



What Is Quantum Computing?

2020



WHAT IS CB INSIGHTS?

CB Insights helps the world's leading companies make smarter technology decisions with data, not opinion.

Our Technology Insights Platform provides companies with comprehensive data, expert insights and work management tools to drive growth and improve operations with technology.

SIGN UP FOR A FREE TRIAL

Table of Contents

The rise of quantum computing **6**

- Computing beyond Moore's Law
- What is a qubit?
- Types of quantum computers

The quantum computing landscape **12**

- Deals to startups are on the rise
- Corporates and big tech companies are going after quantum computing

Uses of quantum computing across industries **15**

- Healthcare
- Finance
- Cybersecurity
- Blockchain and cryptocurrencies
- Artificial intelligence
- Logistics
- Manufacturing and industrial design
- Agriculture
- National security

The outlook for quantum computing **26**

Quantum computing is poised to upend entire industries from finance to cybersecurity to healthcare, and beyond – but few understand how quantum computers actually work.

Soon, quantum computers could change the world.

Quantum computing is the processing of information that's represented by special quantum states. By tapping into quantum phenomena like “superposition” and “entanglement,” these machines handle information in a fundamentally different way to “classical” computers like smartphones, laptops, or even today's most powerful supercomputers.

Why is quantum computing important?

Researchers have long predicted that quantum computers could tackle certain types of problems – especially those involving a daunting number of variables and potential outcomes, like simulations or optimization questions – much faster than any classical computer.

But now we're starting to see hints of this potential becoming reality.

In 2019, Google said that it ran a calculation on a quantum computer in just a few minutes that would take a classical computer 10,000 years to complete. A little over a year later, a team based in China took this a step further, claiming that it had performed a calculation in 200 seconds that would take an ordinary computer 2.5B years – 100 *trillion* times faster.

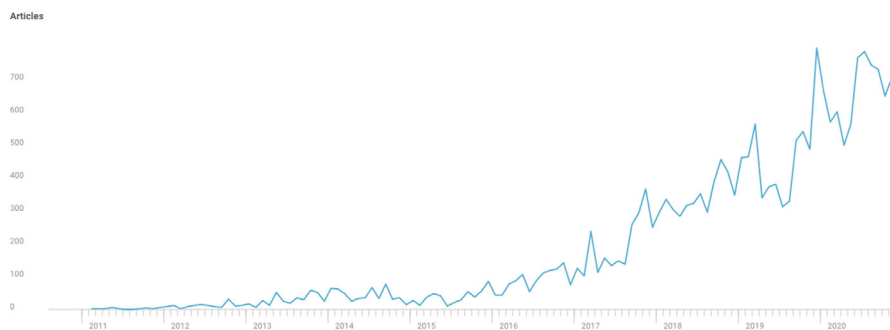
**“It looks like nothing is happening,
nothing is happening, and then whoops,
suddenly you’re in a different world.”**

**— HARTMUT NEVEN, DIRECTOR, GOOGLE QUANTUM
ARTIFICIAL INTELLIGENCE LAB**

Though these demonstrations don't have practical use cases, they point to how quantum computers could dramatically change how we approach real-world problems like financial portfolio management, drug discovery, logistics, and much more.

Propelled by the prospect of disrupting countless industries and quick-fire announcements of new advances, quantum computing is attracting more and more attention from players including big tech, startups, governments, and the media.

Quantum computing is gaining momentum Articles mentioning quantum computing, 2011 – 2020 YTD (11/30/2020)



Source: cbinsights.com

 CBINSIGHTS

In this explainer, we dive into how quantum computing works, funding trends in the space, players to watch, and the tech's applications across major industries.

The rise of quantum computing

COMPUTING BEYOND MOORE'S LAW

In 1965, Intel co-founder Gordon Moore observed that the number of transistors per square inch on a microchip had doubled every year since their invention while the costs were cut in half. This observation is known as Moore's Law. (See [more laws that have predicted success in tech in this report](#)).

Moore's Law is significant because it predicts that computers get smaller and faster over time. But now it's slowing down — some say to a halt.

More than 50 years of chip innovation have allowed transistors to get smaller and smaller. Apple's latest computers, for example, run on chips with 5 nm transistors — about the size of just 16 oxygen molecules lined up side-by-side. But as transistors start to butt against physical limitations, Intel and other chipmakers have signaled that improvements in transistor-based computing might be approaching a wall.

Soon, we will have to find a different way of processing information if we want to continue to reap the benefits of rapid growth in computing capabilities.

Enter qubits.










WHAT IS A QUBIT?

Qubits, the quantum version of bits used in classical computing, are the basic units of information in a quantum computer.

They make use of a quantum mechanical phenomenon called "superposition," where some properties of a particle — such as the angle of polarization of a photon — are not defined for certain until they're actually measured.

In this scenario, each possible way these quantum properties could be observed has an associated probability. This effect is a bit like flipping a coin. A coin is definitely heads or tails when it lands, but while in the air it has a chance of being either.

Quantum computers conduct calculations by manipulating qubits in a way that affects these superimposed probabilities before making a measurement to gain a final answer. By avoiding measurements until an answer is needed, qubits can represent both parts of binary information, denoted by "0" and "1," at the same time during the actual calculation. In the coin flipping analogy, this is like influencing the coin's downward path while it's in the air – when it still has a chance of being either heads or tails.

Quantum Computing	Vs.	Classical Computing
 <p>Calculates with qubits, which can represent 0 and 1 at the same time</p>		 <p>Calculates with transistors, which can represent either 0 or 1</p>
 <p>Power increases exponentially in proportion to the number of qubits</p>		 <p>Power increases in a 1:1 relationship with the number of transistors</p>
 <p>Quantum computers have high error rates and need to be kept ultracold</p>		 <p>Classical computers have low error rates and can operate at room temp</p>
 <p>Well suited for tasks like optimization problems, data analysis, and simulations</p>		 <p>Most everyday processing is best handled by classical computers</p>
		

A single qubit can't do much, but quantum mechanics has another trick up its sleeve. Through a delicate process called "entanglement," it's possible to set qubits up such that their individual probabilities are affected by the other qubits in the system. A quantum computer with 2 entangled qubits is a bit like tossing 2 coins at the same time, while they're in the air every possible combination of heads and tails can be represented at once.

The more qubits that are entangled together, the more combinations of information that can be simultaneously represented. Tossing 2 coins offers 4 different combinations of heads and tails (HH, HT, TH, and TT) but tossing 3 coins allows for 8 distinct combinations (HHH, HHT, HTT, HTH, THT, THH, TTH, and TTT).

This is why quantum computers could eventually become much more capable than their classical counterparts — each additional qubit doubles a quantum computer's power.

At least, that's the theory. In practice, the properties of entangled qubits are so delicate that it's difficult to keep them around long enough to be put to use. Quantum computer makers also contend with lots of engineering challenges — like correcting for high error rates and keeping computer systems incredibly cold — that can significantly cut into performance.

Still, many companies are progressing toward making powerful quantum computers a reality.

Quantum computers are rapidly becoming more powerful

In 2019, Google used a 53-qubit quantum chip to outcompete classical computers at solving a specially chosen mathematical problem — the first example of so-called "quantum supremacy" over classical computers. IBM aims to build a 1,000-qubit machine by 2023. Meanwhile, Microsoft-backed [PsiQuantum](#), the most well-funded startup in the space, claims it will build a 1M qubit quantum computer in just "a handful of years."

This quickening pace is being described by some as the start of a quantum version of Moore's Law — one that may eventually reflect a double exponential increase in computing power.

This could be achieved from the exponential increase in power offered by adding a single qubit to a machine alongside an exponential increase in the number of qubits being added. Hartmut Neven, the director of Google Quantum Artificial Intelligence Lab, summed up the staggering rate of change: “it looks like nothing is happening, nothing is happening, and then whoops, suddenly you're in a different world.”

TYPES OF QUANTUM COMPUTERS

Most discussions of quantum computers implicitly refer to what's called a “universal quantum computer.” These machines use qubits and quantum logic gates — similar to the logic gates that manipulate information used in today's classical computers — to conduct a wide range of calculations.

However, some players, including [D-Wave](#), have built a type of quantum computer called a “quantum annealer.” These machines can currently handle a lot more qubits than universal quantum computers, but they don't use quantum logic gates and are mostly limited to tackling optimization problems like finding the shortest delivery route or figuring out the best allocation of resources.

What is a universal quantum computer?

Universal quantum computers can be used to solve a wide range of problems. They can be programmed to run quantum algorithms that make use of qubits' special properties to speed up calculations.

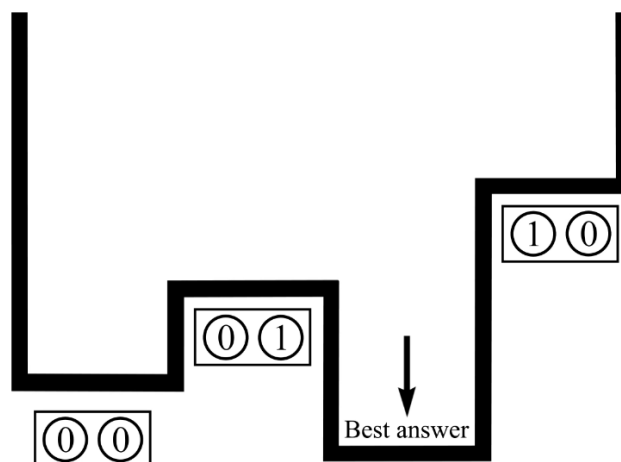
For years, researchers have been designing algorithms that are only possible on a universal quantum computer. The most well-known algorithms are Shor's algorithm for factoring large numbers (which can be used to break commonly used forms of encryption), and Grover's algorithm for quickly searching through massive sets of data.

New quantum algorithms are constantly being designed that could broaden the use cases of quantum computers even more – potentially in ways that are currently hard to predict.

What is a quantum annealer?

Quantum annealing is well suited for solving optimization problems. In other words, the approach can quickly find the most efficient configuration among many possible combinations of variables.

D-Wave offers a commercially available quantum annealer that uses the properties of qubits to find the lowest energy state of a system, which corresponds to the optimal solution for a specific problem that has been mapped against this system.



Source: D-Wave

Optimization problems are notoriously difficult for classical computers to solve due to the overwhelming number of variables and possible combinations involved. Quantum computers, however, are well suited to this type of task as different options can be sifted through at the same time.

For example, D-Wave says that Volkswagen used its quantum annealer to make its paint shops more efficient by figuring out how to reduce color switching on its production line by more than a factor of 5. Meanwhile, Canadian grocer Save-On-Foods claims that D-Wave's system helped it reduce the time taken to complete a recurring business analytics task from 25 hours per week to just 2 minutes.

Though quantum annealers are good at optimization problems, they cannot be programmed to solve any type of calculation — unlike universal quantum computers.

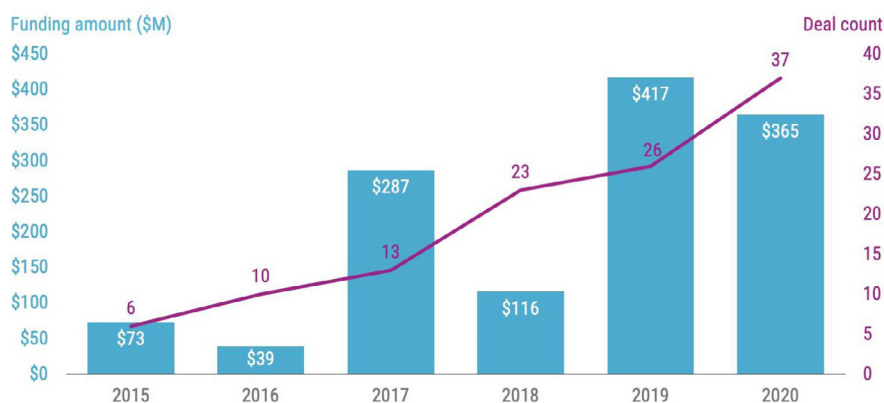
The quantum computing landscape

DEALS TO STARTUPS ARE ON THE RISE

Deals to quantum computing-focused startups have climbed steadily over the last few years and set a new record in 2020 with 37 deals.

Quantum computing deals are on the rise

Disclosed deals & equity funding (\$M), 2015 – 2020



Source: cbinsights.com

 CBINSIGHTS

PsiQuantum is the most well-funded startup in the space, with \$278.5M in total disclosed funding. Backed by Microsoft's venture arm, the company claims that its optical-based approach to quantum computing could deliver a 1M qubit machine in just a few years — far beyond what other companies say they can deliver in that timeframe.

[Cambridge Quantum Computing](#) is the most well-funded startup focused primarily on quantum computing software. The company has raised \$95M in disclosed funding from investors including IBM, Honeywell, and more. It offers a platform to help enterprises build out quantum computing applications in areas like chemistry, finance, and machine learning.

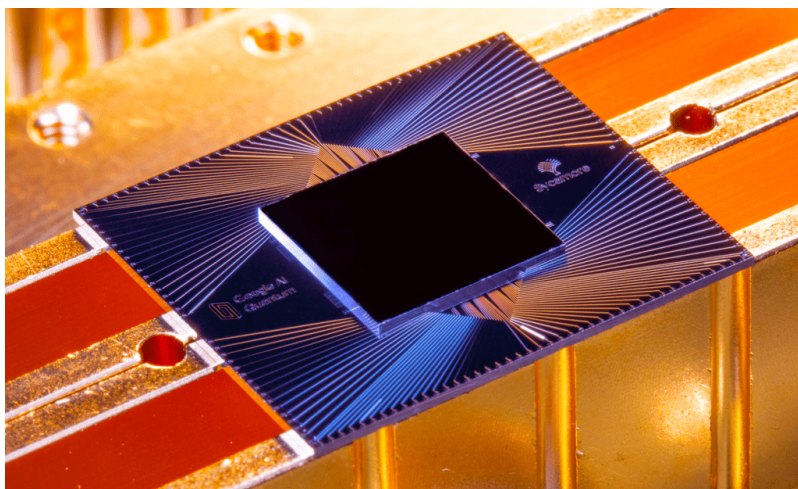
The most active VCs in the space include:

- Threshold Ventures (formerly Draper Fisher Jurvetson), which was an early backer of D-Wave and has participated in many of its follow-on rounds
- Quantonation, a France-based VC which has provided seed funding to several quantum computing startups
- Founders Fund, which has backed PsiQuantum, [Rigetti](#), and [Zapata](#)

CORPORATES AND BIG TECH COMPANIES ARE GOING AFTER QUANTUM COMPUTING

Corporates are also making waves in the quantum computing space.

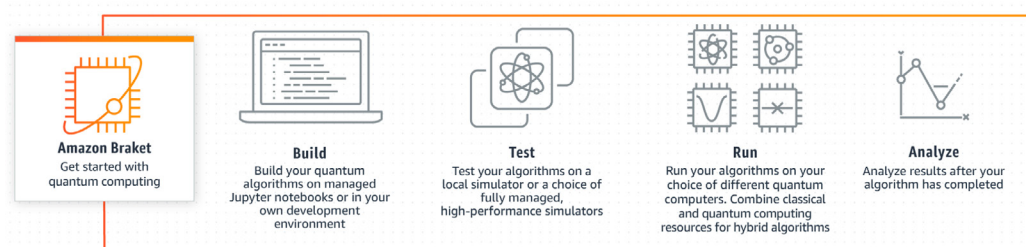
For example, Google is developing its own quantum computing hardware and has hit several key milestones, including the first claims of quantum supremacy and simulating a chemical reaction using a quantum computer. Google entities have also invested in startups in the space, including [IonQ](#), [ProteinQure](#), and [Kiano](#).



Google's Sycamore processor was used to achieve quantum supremacy. Source: Google

IBM is another corporation developing quantum computing hardware. It has already built numerous quantum computers, but it wants to develop a much more powerful 1,000-qubit machine by 2023. From a commercial side, the company runs a platform called the IBM Q Network that gives participants — including Samsung and JPMorgan Chase — access to quantum computers over the cloud and helps them experiment with potential applications for their businesses.

Meanwhile, Microsoft and Amazon have partnered with companies like IonQ and Rigetti to make quantum computers available on Azure and AWS, their respective cloud platforms. Both tech giants have also established development platforms that aim to help enterprises experiment with the technology.



Cloud service providers like AWS and Azure are already hosting quantum computers.
Source: Amazon

An array of other big tech companies including Honeywell, Alibaba, Intel, and more are also looking to build quantum computing hardware.

Uses of quantum computing across industries

As quantum computing matures and becomes more accessible, we'll see a quick uptick in companies applying it to their own industries.

Some of these implications are already being felt across different sectors.

“We believe we’re right on the cusp of providing capabilities you can’t get with classical computing. In almost every discipline you’ll see these types of computers make this kind of impact.”

– VERN BROWNELL, FORMER CEO, D-WAVE SYSTEMS

From healthcare to agriculture to artificial intelligence, the industries listed below could be among the first to adopt quantum computing.

HEALTHCARE

Quantum computers could impact healthcare in a number of ways.

For example, Google recently announced that it had used a quantum computer to simulate a chemical reaction, a milestone for the nascent technology.

Though the specific interaction was relatively simple — current classical computers can model it too — future quantum computers are predicted to be able to simulate complex molecular interactions much more accurately than classical computers. Within healthcare, this could help speed up drug discovery efforts by making it easier to predict the effects of drug candidates.

Another area where drug discovery could see a boost from quantum computing is protein folding. Startup [ProteinQure](#) — which was featured by CB Insights in the 2020 cohorts for the [AI 100](#), and [Digital Health 150](#) — is already tapping into current quantum computers to help predict how proteins will fold in the body. This is a notoriously difficult task for conventional computers. But using quantum computing to address the issue could ultimately make designing powerful protein-based medicines easier.

Eventually, quantum computing could also lead to better approaches to personalized medicine by allowing faster genomic analysis to inform tailored treatment plans specific to every patient.

Genome sequencing creates lots of data, meaning that analyzing a person's DNA requires a lot of computational power. Companies are already rapidly reducing the cost and resources needed to sequence the human genome; but a powerful quantum computer could sift through this data much more quickly, making genome sequencing more efficient and easier to scale.

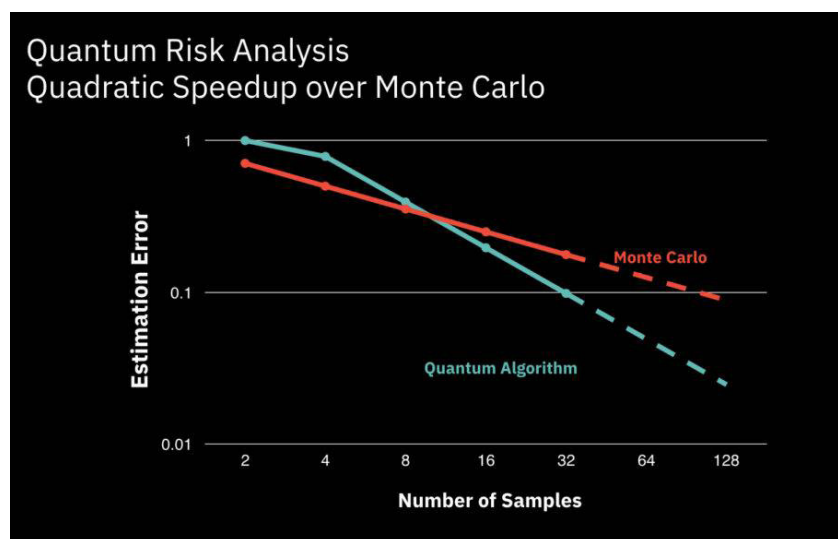
A number of pharma giants have shown interest in quantum computing. Merck's venture arm, for instance, participated in Zapata's \$38M Series B round in September. Meanwhile, Biogen partnered with quantum computing software startup [1QBit](#) and Accenture to build a platform for comparing molecules to help speed up the early stages of drug discovery.

CB Insights clients can [check out this report for more on how quantum technologies are reshaping healthcare](#).

FINANCE

Financial analysts often rely on computational models that build in probabilities and assumptions about the way markets and portfolios will perform. Quantum computers could help improve these by parsing through data more quickly, running better forecasting models, and more accurately weighing conflicting possibilities. They could also help solve complex optimization problems related to tasks like portfolio risk optimization and fraud detection.

Another area of finance quantum computers could change are Monte Carlo simulations — a probability simulation used to understand the impact of risk and uncertainty in financial forecasting models. IBM published research last year on a method that used quantum algorithms to outcompete conventional Monte Carlo simulations for assessing financial risk.



Source: IBM

A number of financial institutions including RBS, the Commonwealth Bank of Australia, Goldman Sachs, Citigroup, and more, have invested in quantum computing startups.

Some are already starting to see promising results. John Stewart, RBS's head of global innovation scouting and research told The Times newspaper that the bank was able to reduce the time taken to assess how much money needed to be offset for bad loans from weeks to "seconds" by using quantum algorithms developed by 1QBit.

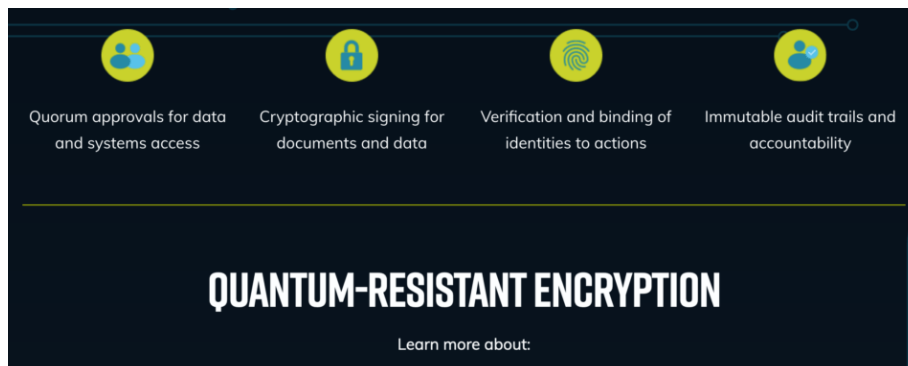
CYBERSECURITY

Cybersecurity could be upended by quantum computing.

Powerful quantum computers threaten to break cryptography techniques like RSA encryption that are commonly used today to keep sensitive data and electronic communications secure.

This prospect emerges from Shor's Algorithm, a quantum algorithm that was theorized in the 1990s. This technique describes how a suitably powerful quantum computer — which some expect could emerge around 2030 — could very quickly find the prime factors of large numbers, a task that classical computers find extremely difficult. RSA encryption relies on this very challenge to protect data being shuttled around online.

But several companies are emerging to counter this threat by developing new encryption methods, collectively known as "post-quantum cryptography." These methods are designed to be more resilient to quantum computers — often by creating a problem that even a powerful quantum computer wouldn't be expected to have many advantages in trying to solve. Companies in the space include [Isara](#) and [Post Quantum](#), among many more. The US National Institute of Standards and Technology (NIST) is also backing the approach and is planning to recommend a post-quantum cryptography standard by 2022.



Source: Post Quantum

Another nascent quantum information technology called quantum key distribution (QKD) could offer some respite from quantum computers' code-breaking abilities. QKD works by transferring encryption keys using entangled qubits. Since quantum systems are altered when measured, it's possible to check if an eavesdropper has intercepted a QKD transmission. Done right, this means that even quantum computer-equipped hackers would have a hard time stealing information.

Though QKD currently faces practical challenges like the distance over which it is effective (most of today's QKD networks are pretty small), many are expecting it to soon become a big industry. Toshiba, for instance, said in October that it expects to generate \$3B in revenue from QKD applications by the end of the decade.

CB Insights clients can see private companies working on post-quantum cryptography and QKD in [this market map](#).

BLOCKCHAIN AND CRYPTOCURRENCIES

Quantum computing's threat to encryption extends to blockchain tech and cryptocurrencies — including Bitcoin and Ethereum — which rely upon quantum-susceptible encryption protocols to complete transactions.

Though specific quantum threats to blockchain-based projects vary, the potential fallout could be severe. For example, about 25% of bitcoins (currently worth \$173B+) are stored in such a way that they could be easily stolen by a quantum-computer equipped thief, according to an analysis from Deloitte. Another fear is that quantum computers could eventually become powerful enough to decrypt and interfere with transactions before they're verified by other participants on the network, undermining the integrity of the decentralized system.

And that's just Bitcoin. Blockchain tech is being used more and more for applications within asset trading, supply chains, identity management, and much more.

Rattled by the profound risks posed by quantum computers, a number of players are moving to make blockchain tech safer. Established networks like Bitcoin and Ethereum are experimenting with quantum-resistant approaches for future iterations, a new blockchain protocol called the Quantum Resistant Ledger has been set up that's specifically designed to counter quantum computers, and startups including [QuSecure](#) and [Qaisec](#) say that they're working on quantum-resistant blockchain tech for enterprises.

Quantum-resistant blockchains may not fully emerge until post-quantum cryptography standards are more firmly established in the coming years. In the meantime, those running blockchain projects will likely be keeping a nervous eye on quantum computing advancements.

Check out [our explainer for more on how blockchain tech works](#).

ARTIFICIAL INTELLIGENCE

Quantum computers' abilities to parse through massive data sets, simulate complex models, and quickly solve optimization problems have drawn attention for applications within artificial intelligence.

Google, for instance, says that it's developing machine learning tools that combine classical computing with quantum computing, stating that it expects these tools to even work with near-term quantum computers.

Similarly, quantum software startup Zapata recently stated that it sees quantum machine learning as one of the most promising commercial applications for quantum computers in the short term.

Though quantum-supported machine learning may soon offer some commercial advantages, future quantum computers could take AI even further.

AI that taps into quantum computing could advance tools like computer vision, pattern recognition, voice recognition, machine translation, and more.

Eventually, quantum computing may even help create AI systems that act in a more human-like way. For example, enabling robots to make optimized decisions in real-time and more quickly adapt to changing circumstances or new situations.

Take a look at [this report for other emerging AI trends](#).

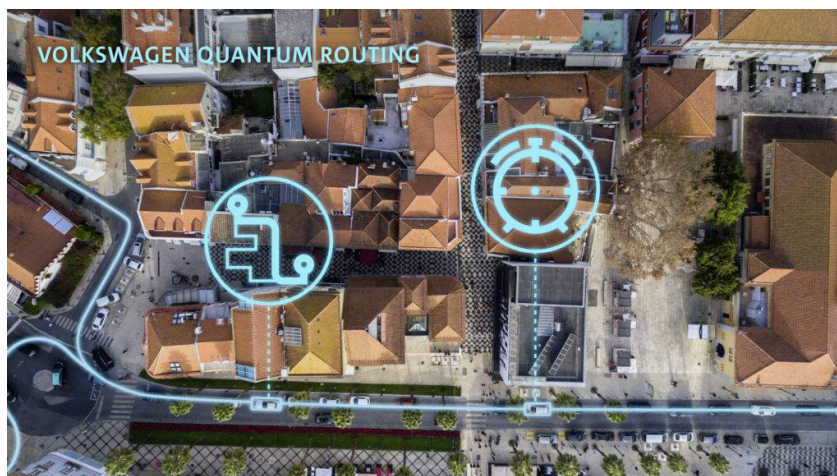
LOGISTICS

Quantum computers are good at optimization. In theory, a complex optimization problem that would take a supercomputer thousands of years to solve could be handled by a quantum computer in just a matter of minutes.

Given the extreme complexities and variables involved in international shipping routes and orchestrating supply chains, quantum computing could be well-placed to help tackle daunting logistics challenges.

DHL is already eyeing quantum computers to help it more efficiently pack parcels and optimize global delivery routes. The company is hoping to increase the speed of its service while also making it easier to adapt to changes — such as canceled orders or rescheduled deliveries.

Others want to improve traffic flows using quantum computers, a capability that could help delivery vehicles make more stops in less time.



Source: Volkswagen.

For example, Volkswagen, in partnership with D-Wave Systems, ran a pilot last year to optimize bus routes in Lisbon, Portugal. The company said that each of the participating buses was assigned an individual route that was updated in real-time based on changing traffic conditions. Volkswagen states that it intends to commercialize the tech in the future.

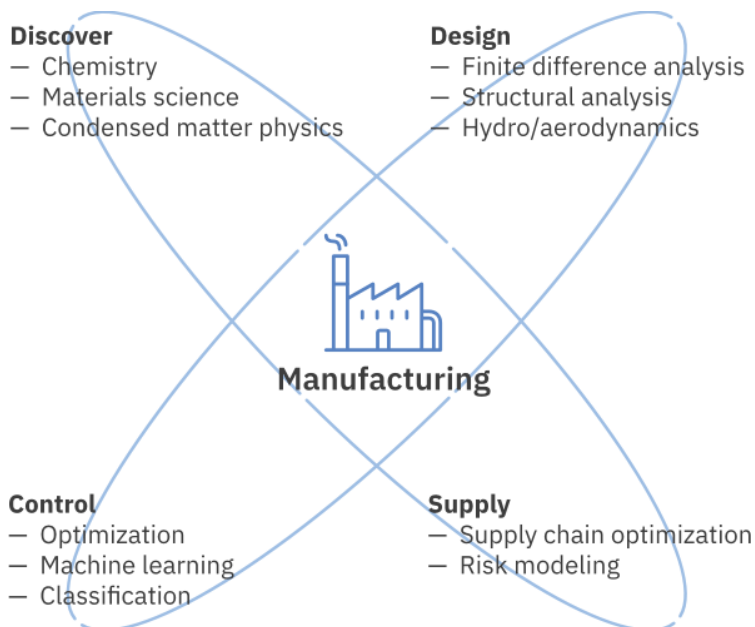
MANUFACTURING AND INDUSTRIAL DESIGN

Quantum computing is also drawing interest from big players thinking about manufacturing and industrial design.

For example, Airbus — a global aerospace corporation — established a quantum computing unit in 2015 and has also invested in quantum software startup [QC Ware](#) and quantum computer maker IonQ.

One area the company is looking at is quantum annealing for digital modeling and materials sciences. For instance, a quantum computer could filter through countless variables in just a few hours to help determine the most efficient wing design for an airplane.

IBM has also identified manufacturing as a target market for its quantum computers, with the company highlighting areas like materials science, advanced analytics for control processes, and risk modeling as key applications for the space.



*A selection of IBM's envisioned manufacturing applications for quantum computing.
Source: IBM*

Though quantum computing will likely be implemented in manufacturing only gradually as more powerful machines emerge over the coming years, some companies — including machine learning startup [Solid State AI](#) — are already offering quantum-supported services for the industry.

AGRICULTURE

Quantum computers could boost agriculture by helping to produce fertilizers more efficiently.

Nearly all of the fertilizers used in agriculture around the world rely on ammonia. The ability to produce ammonia (or a substitute) more efficiently would mean cheaper and less energy-intensive fertilizers. In turn, easier access to better fertilizers could help feed the planet's growing population.

Ammonia is in high demand and is estimated to be a \$77B global market by 2025, according to CB Insights' Industry Analyst Consensus.

Little recent progress has been made on improving the process to create or replace ammonia because the number of possible catalyst combinations that could help us do so is extremely large — meaning that we essentially still rely on an energy-intensive technique from the 1900s known as the Haber-Bosch Process.

Using today's supercomputers to identify the best catalytic combinations to make ammonia would take centuries to solve.

However, a powerful quantum computer could be used to much more efficiently analyze different catalyst combinations — another application of simulating chemical reactions — and help find a better way to create ammonia.

Moreover, we know that bacteria in the roots of plants make ammonia every day with a very low energy cost using a molecule called nitrogenase. This molecule is beyond the abilities of our best supercomputers to simulate, and hence better understand, but it could be within the reach of a future quantum computer.

NATIONAL SECURITY

Governments around the world are investing heavily in quantum computing research initiatives, partly in an attempt to bolster national security.

Defense applications for quantum computers could include, among many others, code breaking for spying, running battlefield simulations, and designing better materials for military vehicles.

Earlier this year, for instance, the US government announced an almost \$625M investment in quantum technology research institutes run by the Department of Energy — companies including Microsoft, IBM, and Lockheed Martin also contributed a combined \$340M to the initiative.

Similarly, China's government has put billions of dollars behind numerous quantum technology projects and a team based in the country recently claimed to have achieved a quantum computing breakthrough.

Though it is uncertain when quantum computing may play an active role in national security, it is beyond doubt that no country will want to fall behind the capabilities of its rivals. A new “arms race” has already begun.

The outlook for quantum computing

It will be a while yet before quantum computers can live up to the lofty expectations many have for the tech, but the industry is developing fast.

In 2019, Google announced that it had used a quantum computer to complete a task much more quickly than a classical counterpart could manage. Though the specific problem solved is not of much practical use, it marks an important milestone for the nascent quantum computing industry.

Looking ahead, many think that we'll see quantum computers drastically outpace classical counterparts at useful tasks by the end of the decade.

In the meantime, expect an increasing number of commercial applications to emerge that make use of near-term quantum computers. It may not matter to businesses that these initial applications won't represent quantum computing's full potential — a commercial advantage doesn't have to be revolutionary to still be lucrative.

Despite this momentum, the space faces a number of hurdles. Significant technical barriers must be surmounted around critical issues like error correction and stability, tools to help more businesses develop software for quantum computers will need to become established, and companies sizing up quantum computing might need to start hiring for brand new skill sets from a small pool of talent.

But the payoff may still be worth it. Some think that quantum computing represents the next big paradigm shift for computing — akin to the emergence of the internet or the PC. Businesses would be right to be concerned about missing out.

Additional reading

This report was created with data from CB Insights' emerging technology insights platform, which offers clarity into emerging tech and new business strategies through tools like:

- [Earnings Transcripts Search Engine & Analytics](#) to get an information edge on competitors' and incumbents' strategies
- [Patent Analytics](#) to see where innovation is happening next
- [Company Mosaic Scores](#) to evaluate startup health, based on our National Science Foundation-backed algorithm
- [Business Relationships](#) to quickly see a company's competitors, partners, and more
- [Market Sizing Tools](#) to visualize market growth and spot the next big opportunity

If you aren't already a client, [sign up for a free trial](#) to learn more about our platform.