CB INSIGHTS

What Is Quantum Computing?

2019

CBINSIGHTS

WHAT IS CB INSIGHTS?

CB Insights is a tech market intelligence platform that analyzes millions of data points on venture capital, startups, patents, partnerships and news mentions to help you see tomorrow's opportunities, today.

CLICK HERE TO LEARN MORE

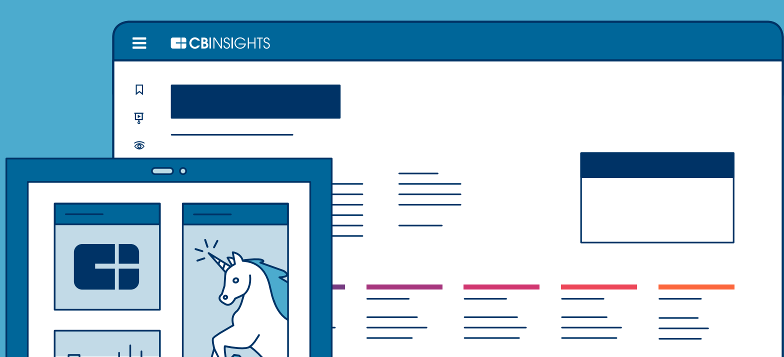


Table of Contents

CONTENTS

Intro

Quantum computing is poised to upend entire industries from telecommunications and cybersecurity to advanced manufacturing, finance, medicine, and beyond — but few understand how quantum computers actually work.

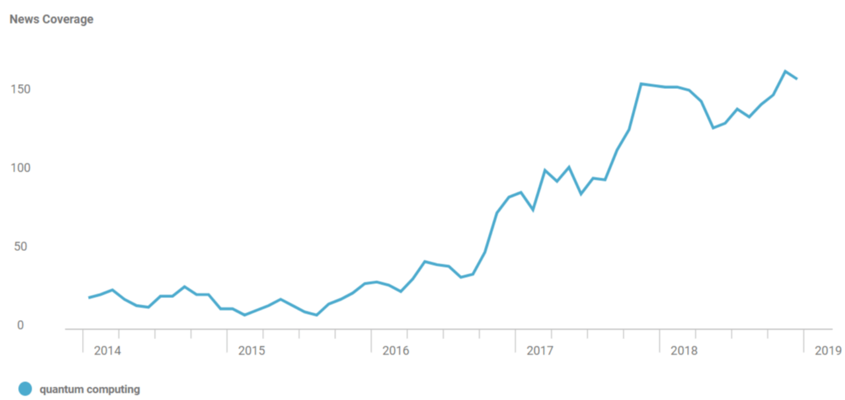
In the near future, quantum computing could change the world.

Take climate change for example: Because of the complexity of the climate system, seemingly endless data, and growing limitations on today's computing power, no classical computer (like your desktop) can simulate the earth's climate changes with 100% accuracy.

Quantum computers, on the other hand, are supercomputers equipped with advanced processing powers. Taking tons of climate variables into account, they could create data-driven models to help forecast weather patterns and prepare for natural disasters.

Beyond climate simulations, these advanced computing systems could make ultra-fast calculations on the biggest and most complex datasets — and the technology is certainly catching media attention.

News Coverage



But how exactly does it work?

What is quantum computing?

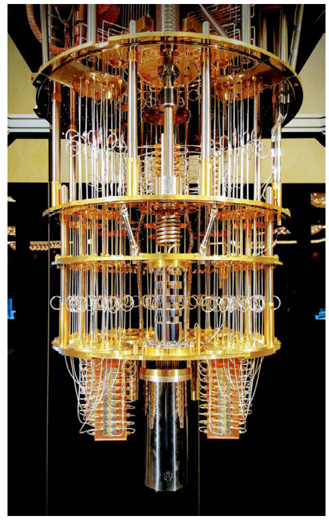
Quantum computers can process massive and complex datasets more efficiently than classical computers.

They use the fundamentals of quantum mechanics to speed up the process of solving complex computations. Often those computations incorporate a seemingly unlimited number of variables, and the potential applications span industries from genomics to finance.

Quantum computers are already reinventing aspects of cybersecurity through their ability to break codes and encrypt electronic communications. Some of the biggest players in tech — including Google, Microsoft, Intel, IBM, and Alibaba — are exploring quantum computing for better cybersecurity and more, a sign that the next big computing race is already underway.

While Google has been exploring quantum computing for ultra-fast internet search since at least 2009, it remains to be seen who will emerge as the leader in the nascent commercial quantum computing industry.

In this explainer, we dive more into what quantum computing is, the benefits associated with the technology, its applications, and industry players to watch.



IBM's "Q" machine

A changing computing landscape

Before we can understand quantum computing and its applications, we must take a look at how its predecessor — classical computing (transistor-based computing) — has reached its limits.

Note, classical bits (stored on transistors) are the basic units f information processing in a classical computer.

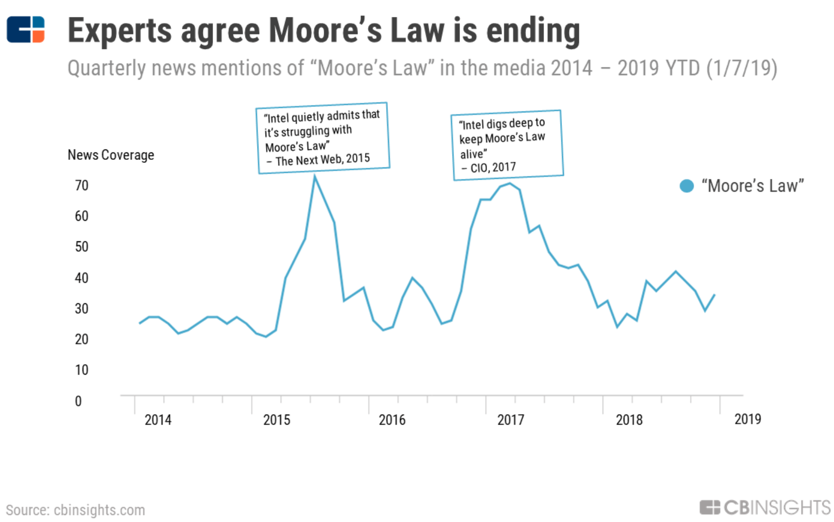
They are basically electronic on/off switches embedded in microchips that alternate between 0 or 1 to process information. The more transistors on a chip, the faster the chip can process electrical signals, and the better a computer becomes.

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 while the costs were cut in half (since their invention in 1958). This observation is known as Moore's Law.

Moore's Law is significant because it means that computers and computing power both get smaller and faster over time.

However, Moore's law is slowing down (some say to a halt), and consequently, classical computers are not improving at the same rate they used to.



Intel, unsurprisingly, has relied on Moore's Law to fuel chip innovation for the last 50+ years. Now, Intel, along with other computer manufacturing giants, has suggested that transistor-based computing is approaching a wall.

Sometime in the 2020s — if we want to continue to reap the benefits of exponential growth in computing power — we will have to find a fundamentally different way of processing information.

Enter quantum computing.

THE RISE OF QUANTUM COMPUTING

Quantum computers could offer a huge efficiency advantage for solving certain types of computations that stump today's computers — and would continue to stump them even if Moore's Law were to carry on indefinitely.

For starters, think about a phone book, and then imagine you have a specific number to look up in that phone book. A classical computer will search each line of the phone book, until it finds and returns the match. In theory, a quantum computer could search the entire phone book instantaneously, assessing each line simultaneously and returning the result much faster than a classical computer.

These problems, which require the best combination of variables and solutions, are often called optimization problems. They are some of the most complex problems in the world, with potentially game-changing benefits.

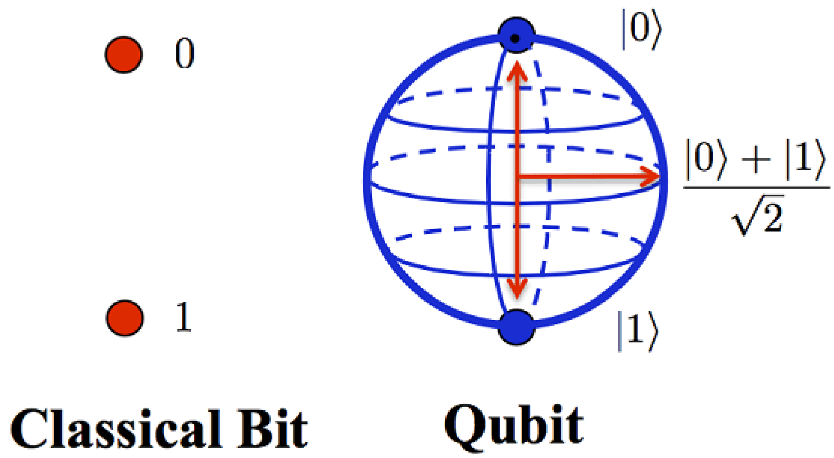
Imagine you are building the world's tallest skyscraper, and you have a budget for the construction equipment, raw materials, and labor, as well as compliance requirements. The problem you need to solve is how to determine the optimum combination of equipment, materials, and labor, etc. to maximize your investment. Quantum computing could help factor in all these variables to help us most efficiently plan for massive projects.

Optimization problems are faced across industries including software design, logistics, finance, web search, genomics, and more. While the toughest optimization problems in these industries stump classical computers, they are well-suited for being solved on a quantum machine.

Quantum computers differ from classical computers in that improvement for the latter mainly relies on advancement in the materials that make up transistors and microchips.

Quantum computers do not use transistors (or classical bits). Instead, they use qubits.

Qubits are the basic units for processing information in a quantum computer.



Qubits can be any value from 0 to 1, or have properties of both of these values simultaneously. Right away, there are a whole lot more possibilities for performing computations.

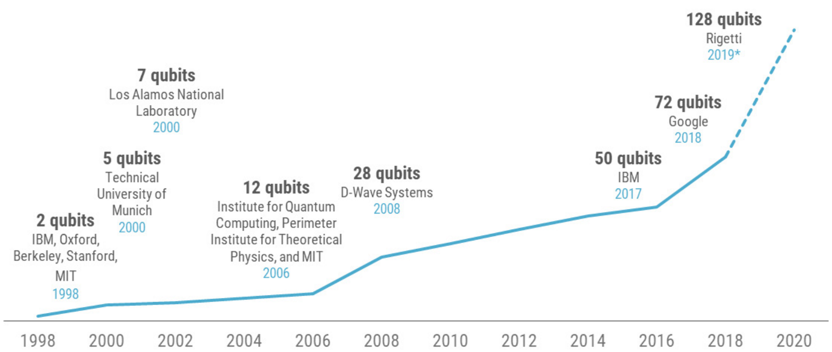
Additionally, quantum computers rely on naturally occurring quantum-mechanical phenomena, or two important states of matter known as superposition and entanglement. These states of matter, when harnessed for computing purposes, can speed up our ability to perform immense computations.

The most advanced quantum computing chips available today, under development by Berkeley-based startup Rigetti Computing, can make use of up to 19 qubits, although the company is in the process of creating a 128 qubit chip by late 2019.

However, the race to build the most powerful quantum computer with the most qubits has been underway since at least the late 1990s.

Quantum computers are getting more powerful

Number of qubits achieved by date and organization 1998 – 2020*



Source: MIT, Qubit Counter. *Rigetti quantum computer expected by late 2019. CBINSIGHTS

In 1998, Oxford University researchers in the UK announced that they had made a breakthrough with the ability to compute information using two qubits. Fast forward to 2017, and IBM proved the ability to compute on 50 qubits. Quantum computing power increased by 25x in 20 years — a seemingly slow start compared to today's pace of advancement.

In 2018, Google demonstrated 72 qubit information processing. In August, Rigetti Computing announced plans for a 128 qubit quantum chip.

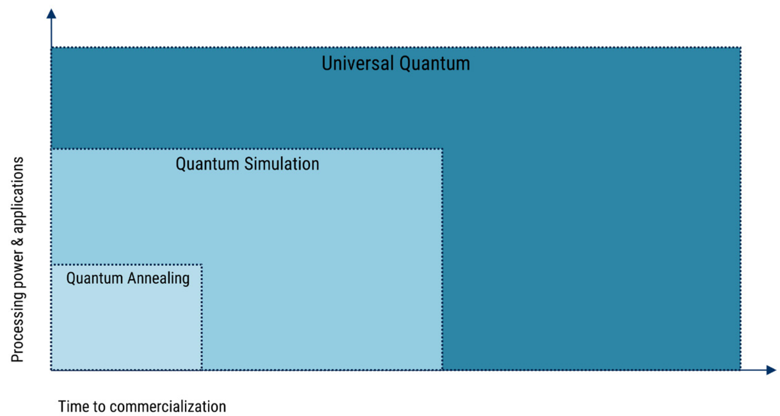
Steve Jurvetson, managing director of the investment firm Draper Fisher Jurvetson and an investor in the quantum computing company D-Wave Systems (an early leader specializing in hybrid-quantum and classical machines), dubbed the phenomenon of the increasing capacity of quantum computers as "Rose's Law."

Rose's Law for quantum computing parallels the idea behind Moore's Law for semiconductor processor development. In short, quantum computers are already getting really fast, really quickly.

Types of quantum computing

There are three primary types of quantum computing. Each type differs by the amount of processing power (qubits) needed and number of possible applications, as well as the time required to become commercially viable.

Three types of quantum computing



Source: cbinsights.com

CBINSIGHTS

QUANTUM ANNEALING

Quantum annealing is best for solving optimization problems.

In other words, researchers are trying to find the best (most efficient) possible configuration among many possible combinations of variables.

For example, Volkswagen (VW) recently conducted a quantum experiment to optimize traffic flows in the overcrowded city of Beijing, China. The experiment was run in partnership with Google and D-Wave Systems.

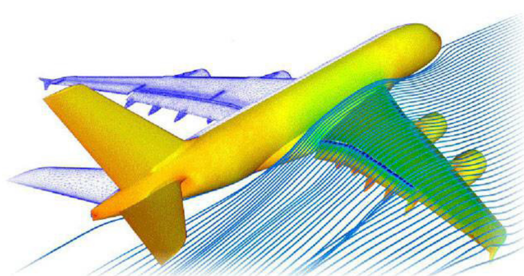
The algorithm could successfully reduce traffic by choosing the ideal path for each vehicle, according to VW.

Imagine applying this experiment on a global scale — optimizing every airline route, airport schedule, weather data, fuel costs, and passenger information, etc. for everyone, to get the most cost efficient travel and logistics solutions.

Classical computers would take thousands of years to compute the optimum solution to such a problem. Quantum computers, theoretically, can do it in a few hours or less, as the number of qubits per quantum computer increases.

Annealing applies to an array of industry problems. For example, Airbus — a global aerospace & defense corporation known for developing military and commercial aircraft — established a quantum computing unit at its Newport, UK plant in 2015.

The company is exploring quantum annealing for digital modeling and materials sciences.



Airflow modeling of an aircraft wing

While it currently takes engineers years to model the process of air flowing over an aircraft's wing, a quantum computer could take just a few hours to model every single atom of air flowing over a wing at all angles and speeds to determine the optimum or most efficient wing design.

Quantum annealing is the least powerful and most narrowly applied form of quantum computing.

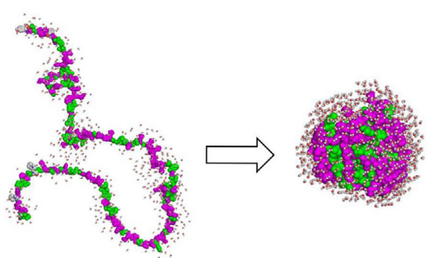
In fact, experts agree that today's supercomputers can solve some optimization problems on par with today's quantum annealing machines.

QUANTUM SIMULATIONS

Quantum simulations explore specific problems in quantum physics that are beyond the capacity of classical systems. Simulating complex quantum phenomena could be one of the most important applications of quantum computing.

One area that is particularly promising includes modeling the effect of a chemical stimulation on a large number of subatomic particles — otherwise known as quantum chemistry.

In particular, quantum simulators could be used to simulate protein folding — one of biochemistry's toughest problems.



Unfolded versus folded protein structure

Misfolded proteins can cause diseases like Alzheimer's and Parkinson's, and researchers testing new treatments must learn which drugs cause reactions for each protein through the use of random computer modeling.

It is said that if a protein were to attain its correctly folded configuration by sequentially sampling all the possible drug-induced effects, it would require a time longer than the age of the universe to arrive at its correct natural state.

A realistic mapping of the protein folding sequence would be a major scientific and healthcare breakthrough that could save lives.

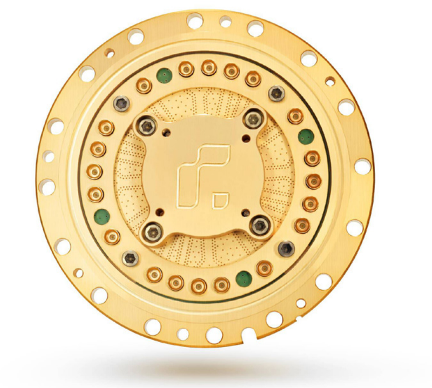
Quantum computers can help compute the vast number of possible protein folding sequences for making more effective medications. In the future, quantum simulations will enable rapid designer drug testing by accounting for every possible protein-to-drug combination.

UNIVERSAL QUANTUM COMPUTING

Universal quantum computers are the most powerful and most generally applicable, but also the hardest to build. A truly universal quantum computer would likely make use of over 100,000 qubits — some estimates put it at 1M qubits. Remember that today, the most qubits we can access is not even 128.

The basic idea behind the universal quantum computer is that you could direct the machine at any massively complex computation and get a quick solution. This includes solving the aforementioned annealing equations, simulating quantum phenomena, and more.

Researchers have been designing algorithms for years that are only possible on a universal quantum computer. The most well-known algorithms are Shor's algorithm for factoring numbers (to be used for advanced code breaking), and Grover's algorithm for quickly searching unstructured and massive sets of data (to be used for advanced internet search, etc).



Rigetti's 128 qubit quantum chip

At least 50 other unique algorithms have been developed to run on a universal quantum computer.

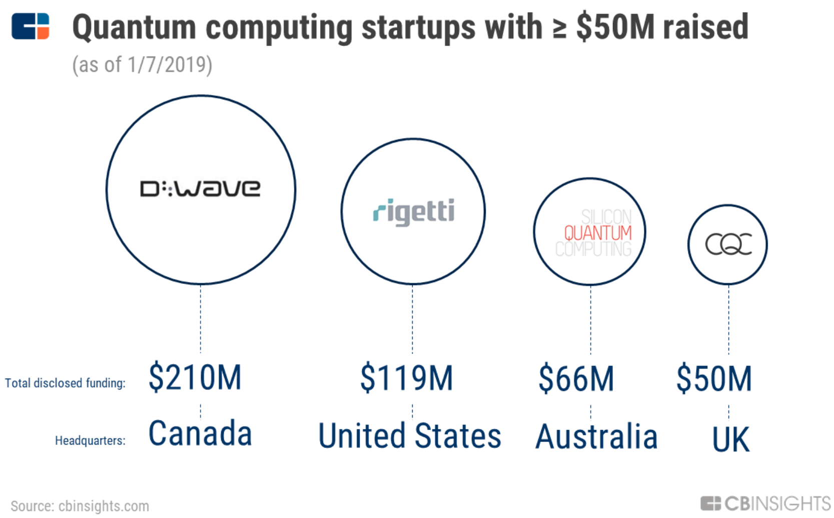
In the distant future, universal quantum computers could revolutionize the field of artificial intelligence.

Quantum AI could enable machine learning that is faster than that of classical computers.

Recent work has produced algorithms that could act as the building blocks of quantum machine learning, but the hardware and software to fully realize quantum artificial intelligence are still as elusive to us as a general quantum computer itself.

Quantum computing industry landscape

There are only a small number of private companies in the industry that have been able to raise at least $50M (and fewer with over $100M), which suggests that commercial application of quantum computers — for both hardware and software — is nascent at this point, despite the hype.

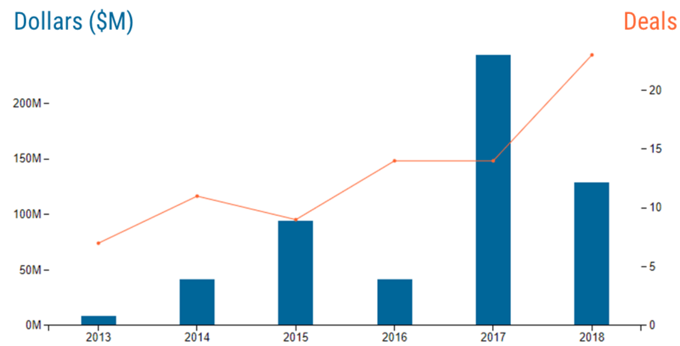


D-Wave is the most well-funded private quantum computing company with $210M raised to date, followed by Rigetti Computing ($119M), Silicon Quantum Computing ($66M), and Cambridge Quantum Computing (CQC) ($50M).

Notably, deals to these four companies accounted for ~70% of the industry's total funding since 2013. Additionally, deals to private quantum computing companies overall reached an all-time high in 2018.

Dollars and deals to quantum computing startups

2013 – 2018



Source: cbinsights.com

Over the past 6 years, total deals increased over 200% — from 7 in 2013 to 24 in 2018. Among the top deals in 2018, Rigetti Computing raised a $50M Series C in August.

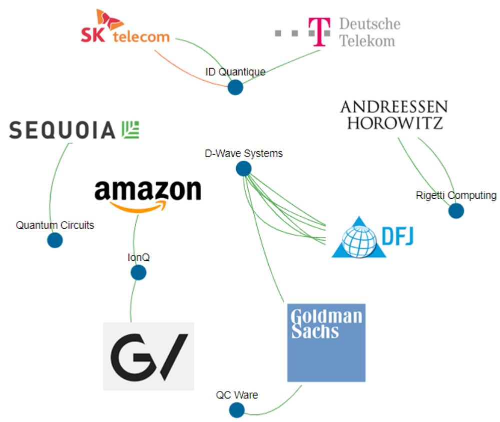
In 2017, total funding to quantum computing startups reached an all-time high at over $200M invested across just 14 deals. Notably, five startups raised rounds of over $20M in 2017, including: Silicon Quantum Computing, Rigetti, 1QBit, IonQ, and D-Wave.

WHO'S INVESTING IN QUANTUM COMPUTING?

In tandem with increasing interest across the space, the overall ecosystem supporting the development of these companies is also growing. Mainstream VCs along with corporations are already betting on private quantum computing companies.

Select investors betting on quantum computing startups

2010 – 2019 YTD (1/7/2019)



Source: cbinsights.com

CBINSIGHTS

green lines = investments
orange lines = acquisitions

Google Ventures (GV) and Amazon, among others, have backed IonQ, which is developing general purpose quantum computers to address a broad array of applications. Notable VCs in the industry include Sequoia Capital, which invested in quantum computing hardware company Quantum Circuits, Inc. (QCI). Andreessen Horowitz (a16z) has invested in Rigetti Computing and Draper Fisher Jurvetson (DFJ) has been involved with multiple investments in D-Wave Systems.

Securing communications with quantum computing got a boost in February 2018, when South Korean mobile telecommunications operator SK Telecom entered the game, followed by Germany's Deutsche Telekom a few months later. The telecom companies bought a $65M majority stake and a minority stake, respectively, in ID Quantique, a provider of multi-protocol network encryption for securing communications based on quantum technologies.

Some of the world's largest corporations are also pursuing in-house quantum computing projects.

Google operates a D-Wave Systems quantum computer in the Quantum Artificial Intelligence Lab (QuAIL). The lab is hosted by NASA and the Universities Space Research Association at the NASA Ames Research Center in Mountain View, California.

In July 2015, Alibaba's Aliyun cloud unit and the Chinese Academy of Sciences established a research facility based in Shanghai called the Alibaba Quantum Computing Laboratory. The lab looks into quantum security technology for e-commerce and data centers.

In January 2019, IBM unveiled its first commercial quantum computer at the Consumer Electronics Show (CES). IBM's Q System One uses 20 qubits and has both classical and quantum components. The company's announcement made it clear that it will take time before commercial quantum computers can beat today's classical machines:

"IBM Q systems are designed to *one day* tackle problems that are currently seen as too complex and exponential in nature for classical systems to handle."

An array of other tech companies including Hewlett Packard, Intel, and Microsoft are also pursuing quantum computing.

Several defense contractors and consulting firms have also made quantum computing plays including: Booz Allen Hamilton, Lockheed Martin, and Raytheon, among others.

Along with company investments, the EU, US, Australian, and Chinese governments are also backing projects aimed at building quantum computers.

In the US, NASA, the NSA, and the Los Alamos National Laboratory are all involved in quantum computing projects.

China's government launched the world's first quantum satellite in the quest for more secure communications in 2016.

Quantum computing across industries

As the cost of quantum computing resources comes down, more industry players will emerge.

And as more players delve into the industry, quantum computing will see increasing applications across industries, especially as classical computers prove inefficient in some cases.

We are already beginning to see its implications across different sectors.

“We’re at the dawn of this quantum computing age. 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, CEO, D-Wave Systems

From healthcare to agriculture, here are several sectors that would benefit from quantum computing’s potential.

HEALTHCARE

Quantum computers could help speed up the process of comparing the interactions and effects of different drugs on a range of diseases to determine the best medications.

Additionally, quantum computing could also lead to truly personalized medicine — using advancements in genomics to create tailored treatment plans specific to every patient.

DNA Double Helix

Genome sequencing creates lots of data such that a representation of a person's whole DNA strand requires massive computational power and storage capacity. Companies are rapidly bringing down the cost and resources needed to sequence the human genome; however, a quantum computer would theoretically make the way genomes are sequenced more efficient and easier to scale globally.

A quantum computer could assemble and sort through all possible gene variants at the same time and instantly find all nucleotide pairs, making the whole process of genome sequencing exponentially shorter.

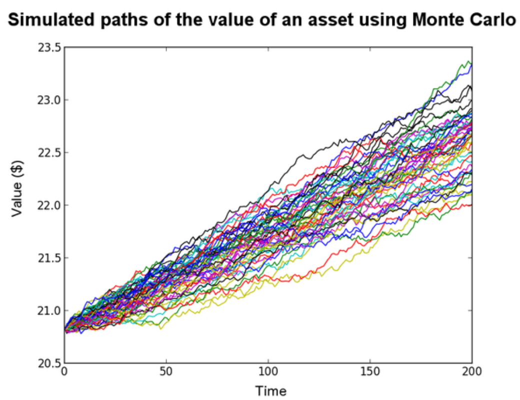
Rapid quantum genome sequencing could allow us to pool the world's DNA into a broad population health database. Using quantum computers, we would also be able to synthesize patterns in the world's DNA data for understanding our genetic makeup at a deeper level, and also potentially uncover previously unknown patterns of disease.

FINANCIAL SERVICES

Financial analysts typically rely on algorithms that are made up of probabilities and assumptions about the way markets and portfolios will perform. Quantum computing could help eliminate data blind spots and prevent unfounded financial assumptions from creating losses.

Specifically, the areas of quantum computing that show the most promise for financial services are in solving complex optimization problems such as portfolio risk optimization and fraud detection.

Quantum computing could be used to better determine attractive



Monte Carlo simulation in finance

portfolios given thousands of assets with interconnecting dependencies and identify key fraud patterns more effectively.

One other area of finance quantum computers could change involves running what are known commonly in the industry as Monte Carlo simulations — a probability simulation used to understand the impact of risk and uncertainty in financial forecasting models.

While classical computers can only search one file at a time or run a single Monte Carlo simulation of a portfolio, a quantum computer could perform these operations in parallel and optimize transactions more efficiently.

CYBERSECURITY

Quantum computers can be used to break cryptographic codes that we use today to keep sensitive data and electronic communications secure.

However, quantum computers could also be used to secure data from quantum hacking — a technique known as quantum encryption.

Quantum encryption is the idea of sending entangled particles of light (entangled photons) over long distances in what is known as Quantum Key Distribution (QKD) for the purpose of securing sensitive communications.

China's Micius quantum satellite

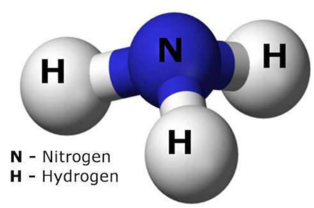
The most important point is that if quantum encrypted communications are intercepted by anyone, the encryption scheme will show immediate signs of disruption and reveal that the correspondence is not secure. This relies on the principle that the act of measuring a quantum system disrupts the system. This is known as the “measurement effect.”

AGRICULTURE

Quantum computers could help us more efficiently make fertilizers.

Nearly all of the fertilizers that help feed us are made out of ammonia. The ability to produce ammonia (or a substitute) more efficiently would mean cheaper and less energy intensive fertilizers. Easier access to better fertilizers would benefit the environment and help feed the planet’s growing population.

So little progress has been made on improving the process to create or replace ammonia because the number of possible catalyst combinations to do so is infinite.



Ammonia = nitrogen and hydrogen

Essentially, we cannot artificially simulate the process without an industrial technique from the 1900s known as the Haber-Bosch Process. The process involves extremely high heat and pressure to convert nitrogen, hydrogen, and iron into ammonia.

Using today's supercomputers to digitally test for the right catalytic combinations to make ammonia would take centuries to solve.

A quantum computer would be able to quickly analyze chemical catalytic processes, and come up with the optimal catalyst combination to create ammonia.

Moreover, we know that a tiny bacteria in the roots of plants performs this same process every day at very low energy cost using a specific molecule called nitrogenase. This molecule is beyond the abilities of our largest supercomputers to simulate, but would be within the reach of a quantum computer.

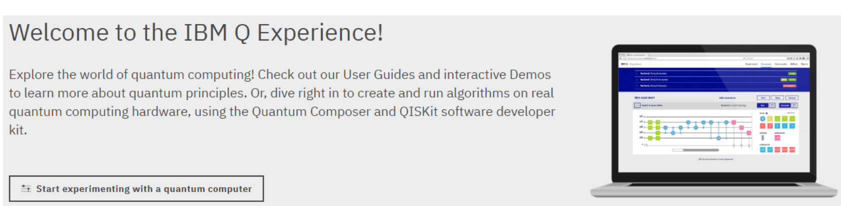
Note, producing energy efficient fertilizer is just one of the many ways we can solve big problems with the ability to accurately simulate molecular behavior. Similar problems exist across climate change, healthcare, materials sciences, energy, and more.

CLOUD COMPUTING

Quantum cloud computing is emerging as a promising field within the industry. Quantum cloud platforms could simplify programming and provide low-cost access to quantum machines.

The company QC Ware is an early-stage startup developing a cloud-based platform for quantum computing. QC Ware's backers include Airbus Ventures and Goldman Sachs, among others.

Major corporations including IBM, Google, and Alibaba are also pursuing quantum cloud computing projects.



OTHER

Remember, quantum computers are good at finding optimum solutions to problems with a seemingly infinite number of variables, protecting sensitive data and communications, and accurately simulating quantum phenomena and molecular behavior. Solving those problems is at the core of nearly every commercial application of quantum computing.

Notably, quantum computers may also be the key to safeguarding our digital future with secure software development operations.

We increasingly rely on software to drive cars, fly planes, provide healthcare, make financial decisions, and more. Quantum computers can rapidly evaluate every possible scenario and condition of a code base to find flaws before there is a problem. Capturing flaws in the code behind these critical activities could soon mean the difference between life and death for many people.

Every material sciences problem gets easier to solve with a quantum computer. Quantum computers could apply to the design of almost any material for any purpose. The range of possibilities spans transport, construction, sensors, defense, medical equipment, and much more. Materials in those industries are ultimately made of molecules and atoms whose properties and interactions are fundamentally quantum mechanical.

LOOKING AHEAD WITH QUANTUM ARTIFICIAL INTELLIGENCE

In the distant future, quantum computers could be used to accelerate the field of artificial intelligence.

Quantum machine learning could create AI that more efficiently performs complex tasks in human-like ways. For example, enabling humanoid robots to make optimized decisions in real-time and under unpredictable circumstances.

Training AI on quantum computers could advance computer vision, pattern recognition, voice recognition, machine translation, and more.

Quantum AI is still a young and unproven part of the industry. However, several startups have begun to advance research and development in the field including: Zapata Computing, Xanadu, and Qindom.

How close are we to quantum supremacy?

Quantum supremacy is the ability of quantum computers to solve problems that classical computers practically cannot. Remember, the ideal quantum computer is one that is universally applicable and superior to classical machines.

Companies and governments have claimed to operate a quantum computer that achieves quantum supremacy. In March 2018, for example, Google claimed its 72 qubit chip solved a carefully selected problem faster than classical machines. Shortly after the announcement, Alibaba's researchers announced they had solved the same problem using classical systems. The exchange underscores the veracity with which the world's most powerful companies are racing to lead the charge into quantum supremacy.

Today, the most powerful quantum computers made by companies that include D-Wave Systems, Alibaba, IBM, and Rigetti Quantum Computing, among others, are a hybrid classical quantum offering. That is, they offer a mix of powerful classical systems boosted by impressive quantum capabilities.

However, the industry is developing fast. Experts agree that by 2030, we could see quantum computers outpace classical counterparts.

Significant technical barriers must be surmounted before quantum computing achieves its potential. This will require the development of more stable hardware, commercial platforms for software development, and the development of cloud computing capabilities for the distribution and access of quantum computing resources.

CB INSIGHTS

WHERE IS ALL THIS DATA FROM?

The CB Insights platform has the underlying data included in this report

CLICK HERE TO SIGN UP FOR FREE