwiler: And I guess maybe that's one of the questions that a lot of people have is, "What can I do with this? What are the right kinds of problems?" We talk about quantum computers being very good for optimization problems or we talk about them being good for maybe chemical assimilation problems, whether it's chemical simulations, environmental simulations, drug research, things like that. And then maybe on down the

road, AI, we talked about quantum as relates to communications. What are some of the ways you're seeing people use the quantum computers? I mean what problems are they trying to solve?

Because I can sit here at my desk and think, "Man, you know, that would really be cool. I'd like to try this. I'd like to write this, but I don't know what I would solve. Do I just want to know the quickest route for me to get from my house to my office and have it run every computation of every road and every left turn and right turn." That sounds cool. But it also sounds like a waste. I don't want to take up time on one of IBM's machines when it could be devoted to solving a health crisis, solving a cure for disease, finding something much more important than what's the optimal way for me to get from here to the office if we ever go back to the office anyway.

Abe Asfaw: So two things to think about. The first thing is that a quantum computer is just not going to replace the laptop that I'm using to talk to you right now. A quantum computer is going to work in union with a classical computer. For example, we just talked about a few examples. You take a quantum circuit, you measure the output of that quantum circuit and then you interpret whatever that output was relative to the problem that you're trying to solve. Well, the problem that you fed to the quantum computer presumably it was some real world problem, which means there's nothing quantum about it. It's a classical issue. You have some numbers, you want to feed that kind of set of numbers in some special way to a quantum computer. So all of that is done by a classical computer. And then you want to get the results back from the quantum computer and process them, which is also a classical thing.

So we'll always be in this regime where quantum computers and classical computers will work together. So now the question becomes, "Well, if you have these two working together, how can you extract some sort of advantage from them?" So the kinds of examples that I'm seeing people working on fundamentally are all about learning how to take your problem. For example, let's say it's simulating a molecule. Learning how to take that problem of, "Let me simulate this molecule to a real quantum system." How do you map that problem onto a real quantum system? And once you do, how do you take the results back out and interpret them? And in the presence of noise in today's systems, how do you overcome noise and extract meaningful results from quantum computers? These are the kinds of things that people are doing. Learning how to map problems, and learning how to work with the quantum computers today.

Bill Detwiler: And what gets you the most excited as you look at the next one year, two years, and we've talked about the progress that you've made in just the last four years? What gets you the most excited in the immediate near term future?

Abe Asfaw: This is a very biased opinion. Okay. So let me preface this by saying my background is in physics. So I'll say something along the lines of physics. The fundamental motivation for building quantum computers

is to use quantum mechanics, which is inherently what we're using here to compute, to understand systems that are quantum mechanical in nature. So to get a better glance at nature using the fundamental principles of nature that we know best today. So for me the most exciting thing is seeing as these quantum computers grow in size, the number of qubits grows, the quality of the qubits grows, and overall we're getting better and better systems, what kinds of new physics that we haven't seen before can we simulate on these systems? And maybe a sort of related topic is what kinds of chemistry problems are people solving on these systems that can have societal impact that a large scale?

So all of these require taking advantage of quantum mechanics to compute something to then learn more about quantum mechanics, to then make better systems. So it's this feedback loop that I'm very excited to monitor as the years go by.

Bill Detwiler: Well Abe, I really want to thank you again. I appreciate you taking the time to talk to us today. This has been a great conversation. Where can folks go to learn more about IBM's Quantum Challenge, quantum computing in general to get the tools that they need to get started?

Abe Asfaw: So thanks for having me Bill. So the quantum challenge is at ibm.co/quantumchallenge and all of our quantum computers are accessible at quantum-computing.ibm.com. And the learning materials that we have can be accessed at qiskit.org/education and that includes our textbook, series of videos that we have to help people, all of these things wrapped up together in one webpage.

QUANTUM COMPUTING MEETS CLOUD COMPUTING: D-WAVE SAYS ITS 5,000-QUBIT SYSTEM IS READY FOR BUSINESS

Quantum-as-a-service can solve in minutes the problems that might take classical computers a whole day to work through.

BY DAPHNE LEPRINCE-RINGUET/ZDNET

IMAGE: D-WAVE

Quantum-computing company D-Wave has doubled the scale of its cloud-based computing platform and said it is already solving real-world problems in minutes that would take traditional computers a whole day of number crunching.

D-Wave, through a service called Leap, grants developers access to a cloud-based quantum processor that can be used to test and trial applications in real time.

In the previous iteration of Leap, the quantum processor was 2,000-qubits strong, with each qubit capable of connecting to six other qubits. D-Wave has more than doubled the performance of the technology: Advantage's quantum processor – which is available through the Leap platform – boasts 5,000 qubits, and each qubit can connect to 15 others. In other words, programmers will have access to a much larger graph to build their quantum applications.

As part of Leap, developers can also use a feature called the hybrid solver service (HSS), which combines both quantum and classical resources to solve computational problems. This "best-of-both-worlds" approach, according to D-Wave, enables users to submit problems of ever-larger sizes and complexities.

Advantage comes with an improved HSS, which can run applications with up to one million variables – a jump from the previous generation of the technology, in which developers could only work with 10,000 variables.

"When we launched Leap last February, we thought that we were at the beginning of being able to support production-scale applications," Alan Baratz, the CEO of D-Wave, told ZDNet. "For some applications, that was the case, but it was still at the small end of production-scale applications."

"With the million variables on the new hybrid solver, we really are at the point where we are able to support a broader array of applications," he continued.

A number of firms, in fact, have already come to D-Wave with a business problem, and a quantum-enabled solution in mind. According to Baratz, in many cases customers are already managing the small-scale deployment of quantum services, and are now on the path to full-scale implementation.

Baratz gave the example of Canadian grocery chain Save-On-Foods, which reached out to D-Wave a couple of months ago to find out if quantum technologies could help them better manage some of the logistics of their operations.

In the space of two months, D-Wave's team designed a concept and built up an application that Save-On-Foods is now trialing in one of the retailer's stores. Using a hybrid quantum algorithm, the Canadian company was able to reduce the time for some optimization tasks from 25 hours down to two minutes of calculations per week.

"They believe that it represents significant savings for them," said Baratz. "Of course, so far it has only been used in one store, but based on the results, the intention is to roll it out to every one of their stores."

Lowering the barrier to entry for quantum computing is, according to Baratz, one of D-Wave's objectives.

As part of the Advantage platform, the tech company has started a program called Launch, designed for businesses that want to build hybrid quantum applications but may need additional technical support.

Users can access Launch via D-Wave's website and fill out a form describing the business problem they wish to translate into a quantum algorithm. The company will then connect them to a developer from D-Wave or a partner expert to provide advice on designing, building and running the appropriate application.

"We think now is absolutely the best time to be doing this," said Baratz. "We are delivering very compelling technology and we are excited to be opening up the opportunity for businesses to make use of quantum computing."

A new survey commissioned by D-Wave, carried out among 250 Fortune 1000 companies, showed that while only 4% of businesses are currently developing their own quantum-computing applications, an overwhelming 81% of respondents reported having a use case in mind for quantum in the next three years.

Particular enthusiasm for the technology was found in the transportation, insurance, financial services and chemical industries; and at the heart of most respondents' interest was the drive to improve efficiency and profitability.

Hans Melo is the CEO of synthetic biology startup Menten AI and a long-time customer of D-Wave's. With his team of designers and engineers, Melo is using hybrid quantum algorithms to create new proteins that could eventually be used as therapeutic drugs.

Melo identified what he sees as an efficiency problem in the pharmaceutical industry: most drugs are currently discovered in labs by trial and error, with scientists testing thousands of molecules against a target until a successful match is found. The procedure is highly inefficient, according to the start-up CEO – and yet the approach has not changed for the past four decades.

With Menten AI, Melo is hoping to tap quantum computing and machine learning to design molecules specifically for a target. "In order to design a protein, you need to consider all the different possibilities in which it could fold," he explained to ZDNet. "That's a huge search problem: there are trillions upon trillions of possibilities, and you can't test them all in the lab."

"Our approach is to do this computationally," he continued. "But the search problem is so large you can't solve it on a classical computer. That's where quantum computing becomes useful."

Using D-Wave's hybrid solver service, Menten AI's team was able to design new molecules; the company has now tested some of the designs in the lab and confirmed that the technology's predictions matched real-life results.

But despite such encouraging developments, Melo is keeping a cool head. The moment of true excitement will come when Menten AI is sitting on a method that is demonstrably more effective than classical approaches. For now, said the start-up CEO, the experiment is still a proof of concept, and will be for the next few years.

"We are at a stage where it is actually feasible to apply quantum to a real-life problem," said Melo. "And we are going into the stage where it is not only feasible, but practical, as opposed to classical methods. We're thinking in three years, certainly before five years, we will be using the technology not only because we can, but because it's actually better."

For all the promises of quantum computing, therefore, it will still be some time before the technology becomes commercially viable and fully integrated into business models. D-Wave, for its part, is committed to scaling up the performance of its quantum processors, and to helping developers run applications that are increasingly complex. "We've proven that our technology continues to scale," said Baratz. "We're able to scale and we will continue to scale."

The Advantage platform is already available in the Leap cloud service, for all current customers to access with no additional charge. New customers will also be able to use all the new and existing capabilities on the platform.

CREDITS

Editor In Chief
Bill Detwiler

Editor In Chief, UK
Steve Ranger

Associate Managing Editors
Teena Maddox
Mary Weilage

Editor, Australia
Chris Duckett

Senior Writer
Veronica Combs

Senior Reporter, UK
Owen Hughes

Editor
Melanie Wachsman

Staff Writer
R. Dallon Adams

Multimedia Producer
Derek Poore

Staff Reporter
Karen Roby

ABOUT ZDNET

ZDNet brings together the reach of global and the depth of local, delivering 24/7 news coverage and analysis on the trends, technologies, and opportunities that matter to IT professionals and decision makers.

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

COVER IMAGE: ISTOCKPHOTO