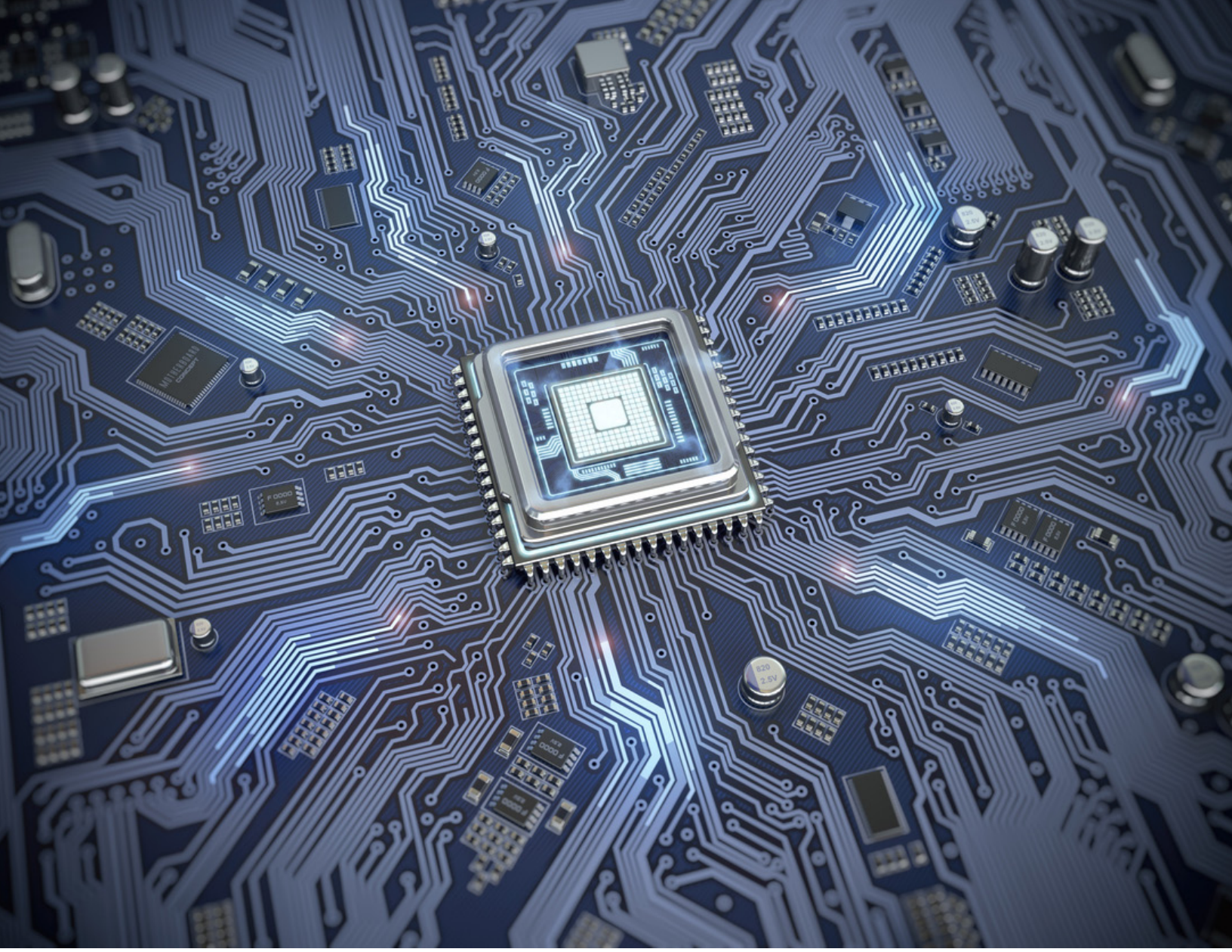


QUANTUM COMPUTING: AN INSIDER'S GUIDE

TechRepublic

TABLE OF CONTENTS

QUANTUM COMPUTING: SEVEN IMPORTANT TRUTHS

BY NICK HEATH

Quantum computers promise to solve tasks that would be impossible using conventional machines. But those benefits are still theoretical at present, with quantum computers lacking a sufficient number of processing units, known as qubits, and enough stability to do useful work.

Companies are going to huge lengths to build quantum computers, cooling devices to a few micro kelvins above absolute zero. But even then, challenges remain. While IBM has a 50-qubit prototype machine and Google a 72-qubit chip, both have their own roadblocks that prevent them from being truly useful devices at this moment.

Here is the expert view on what quantum computers will and won't be able to do and the challenges we still face.

1. QUANTUM COMPUTERS WON'T REPLACE CLASSICAL COMPUTERS

"Quantum computers will never be able to run the if/then/else type of logic that we're familiar with with our traditional Von Neumann architecture computers, [where they are] sequentially going from step to step," said Andy Stanford Clark, IBM CTO for UK and Ireland.

2. QUANTUM COMPUTERS EXCEL AT OPTIMIZATION PROBLEMS

"Quantum computers are really good at solving those problems where you've got an exponential number of permutations to try out," Stanford Clark said.

He offered the examples of optimizing the lengths of aircraft routes and optimizing the layout of spare parts for a rail network—situations where there are two possibilities and you have to try each one to find the best solution.

"If you had a 2^{100} problem, which would be basically impossible to solve on a classical computer, with a 100-qubit quantum computer, you'd be able to solve it in one operation."

Stefan Filipp, technical leader for superconducting qubit quantum computation at IBM, said, "We know a few algorithms where we can get exponential speed up. For example, quantum chemistry or material science questions, calculating properties of molecules, that's definitely a thing where a quantum computer can help."

3. QUANTUM COMPUTERS WILL AUGMENT CLASSICAL COMPUTERS

"We're not going to see people throwing away all their classical computers and replacing them with quantum computers," Stanford Clark said.

"We're going to see, in the same way as you have a maths co-processor and a GPU on your classical computer ... you'll have a quantum computer co-processor alongside your classical computer.

"When you come to a point where you've got to solve some massive exponential problem, you'll package it up, throw it over to the quantum co-processor, it'll burp out its answer, and then you'll carry on with the answer to your computation in your classical algorithm."

4. WE NEED 50-60 QUBIT COMPUTERS TO DO USEFUL WORK

"The tipping point as to where classical computers give way to quantum computers is in the 50-60 qubit mark," Stanford Clark said.

"In terms of years, I don't know if it's five or 10 [until we reach that point], probably that sort of order of magnitude where we have something at the 50-qubit level that is actually doing useful stuff, in that it stays up long enough to do useful computation."

5. BUILDING A WORKING QUANTUM COMPUTER IS ABOUT MORE THAN QUBITS

"We've got a prototype 50-qubit computer at the moment but the problem is one of quantum coherence, this 100-microsecond window during which it's stable means you can't get very much useful done with your 50 qubits, so we're a little way off that yet," Stanford Clark said.

Filipp said, "The challenge is getting hardware to the point where we can use it and run practical algorithms. That means we have to not only increase the number of qubits, but also have to increase the coherence. We have to improve this to get to the point where we can solve practical algorithms.

"We have a roadmap that goes in the direction of improving coherence, but it is still a significant challenge in getting to real practical quantum computers."

6. WE HAVE NO IDEA HOW TO WRITE USEFUL QUANTUM SOFTWARE

"At the moment we have no real idea how to write big complicated algorithms for quantum computers as we're so used to doing with classical computers," Stanford Clark said. "We just haven't had the experience and exposure to try to try to solve problems with quantum computers that we have with classical computers."

7. QUANTUM COMPUTERS NEED ERROR CORRECTION

"There's fault tolerance inside the qubits as well," Stanford Clark said, adding that quantum computers will need an equivalent to the error-checking parity bits found in conventional computers.

"You'll need the same sort of equivalent technology inside a quantum computer, so that we can detect when a bit has inadvertently flipped or come out in the wrong state and therefore can be error corrected for."

D-WAVE QUANTUM COMPUTERS: WHAT YOU NEED TO KNOW

BY NICK HEATH

D-Wave Systems' quantum computers have the potential to solve problems that the fastest supercomputers available today just can't crack. But claims of performance superiority have been criticized as premature by some academics, because D-Wave's machines have yet to definitively prove themselves in the real world.

You'll find everything you need to know about the D-Wave quantum computers in this guide.

EXECUTIVE SUMMARY

- What are D-Wave quantum computers? They are machines that solve a specific class of problem by exploiting the counterintuitive behavior of matter at the atomic level.
- Why do D-Wave quantum computers matter? D-Wave quantum computers have the potential to tackle problems that would be impossible for conventional computers to practically solve, with applications ranging from bioscience to cybersecurity.
- Who do D-Wave quantum computers affect? They mainly affect large organizations with deep pockets, as each D-Wave machine costs $15m. However, while early customers are restricted to the likes of Lockheed Martin, the US government, Google, and NASA, D-Wave also provides access to its machines via a cloud service.
- When are D-Wave quantum computers happening? D-Wave plans to continue to develop its quantum processors. It's backed by high-profile investors and sells machines to the occasional early adopter.
- Who are D-Wave quantum computers' competitors? Google's Quantum AI Lab has developed a 72-qubit quantum processor called Bristlecone, while IBM has pledged it will build a 50-qubit quantum computer within "the next few years."

WHAT ARE D-WAVE QUANTUM COMPUTERS?

D-Wave's quantum computers use very different technology from that found in everyday computers. The latest D-Wave machine is 10-feet tall, costs $15m, and tackles problems using "quantum transistors," tiny loops of niobium cooled to almost absolute zero (-459.6F) by liquid helium.

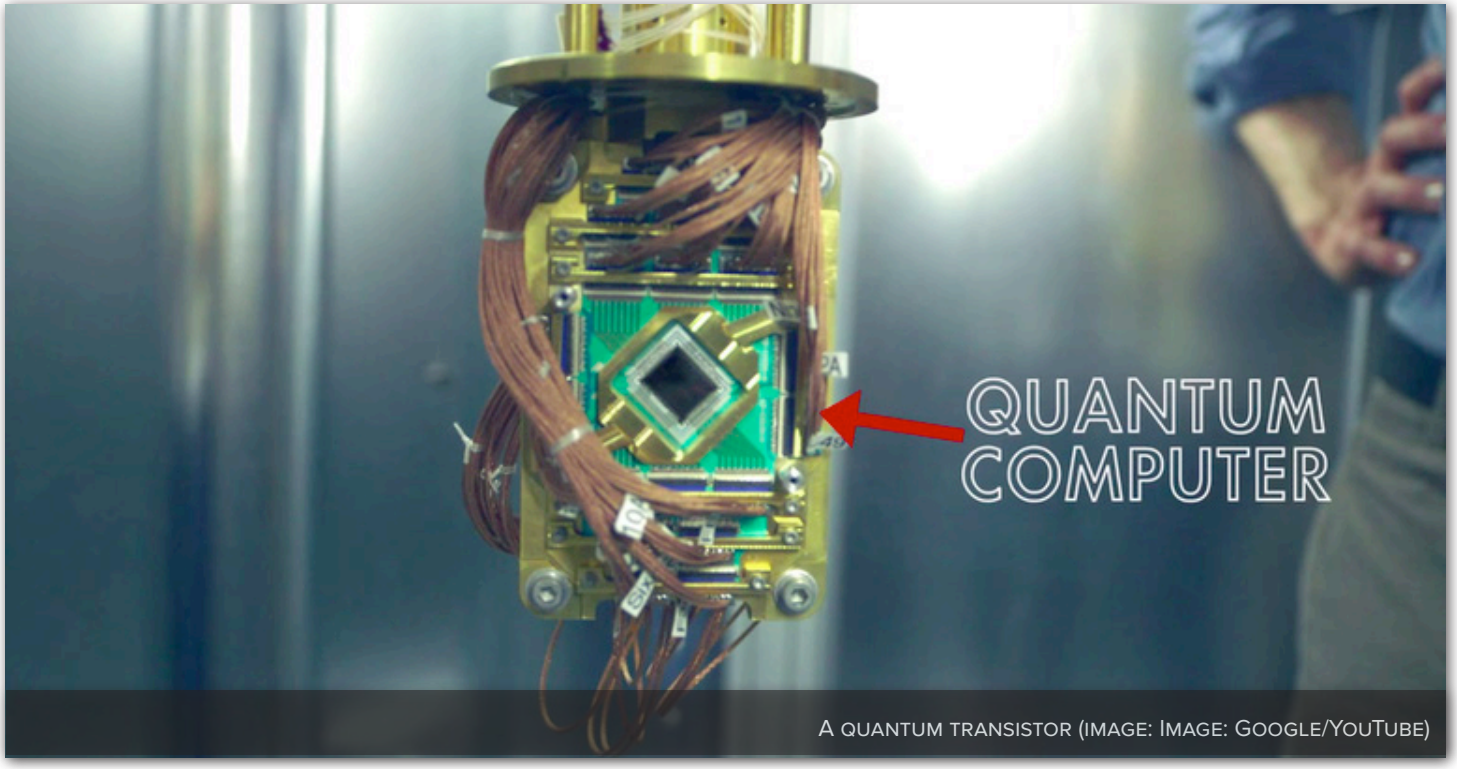
This exotic architecture is necessary for the D-Wave chips to exploit quantum phenomena, the counterintuitive way that matter behaves at an atomic level. D-Wave has gone to these lengths because it believes its processors have the potential to massively outstrip classical computers when it comes to solving a particular class of problem.

However, these processors are also fundamentally more limited in the breadth of problems they can tackle than the general-purpose computers in use today, with D-Wave's systems able to handle only a specific type of computation. Even though D-Wave calls its systems "computers," John Morton, professor of nanoelectronics and nanophotonics at UCL, said that just as a calculator isn't a computer, the D-Wave system isn't a universal quantum computer.

"A calculator solves a very specific set of problems. Lots of people use it, and you can use calculators across many different industries," he said. "So when D-Wave shows you many different industries that might use a D-Wave machine, there may be many areas that it can be used in, but it remains a specialized device."

Additional resources

- Quantum leap: D-Wave's next quantum computing chip offers a 1,000x speed-up
- Quantum computing: The smart person's guide



A QUANTUM TRANSISTOR (IMAGE: IMAGE: GOOGLE/YOUTUBE)

WHY DO D-WAVE QUANTUM COMPUTERS MATTER?

What makes D-Wave systems interesting is their potential.

Despite being at an early stage of development, organizations such as NASA, Google, Lockheed Martin, and Los Alamos National Laboratory have shelled out the $15m it costs for one of D-Wave's machines. That's because D-Wave processors may eventually massively outperform classical computers when it comes to solving a particular class of mathematical problem called unconstrained binary optimization. A very simple example of this type of problem might be the challenge of drawing up a plan for a house that comes as close to your dream spec as possible, while staying within your budget.

To understand just how much D-Wave's machines might one day outclass conventional computers, consider a 2015 test by Google. It found that the D-Wave 2X processor was 100 million times faster than a classical processor running a similar operation.

The significance of that 100 million speedup was disputed on the grounds that the tests were synthetic and massively favored the D-Wave processor. However, D-Wave said the test was meaningful because it demonstrated that D-Wave's fundamental approach was sound and that the chips were capable of exploiting the phenomenon called quantum tunneling to help perform calculations.

This tunneling is necessary for D-Wave processors to carry out quantum annealing, the process of finding the minimum energy state for a system of particles, which is useful in modeling and solving the class of optimization problems mentioned above.

However, much of the promise of the D-Wave systems lies in their future, and there are some who doubt whether that potential will ever be reached.

D-Wave's most vociferous skeptic is probably Scott Aaronson, a computer science professor at the University of Texas in Austin. While D-Wave has repeatedly claimed its tests show its processors' superiority over classical counterparts for cracking certain problems, Aaronson says that barring D-Wave's most recent performance claims, which are still being examined, past assertions of performance leads have been debunked and that in each instance a different classical approach was found that "eliminated the claimed gap."

D-Wave is yet to definitively demonstrate the so-called quantum supremacy of its processor, the ability to perform a calculation at a speed that classical supercomputers have no hope of matching.

However, Google's director of engineering, Hartmut Neven, has said the technology giant is "optimistic" that the "significant runtime gains" demonstrated by using D-Wave in testing will "carry over to commercially relevant problems as they occur in tasks relevant to machine intelligence."

Additional resources

- The latest in quantum computing: 10ft tall, 2,000 qubits, $15m price tag (ZDNet)
- UNSW obtains 10-fold boost in quantum computing stability (ZDNet)

WHO DO D-WAVE QUANTUM COMPUTERS AFFECT?

The binary optimization problem that D-Wave processors excel at has practical applications in a variety of areas. D-Wave says that its processors have been used in the financial sector for trading trajectory optimization to work out how proteins fold in bioscience, to create filters for lists that never miss a potential match (useful for security services checking terrorist watch lists), to spot cybersecurity threats in online traffic, and to develop binary classifiers in AI and for computer vision.

Of particular interest to D-Wave is the potential for its processors to be used to carry out unsupervised machine learning, where unlabeled training data is fed into a neural network and the machine learns by identifying patterns.

D-Wave has already experimented with machine learning on the chip, setting up a Boltzmann machine—a type of stochastic recurrent neural network—as well as a "Quantum Boltzmann machine," which Colin Williams, director of business development and strategic partnerships at D-Wave, said is "fundamentally different from previous machine learning models" and could eventually allow a machine to "generate new data that is statistically indistinguishable from the kind of data on which it was trained."

Williams predicts that eventually, a D-Wave-based machine learning model could be trained to produce new and convincing works of art in the style of the painter it was trained on or to replicate human speech.

D-Wave has launched a spin-off company called Quadrant to focus on how its quantum machines could be applied to deep learning, specializing in training machines using only small amounts of labelled data.

D-Wave doesn't see its machines as a replacement for conventional computers, but as a complement, used to handle particular tasks before handing off work to a classical system.

Additional resources

- Quantum physics meets IT security
- How quantum computing could unpick encryption to reveal decades of online secrets

WHEN ARE D-WAVE QUANTUM COMPUTERS HAPPENING?

Given the level of interest in D-Wave, it seems highly likely it will continue to release new machines for the foreseeable future. D-Wave has raised millions of dollars in funding from various high-profile investors, including investment bank Goldman Sachs, In-Q-Tel (the investment arm of the US Central Intelligence Agency), Bezos Expeditions (the investment arm of Amazon founder Jeff Bezos), and BDC Capital, Harris & Harris Group, and DFJ.

Even though D-Wave has sold only a handful of its quantum computers, it continues to attract buyers for its machines and to generate interest in its technology. The carmaker Volkswagen has been working with D-Wave since 2017, using its systems to model traffic flows and develop more efficient batteries for electric cars.

In D-Wave's view, the core technology at the heart of the chip has been demonstrated to work, and realizing its promise of quantum supremacy requires adding more qubits (quantum bits) to the processor and making these qubits more densely connected.

Toward the end of 2016, D-Wave launched its first 2,000 qubit "quantum computer," the 2000Q, which, as well as doubling the number of qubits, introduced architectural improvements that the firm claimed helped speed up certain calculations 1,000-fold over its predecessor and 2,600x over classical computers.

US Department of Energy researchers at Oak Ridge National Laboratory in Tennessee will have cloud access to a D-Wave 2000Q system, allowing them to explore hybrid computing architectures with a view to accelerating the development of software designed to run exascale systems.

D-Wave continues to find new customers for its systems. A D-Wave 2000Q system was also installed at the Quantum Artificial Intelligence Lab run by Google, NASA, and Universities Space Research Association early in 2018.

Beyond the 2000Q, D-Wave has a design for a "next-generation chip" with a "fundamentally new topology, based on all the lessons we've learnt,"which reportedly will both increase connectivity between qubits significantly and allow D-Wave to surpass the 10,000-qubit limit in its existing processors. D-Wave announced it had completed fabrication and testing of a working prototype next-generation processor early in February 2018.

Additional resources

- Video: Quantum computing ... in less than two minutes
- Sydney Uni predicts the unpredictable in quantum computing advancement (ZDNet)

WHO ARE D-WAVE QUANTUM COMPUTERS' COMPETITORS?

As mentioned, D-Wave isn't a universal quantum computer and UCL's Morton predicts they may not exist until the 2030s. However, many major tech companies are researching and developing universal quantum computer technology.

In March 2018, Google's Quantum AI Lab showed off a new 72-qubit quantum processor called Bristlecone, which it says could soon achieve "quantum supremacy" by outperforming a classical supercomputer on certain classes of problems.

IBM has also pledged it will build a 50-qubit quantum computer that will be commercially available within "the next few years." In January 2018, the chipmaker Intel announced its own 49-qubit quantum chip, and Microsoft is investing significant funding in quantum computing research.

Additional resources

- IBM Q brings quantum computing to the cloud for businesses
- Microsoft's quantum computer simulator: A glimpse into the future of computers

FUJITSU "QUANTUM INSPIRED" COMPUTER: COMPLEX BUSINESS CALCULATIONS IN THE CLOUD

BY JAMES SANDERS

In May, Fujitsu announced the launch of its Digital Annealer cloud service, which allows organizations to perform specific types of complex calculations commonly run on quantum computers, while not requiring the sizable upfront hardware investment for purchasing a quantum computer outright.

Fujitsu's Digital Annealer currently operates at 1,024 bits, which can express bonding power in 65,536 gradations. Fujitsu's solution uses traditional digital circuitry, which allows it to operate at room temperature without requiring helium-based cooling solutions, as well as making it more resistant to noise and environmental conditions impacting performance. Fujitsu is planning further upgrades that would expand the capabilities to 8,192 bits and increase the precision from the current 16-bit model to 64-bit.

Cloud access is now available in Japan, and Fujitsu plans to make the service available in North America, Europe, and Asia during its fiscal year 2018. (As is typical of Japanese companies, the fiscal year starts and ends on April 1st.)

The company is also launching a consulting service to assist in application development for customers to utilize the hardware effectively. This is in addition to a partnership with 1QBit, a software vendor and consulting firm that helps organizations understand how to use quantum computers.

Pricing information is by individual estimate only, though the company is aiming to bring in 100 billion yen over the next five years for Digital Annealer cloud access and technical services.

Fujitsu markets the Digital Annealer as a "quantum inspired" computer, due to the limited use cases it is suited for and the way in which it is built. The Digital Annealer is limited to performing quantum annealing tasks, which Fujitsu noted are helpful for various use cases, including "speeding up the search of similarities in molecules for drug discovery, optimizing portfolios in finance, personalizing advertisements in digital marketing, and optimizing the arrangement of warehoused components for factories and logistics."

The 2000Q, which is marketed as a quantum computer by D-Wave Systems, is capable of performing only quantum annealing calculations. Among other things, hardware offered by Fujitsu and D-Wave is unsuitable

for integer factorization, which is required for cracking RSA encryption systems. The practical difference between the two systems relates to honesty in marketing—while D-Wave claims the 2000Q has 2,000 qubits, Fujitsu does not claim that the links in the Digital Annealer are qubits. For comparison, Google's experimental Bristlecone quantum processor is only 72 qubits, but it's more of a "general purpose" system.

WHY MICROSOFT IS ALL-IN ON QUANTUM COMPUTING

BY LAUREL DEPPEN

Microsoft is reassuring users that it's making advancements in quantum computing, noting in a recent blog post that it's working every day to help reform the future of computing.

Julie Love, Microsoft's director of quantum computing, wrote in the post that her team has a "good understanding of what's needed" to build a quantum computer that could revolutionize the way we get work done and pursue academic research.

Love explained that certain problems that are impossible for humans can be solved in a mere 100 seconds by quantum computing. These problems are in material science, chemistry, genetics, medicine, and the environment. And according to the blog post, they're made solvable based on the physics of qubits.

Love said that not all qubits are equal—and some are unstable. What sets Microsoft apart are topical qubits that correct each other. Microsoft is working on a scalable solution that is set to run on Azure cloud and will be more immune to errors.

The blog post said that Microsoft is the only major company building this kind of correcting qubits, although other companies, like Intel, have been working on their own approaches to qubit-based quantum computing.

Last year, Microsoft released a Quantum Development Kit that included a programing language for people who want to start writing quantum computer applications. The post said that this language, Q#, was designed for developers who are interested in learning how to program for quantum computers regardless of whether they're experts in the quantum physics field. Love said that this development kit was released so developers could "join us on this journey" of quantum computing.

Though quantum computing is having a significant impact on the quantum physics and computing fields, Love said that Microsoft's enterprise customers can look forward to changing their businesses with this newfound technology. Quantum computing can help advance businesses in a variety of ways, including data analysis and pattern matching.

IBM: QUANTUM COMPUTERS COULD INSTANTLY BREAK ENCRYPTION

BY TOM FOREMSKI

Quantum computers will be able to instantly break the encryption of sensitive data protected by today's strongest security, the head of IBM Research warned. This could happen in a little more than five years because of advances in quantum computer technologies.

"Anyone who wants to make sure that their data is protected for longer than 10 years should move to alternate forms of encryption now," said Arvind Krishna, director of IBM Research.

Krishna was speaking at a meeting of The Churchill Club in San Francisco on a panel (above, second from right) discussing quantum computers in business. The panel, which included Kam Moler, a professor of Physics at Stanford University, as well as Bob Stolte, a managing director at JPMorgan, was moderated by journalist Martin Giles (first from left).

Quantum computers can solve some types of problems almost instantaneously compared with billions of years of processing using conventional computers.

Moler said people might feel safe because they have done everything they're supposed to do to secure their existing data—but quantum computing will break it. "I do think that's scary," she said.

It has been known since the 1980s that quantum computers would be great at factoring large numbers, which is the foundation of public key cryptography. But building large enough quantum computers was not possible then.

Advances in novel materials and in low-temperature physics have led to many breakthroughs in the quantum computing field in recent years. and large commercial quantum computer systems may be viable and available within five years.

Krishna said that there is a type of encryption, called Lattice cryptography, that has been mathematically proven to be resistant to quantum computing attacks. So far, no known algorithms can break this method of encoding data.

"The good news is that it is as efficient as our current encryption so it won't cost more," he said.

Quantum computers are currently rare and expensive but can potentially solve many tough computing problems. The IBM Q is an attempt to build a commercial system, and IBM has allowed more than 80,000 developers to run applications through a cloud-based interface.

However, not all types of applications will benefit from quantum computers. The best suited problems are those that can be broken up into parallel processes, and it requires different coding techniques.

"We still don't know which applications will be best to run on quantum computers. We need a lot of new algorithms."
— Arvind Krishna

"We still don't know which applications will be best to run on quantum computers," Krishna said. "We need a lot of new algorithms."

In addition to solving tough computing problems, quantum computers could save huge amounts of energy, as server farms proliferate and applications such as bitcoin grow in their compute needs. Each computation takes just a few watts, yet it could take several server farms to accomplish if it were run on conventional systems.

Moler said we still need additional breakthroughs, such as new types of materials with specific properties at temperatures at near absolute zero.

Single atoms—qubits—are held in place, but temperature fluctuations can create a lot of noise, which creates errors. Additional qubits greatly increase the computational power of a system, but that requires even more qubits for error correction.

The optimum number of qubits for each type of problem is not known.

Also, there are substantial advances in software technologies needed to take advantage of the computing capabilities of quantum systems. And new algorithms have to be developed to handle the error corrections.

Krishna is certain that within five years, there will be widespread commercial use of quantum computers. But don't wait, he said. "Begin experimenting right now."

UNSW UNLOCKS QUBIT SIGNAL FREQUENCY CONTROL IN QUANTUM ADVANCEMENT

BY ASHA MCLEAN

Researchers from the University of New South Wales (UNSW) have announced a new milestone in their pursuit of creating a quantum computer chip in silicon. The scientists from the Centre of Excellence for Quantum Computation and Communication Technology (CQC2T), based out of the university, have demonstrated the ability to tune the control frequency of a quantum bit (qubit) by engineering its atomic configuration.

Working alongside experts at Indiana-based Purdue University, the researchers built two qubits; the first was an engineered molecule consisting of two phosphorus atoms with a single electron; the other was a single phosphorus atom with a single electron. UNSW said the two qubits were then placed 16 nanometres apart in a silicon chip.

"By patterning a microwave antenna above the qubits with precision alignment, the qubits were exposed to frequencies of around 40GHz," the university explained. "The results showed that when changing the frequency of the signal used to control the electron spin, the single atom had a dramatically different control frequency compared to the electron spin in the molecule of two phosphorus atoms."

UNSW explained that creating engineered phosphorus molecules with different separations between the atoms within the molecule allows for families of qubits with different control frequencies. It said that as a result, each molecule can be operated individually by selecting the frequency that controls its electron spin.

"Individually addressing each qubit when they are so close is challenging," said 2018 Australian of the year recipient and CQC2T director Professor Michelle Simmons. "The research confirms the ability to tune neighbouring qubits into resonance without impacting each other."

UNSW Research Fellow Sam Hile said the achievement allows the scientists to "tune" into a molecule in a similar way to tuning in to different radio stations.

According to the university, tuning in and individually controlling qubits within a 2-qubit system is a precursor to demonstrating the entangled states that are necessary for a quantum computer to function and carry out complex calculations.

Australia is banking on silicon being the key to building the first quantum computer and the results the researchers published show how this may be achieved.

"By engineering the atomic placement of the atoms within the qubits in the silicon chip, the molecules can be created with different resonance frequencies. This means that controlling the spin of one qubit will not affect the spin of the neighbouring qubit, leading to fewer errors—an essential requirement for the development of a full-scale quantum computer," UNSW said.

CREDITS

Global Editor in Chief
Jason Hiner

Editor in Chief, UK
Steve Ranger

Managing Editor
Bill Detwiler

Editor, Australia
Chris Duckett

Senior Features Editors
Jody Gilbert
Mary Weilage

Senior Editor
Conner Forrest

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writers
Alison DeNisco Rayome
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

Cover image
iStock/Bet_Noire

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.