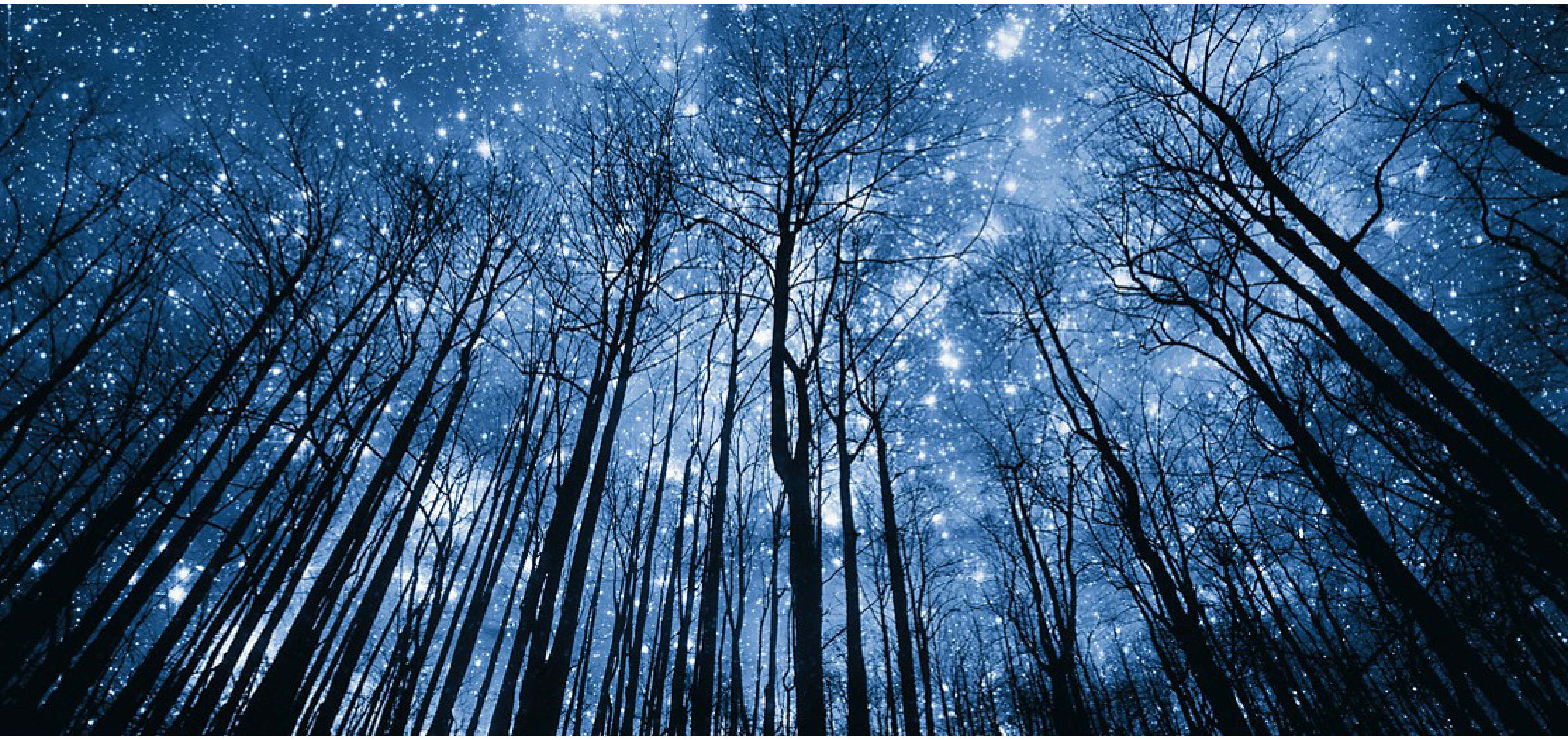
QUANTUM SUPREMACY: DATACENTER TRANSFORMATION



Sneha Venkatesh
Associate Sales Engineer Analyst
Dell Technologies
Sneha_venkatesh@dell.com

Parikshit Patil
Associate Sales Engineer Analyst
Dell Technologies
Parikshit_p@Dell.com

Sai Ganesh
Specialist 2, Inside Product
Dell Technologies
Saiganesh27.is@gmail.com

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Disclaimer: The views, processes or methodologies published in this article are those of the authors. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Abstract

The processing unit – widely considered a computer's most important component – is made up of thousands of transistors that have existed for almost 7 decades now. A computer's size and processing power are largely influenced by the number of transistors used. Over the years, transistors have become smaller and smaller, enabling our computers to become more powerful and smaller at the same time. Today, transistors as small as atoms exist. Further miniaturizing transistors is only going to become harder and soon, this process will reach its physical limits.

The purpose of this article is to help the reader realize how powerful quantum computers are, and the possibility of replacing classical computers by achieving computational feats not possible using classical computers. Some of the topics covered in this article are:

- History of quantum computers
- Limitations of classical computers
- Working of Quantum Computers
- Integration Between Quantum and Classical Computers
- Quantum Supremacy - Computational Power Breakthroughs
- Impact of Quantum Computers on Real World Applications
- New cyber-security concerns and Their Solutions
- Quantum Data Center Transformations

By understanding the working and properties of a quantum computer, this article can draw clear differences between quantum computers and classical computers as well as a hint to what the future of the IT industry could look like with the rise of quantum computers.

Quantum computers have recently shown significant development in overpowering classical computers. For example, using just a 54-qubit processor, a quantum computer has been able to complete a target computation in 200 seconds which would normally require a classical computer at least 10,000 years to complete. Since quantum computers are so powerful, our current standards of encryption could be cracked in a matter of moments. This would lead to a change in data center infrastructure, using quantum networks and quantum security which will be able to directly interface with the quantum computers while maintaining data security. Quantum computers are highly efficient as well; a quantum processor uses around 1.5kW of power compared to an average server rack which uses 5 to 10kW of power. Out of the 1.5kW, most of the power is only used for cooling purposes. Such a transformation would propel data centers into new use cases that would not be possible with classical computers.

This article brings awareness to the capabilities of immense power and potential of quantum computers, as well as its uses in the future. Many enterprise organizations are taking part in the race to conquer the quantum computing industry. For the time being there will only be a small number of quantum computing facilities because of its complexity. However, this time can be used to begin preparing data centers to welcome quantum computers; data center cooling will need to be improved to keep up with the demands of quantum computing, new racks will need to be used and these systems will need to be house in an environment which is electromagnetically isolated.

Introduction

Computer transistors are currently as tiny as we can get them with existing technology. As a result, computer scientists started looking for answers at the atomic and subatomic level; a discipline known as quantum computing.

What is quantum computing, and how does it work? Since the early twentieth century, when the atom was first investigated, quantum physics has defied logic. When we go down to the atomic and subatomic levels, it turns out that the particles don't always obey the usual principles of physics. Quantum computers operate in a fundamentally different manner than traditional computers. Instead of using transistors, which can only represent one of the binary values "1" or "0" at a time, quantum computers employ qubits, which can represent both 0 and 1 at the same time owing to a phenomenon known as “superposition.” Quantum particles may influence the state of another particle even though they are not physically connected, exist in two places at the same time, and even "teleport." Quantum computers intend to make use of these unexpected phenomena.

Classical computers outperform quantum computers in several tasks (email, spreadsheets, and desktop publishing for example). Quantum computers are intended to provide an alternative tool for solving various issues, not to replace traditional computers. Quantum computers outperform classical computers in terms of their ability to run 'Quantum Simulations,' such as chemical reactions, improving solar panels and batteries, developing new medicines, and even rapidly prototyping a variety of materials, which is much easier than physically making and testing them. Quantum computers are also excellent at tackling optimization issues, such as calculating the optimum method to schedule aircraft at an airport or determining the optimal FedEx truck delivery routes.

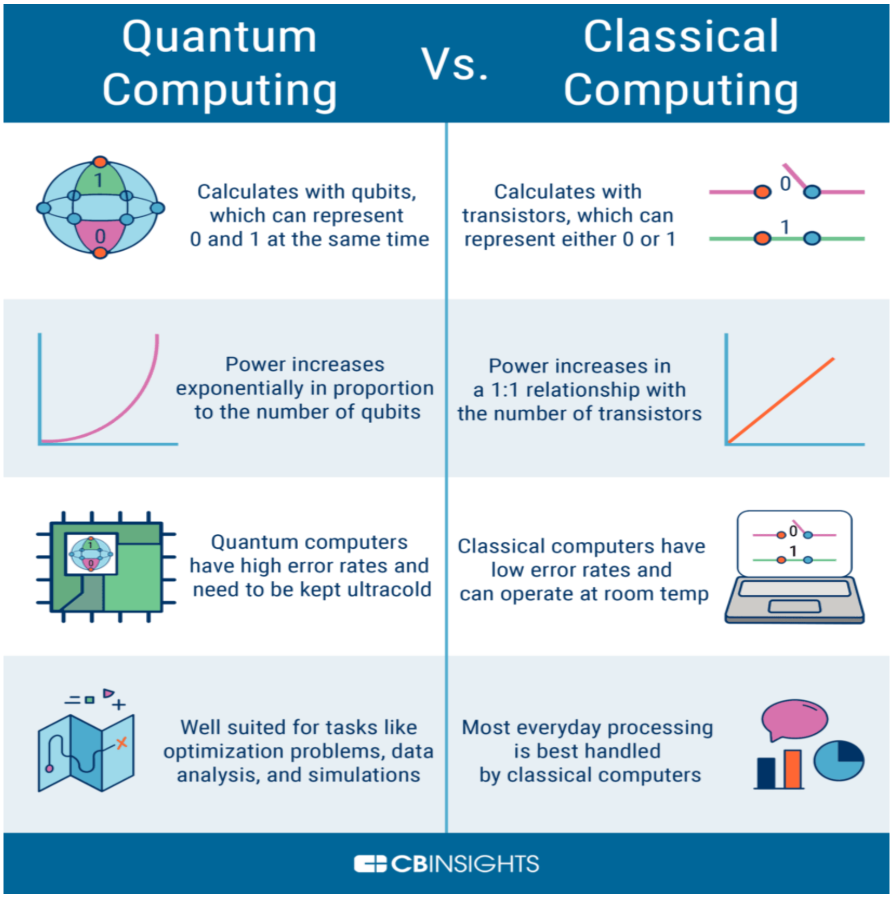


Image Source - https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/

History of Quantum Computers

"Nature isn't classical, dammit," Nobel Prize winner Richard Feynman protested 40 years ago, "and if you want to make a simulation of nature, you'd better make it quantum mechanical." This became a rallying cry for development of quantum computers, resulting in today's tremendous progress in the pursuit of quantum supremacy. Here's a brief history of quantum computing's development over the years.

- **1905** - Albert Einstein discusses the photoelectric effect, which states that exposing light on certain materials can cause electrons to be released, and proposes that light is made up of discrete quantum particles called photons.
- **1924** - Max Born coined the phrase quantum mechanics in a paper published by him.
- **1925** - **Matrix mechanics**, the first conceptually independent and logically consistent formulation of quantum mechanics, is proposed by Werner Heisenberg, Max Born, and Pascual Jordan.
- **1925 to 1927** - Niels Bohr and Werner Heisenberg develop the Copenhagen interpretation, one of the earliest interpretations of quantum mechanics which remains one of the most commonly taught.

- **1930** – ‘The Principles of Quantum Mechanics’ is published by Paul Dirac and has since become a classic reference book still in use today.
- **1935** - An article by Albert Einstein, Boris Podolsky, and Nathan Rosen highlights the surprising character of quantum superpositions and argues that quantum mechanics' account of physical reality is insufficient.
- **1935** - Erwin Schrödinger develops a theory in which a cat (forever known as Schrödinger's cat) is simultaneously dead and alive. Schrödinger discussed quantum superposition with Albert Einstein and criticizes the Copenhagen interpretation of quantum mechanics; Schrödinger also coined the term "quantum entanglement."
- **1947 -** In a letter to Max Born, Albert Einstein describes quantum entanglement for the first time as "spooky activity at a distance."
- **1976** - One of the first attempts at developing a quantum information theory is published by Roman Stanislaw Ingarden of the Nicolaus Copernicus University in Torun, Poland.
- **1980** - The Argonne National Laboratory's Paul Benioff releases a paper providing a quantum mechanical model of a Turing machine or a classical computer, the first to show that quantum computing is possible.
- **1981** - Richard Feynman of the California Institute of Technology argues in a keynote lecture titled Simulating Physics with Computers that a quantum computer has the ability to replicate physical processes that a classical computer cannot.
- **1985** - A quantum Turing machine is described by David Deutsch of the University of Oxford.
- **1992** - One of the first examples of a quantum algorithm that is exponentially faster than any deterministic classical algorithm is the Deutsch–Jozsa algorithm.
- **1993** - The concept of quantum teleportation is first described in a study.
- **1994** - Bell Laboratories' Peter Shor creates a quantum algorithm for factoring integers that has the potential to decrypt RSA-encrypted communications, a commonly used approach for data security.
- **1994** - The National Institute of Standards and Technology hosts the first government-sponsored quantum computing symposium in the United States.
- **1996** Bell Laboratories' Lov Grover creates the quantum database search algorithm.
- **1998** - The first evidence that a specific subclass of quantum calculations may be effectively mimicked using conventional computers; the first instance of quantum error correction.
- **1999** - University of Tokyo's Yasunobu Nakamura and Tokyo University of Science's Jaw-Shen Tsai show that a superconducting circuit may be utilized as a qubit.
- **2002** - The first edition of the Quantum Computation Roadmap is released, which is a live document incorporating prominent quantum computing experts.
- **2004** - Jian-Wei Pan's group at China's University of Science and Technology established the first five-photon entanglement.
- **2011** - D-Wave Systems offers the first commercially accessible quantum computer.
- **2012** - The first specialized quantum computing software business, 1QB Information Technologies (1QBit), is created.
- **2014** - Physicists at Delft University of Technology's Kavli Institute of Nanoscience transfer information between two quantum bits spaced by around 10 feet with a zero percent error rate.

- **2017** - The first quantum teleportation of independent single-photon qubits from a terrestrial observation to a low-Earth orbit satellite at a distance of up to 1400 km has been reported by Chinese researchers.
- **2018** - President Donald Trump signs the National Quantum Initiative Act, which establishes the objectives for a 10-year plan to support the growth of quantum computing science and technology applications in the US.
- **2019** - Google claims to have achieved quantum supremacy by completing a number of operations in 200 seconds which would take a supercomputer 10,000 years to complete; IBM counters that it could take 2.5 days rather than 10,000 years, showcasing techniques that a supercomputer could use to maximize computing speed.

Limitations of Classical Computing/Why Quantum Computers?

Gordon Moore, a co-founder of Intel, noticed in 1965 that the number of transistors for every square inch on a microchip had quadrupled every year since its inception, while the cost had been reduced by half. Moore's Law is the name given to this finding.

Moore's Law is crucial as it predicts that over time, computers will become smaller and faster. However, it is now slowing down – some suggest to a standstill even.

Transistors have continually gotten smaller in size over the last half decade as a result of chip innovation. Apple's recent computers, for example, use 5 nm transistors, which are roughly the same size as 16 oxygen molecules laid out side by side. However, as transistors begin to hit physical limits, Intel and other chipmakers have warned that transistor-based computing may be nearing a major roadblock.

If we want to continue to take advantage of fast expansion in computer capabilities, we'll have to discover a new means of processing data soon. This is where qubits come into the picture.

Our most sophisticated classical supercomputers are stumped by large instances of permutation and combination problems because:

1. Classical supercomputers lack the working memory to handle the countless combinations of real-world situations.

2. Classical supercomputers must assess each combination one by one, which takes a substantial amount of time.

How do quantum computers tackle such problems?

The computing capability of a quantum computer develops exponentially in proportion to the number of qubits in the system. In contrast, the power of a traditional computer increases in direct proportion to the number of transistors. This is one of the reasons why, in the future, quantum computers may be capable of performing operations far more effectively than conventional computers.

Consider an electron system in which the electrons can exist in any of 40 possible locations. As a result, the electrons can be in any of 2^{40} configurations (as each location can either have or not have an electron). To process the state of the electrons in a regular computer memory, more than 130 GB of memory would be required! This is significant, yet it is within the capabilities of some machines. There would be twice as many configurations (2^{41}) if we permitted the particles to be in any of 41 locations, requiring more than 260 GB of memory to hold the quantum state. If we want to save the state classically, we can't play this game of increasing the number of locations indefinitely since we quickly reach the memory capabilities of even the largest and most powerful machines. Because the memory required to store the system exceeds the number of particles in the universe at a few hundred electrons, we will never be able to mimic their quantum dynamics with classical computers. In nature, however, such systems evolve in time according to quantum mechanical laws, blissfully unconscious of the incapacity to engineer and replicate their evolution using ordinary computing power.

This observation prompted those who had foresight into quantum computing to raise a simple yet powerful question: can we turn this challenge into an opportunity? What would happen if we built hardware with quantum effects as fundamental operations, if quantum dynamics are difficult to simulate using classical technology? Could we use a system to model systems of interacting particles that uses the same laws that govern them in nature? Could we look into tasks that aren't found in nature but nonetheless follow or benefit from quantum mechanical laws? Quantum computing was born as a result of these inquiries.

Following are some additional problems which can be solved using Quantum computing

- Encryption that is virtually unbreakable? Quantum computers will alter the data security environment. Despite the fact that quantum computers will be capable of cracking many of today's encryption schemes, it is expected that they would develop hack-proof alternatives.
- Because quantum computers employ quantum tunnelling, rather than using more electricity, they can lower power usage by 100 to 1000 times.

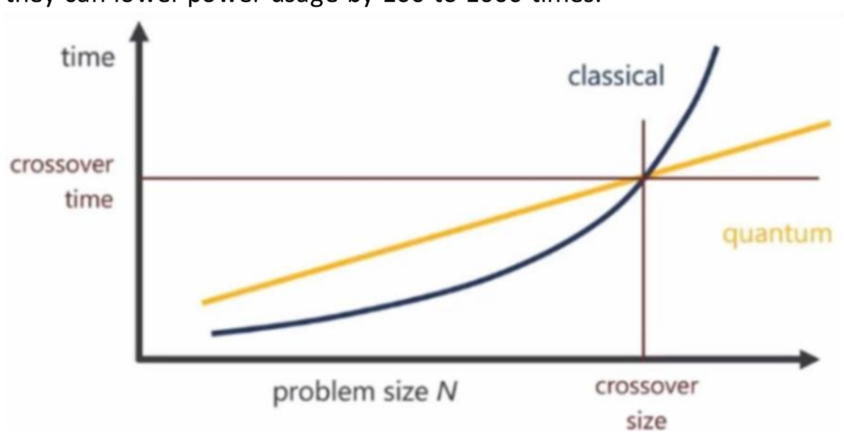


Image Source - https://www.forbes.com/sites/tomcoughlin/2021/09/28/quantum-computing-memory-and-storage/?sh=401885e154f6

Working of Quantum Computers

How do quantum computers work?

There are a few fundamental principles to know in order to comprehend how quantum computing works. We've included some basic explanations of them below:

Qubits - Traditional computers are constructed on bits. The basic units of information in computing are bits (short for binary digits), which may be measured in two different configurations. They can be regarded of as on or off, up or down, or as 0s or 1s when represented in binary. Quantum bits, also known as qubits, are the building blocks of quantum computers. Quantum-mechanical devices with two states can be used to create these qubits. For example, an electron's spin can be measured up or down, and a single photon can be polarized vertically or horizontally.

Quantum computers, in contrast to classical computers, execute calculations based on the likelihood of an object's state before it is measured, rather of only 1s or 0s, allowing them to process exponentially more data. Classical computers use the definite position of a physical state to perform logical operations. These are usually binary, which means that their operations are limited to one of two possibilities. A bit is a single state, such as on or off, up or down, 1 or 0.

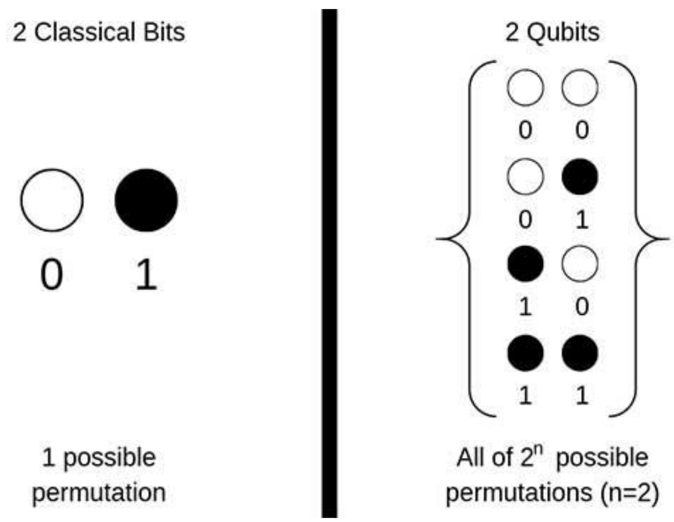


Image Source - https://www.dhyeyaias.com/current-affairs/perfect-7-magazine/quantum-supremacy

Superposition - Unlike standard computer bits, which can only be 0s or 1s, qubits can be 0s, 1s, or a combination of the two at the same time. A state of superposition is a phenomenon in which all possible combinations of information may exist at the same time. When qubits are merged, their capacity to retain all conceivable information configurations at the same time means that complicated problems may be addressed much more quickly than with standard computing approaches.

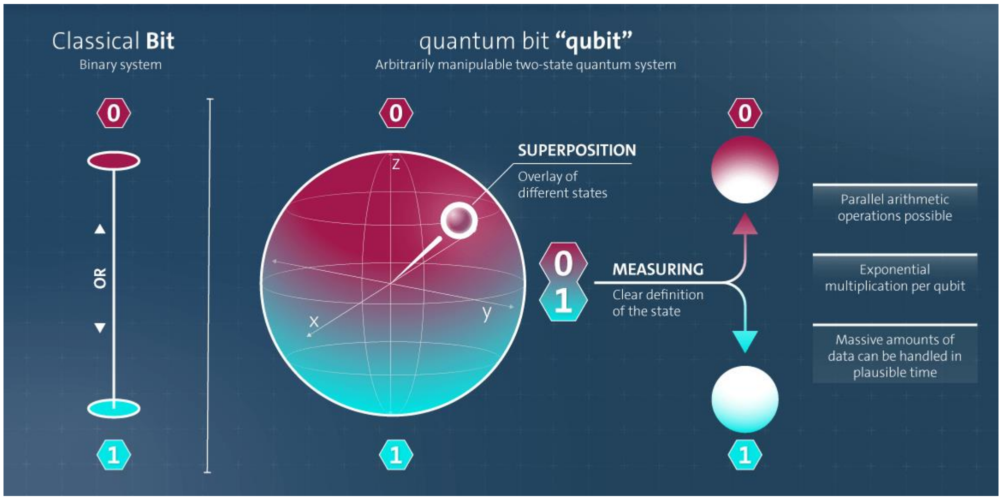


Image Source - https://devopedia.org/qubit

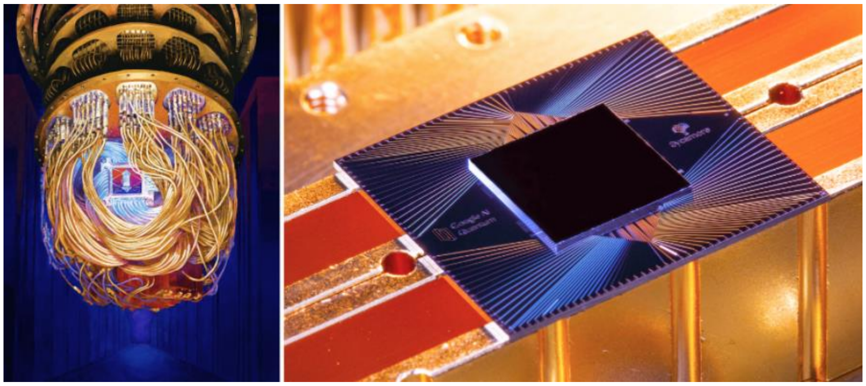
Entanglement - Entanglement, a quantum phenomena, is another important aspect of quantum computing. Simply put, this phenomenon causes two qubits to form a contactless correlation. For example, if the state of one entangled qubit changes, the state of the other entangled qubit will change as well. When two or more qubits are entangled, a change to one can effect the other.

Quantum Supremacy - Computational Power Breakthroughs

If data is the new oil, encryption is the digital economy's driving force. Cryptography protects everything including credit card transactions to health data stored on wearable gadgets. These sophisticated algorithms, in turn, make it easier to make safe use of the massive amounts of data created every day. The path to digitization appears to be obvious, but there are several speed bumps along the way. A group of Google researchers announced that they had achieved 'quantum supremacy,' a key milestone in computer science.

“Our machine performed the target computation in 200 seconds and from measurements in our experiment we determined that it would take the world’s fastest supercomputer 10,000 years to produce a similar output,” according to the release.

This was accomplished with the help of a 54-qubit processor called "Sycamore," which was built using high-fidelity quantum logic gates. A quantum computer can solve issues that are beyond the capabilities of today's supercomputers. However, it runs the danger of destroying existing encryption standards, bringing the digital economy's motor to a standstill.



The Sycamore processor as shown by an artist (left) and the real Sycamore processor (right).
Image Source - https://economictimes.indiatimes.com/magazines/panache/quantum-supremacy-and-the-threat-it-poses-to-data-storage-digital-economy/articleshow/71938704.cms

New cyber-security concerns and Their Solutions

End-to-end encryption, such as that used by WhatsApp, is deemed safe since it is impossible for hackers to decipher the coded message transferred from one user to another if it is intercepted. Even the most advanced computers in use would take hundreds of years to figure out the requisite cryptographic key if they attempted every conceivable combination – a method known as brute force attack.

If quantum computers become commonplace, cryptography's use cases would be jeopardized. In a few minutes, encryption employed in professional networks and Wi-Fi routers might be hacked. The security of email and messaging services would be jeopardized. Banking transactions might be hacked, putting consumers' financial information at risk. An encryption algorithm is a math problem involving very big numbers in its most basic form. Because encryption keys are made up of thousands of bits, it's tough to figure out the proper combination in real time. However, because the number of possible combinations is limited, these methods would not be infallible even if the computational capability to process all of them existed. The 256-bit version of the Advanced Encryption Standard (AES) – the standard used by WhatsApp – would, for example, encrypt the data into 2256-bit cypher text. It is quite unusual that one will have to browse through the entire list of options before finding the correct combination. Even if it were possible to crack the code after attempting 50% of the potential permutations, the time required would be excessive.

The Tianhe-2 (MilkyWay-2) supercomputer in China, widely considered one of the world's fastest, would take millions of years to crack 256-bit AES encryption. As anticipated by astrophysicists, this is longer than the universe's life span. However, how would cryptography be thrown on its head if the cosmos suddenly disintegrated into a cloud of dust in a matter of minutes? This might have a significant impact on how information is shared on the internet. In this case, the end of the cosmos is equivalent to achieving quantum supremacy. The binary system, in which each digit is encoded in 0s and 1s, is used by traditional computers.

Although Google has gained the lead in the quantum race, contemporary cryptography may be jeopardized if such machines fall into the hands of malicious actors or rogue nations. Businesses will need to come up with new ways to protect sensitive data, including data transferred across a network as well as data kept locally on hard drives.

Lattice-based Cryptography

Due to its structure in a virtual grid, lattice-based algorithms are hard to penetrate, unlike traditional encryption approaches now in use. The encryption key is buried at the place where a multidimensional lattice intersects. Quantum computers will be unable to make use of their advantage over conventional computers due to the unlimited number of permutations and the considerably more difficult process of skimming across the spectrum of possibilities.

Only if the attacker knows their way across the lattice can the cryptographic key be found, which is theoretically impossible because there is no mechanism to compute the path. Companies like SAFEcrypto and Privitar are presently offering this type of challenging encryption that might fool quantum computers. Despite the recent discovery, Google researchers are still orders of magnitude away from achieving the computing power required to crack such algorithms.

Scientists will need to add more qubits to the present architecture to make a credible threat. A 54-qubit processor was used in the Google Sycamore system that achieved quantum supremacy. Furthermore, the lack of common libraries for lattice algorithms complicates software integration with quantum technology.

Large corporations may want to explore employing lattice-based encryption services to secure vital data with a lengthy shelf life, despite the fact that they are expensive. The value of transactional data, which is generated in bulk every day, does not appear to necessitate that level of encryption, as it depreciates in value to hackers over time. The threat to national security, on the other hand, is more concerning.

Limitations of Quantum Computers

- They're challenging to construct. A functioning quantum computer, like IBM's Quantum System One, requires a highly particular set of circumstances to operate. To function even at a basic level, they require specialized components, enormous cooling systems, and pricey technology.
- They're prone to making mistakes. Environmental influences may quickly induce mistakes and cause qubits to lose their quantum state due to the nature of quantum mechanics and qubits (a process known as decoherence). Because these faults proliferate as complexity increases, a solution for error correction is required to realize their full potential.
- They're only good for particular jobs. Quantum computers, as we'll see, have the potential to provide innovative answers in a number of fields. However, because to the way they function, they are unlikely to provide benefits in many areas of computing.

Quantum Computers and Real-World Applications

We've highlighted a few existing and future quantum computing uses below:

Molecular modelling. Even with today's supercomputers, simulating atoms and molecules with any degree of precision is difficult. Quantum computing to imitate quantum physics might provide new information about how batteries work or how proteins interact, potentially revolutionizing energy storage and health.

Database searching. Quantum computers, because of the way they solve issues, might be utilized to store and sift through huge quantities of data considerably faster than ordinary computers.

Cryptography. Most present techniques of encryption might be broken by a fully functional quantum computer, which would be a major worry for cyber security. However, research towards quantum-proof cryptography is continuing. Quantum computing might be a key component of cyber and network security in the future.

Weather forecasting. To develop forecasts in the science of meteorology, large volumes of data and many distinct factors are required. Even supercomputers have difficulty accurately predicting the weather. Quantum computing has the potential to increase the level of detail of weather forecasting.

Typically, the first quantum algorithms introduced are for security, particularly quantum cryptography, such as implementing algorithms that can withstand threats posed by quantum computers – which the US National Institute of Standards and Technology (NIST) is on the verge of accomplishing through a project to standardize a Post Quantum Computer (PQC) encryption schema.

Quantum cryptography, as one of the first applications of quantum cybersecurity, offers both opportunities and risks to the cryptographic infrastructure. On the one hand, quantum computers can decode data that has been encrypted using traditional computing methods. It does, however, provide protected communication routes for the sharing of secret keys.

Quantum cryptography systems based on Quantum key distribution (QKD), for example, often use individual photons of light and make use of the fact that measuring a quantum system disrupts it and provides only partial information about its state prior to the measurement. Eavesdropping on a quantum communication channel, as a result, generates an inevitable disruption, causing genuine users to become aware. Quantum cryptography makes use of this phenomena to allow two people who have never met and have no prior knowledge of each other to communicate in complete secrecy under the watchful eye of an opponent. Quantum approaches also aid in fulfilment of more nuanced cryptographic goals, such as allowing two mutually suspicious persons to make joint judgments based on private information without compromising its secrecy as little as possible in the post-cold war environment.

In the quantum computing arena, corporate companies are also creating waves. Google, for example, is creating its own quantum computing hardware and has achieved numerous major milestones, including the first claims of quantum supremacy and the first quantum computer simulation of a chemical reaction. IonQ, ProteinQure, and Kuano are just a few of the Google-backed firms in the sector.

Another company developing quantum computing gear is IBM. It has already developed a number of quantum computers, but by 2023 it hopes to have built a 1,000-qubit machine. On the business side, IBM maintains the IBM Q Network, which provides access to quantum computers through the cloud and allows companies, such as Samsung and JPMorgan Chase, to experiment with possible applications for their organizations.

Meanwhile, businesses like IonQ and Rigetti have worked with Microsoft and Amazon to make quantum computers available on Azure and AWS, respectively. Both digital behemoths have also built development platforms aimed at assisting businesses in experimenting with technology.

What applications does quantum computing have in various industries?

Quantum computing will see a rapid spike in firms using it to their respective sectors as technology evolves and becomes more accessible. Some of these ramifications are already being seen in many industries.

The industries mentioned below, ranging from healthcare to agriculture to artificial intelligence, might be among the first to use quantum computing.

Quantum computing in healthcare

Quantum computers have the potential to change healthcare in a variety of ways. Google, for example, recently claimed that it has deployed a quantum computer to mimic a chemical interaction, marking a watershed moment in the field. Although the specific interaction was rather basic, and existing classical computers can model it as well, quantum computers are expected to be able to mimic complicated molecule interactions far more precisely than classical computers in the future. This might help speed up drug development efforts in the healthcare industry by making it easier to forecast the effects of therapeutic candidates.

Protein folding is another area where quantum computing might help with drug development. ProteinQure, a startup recognized by CB Insights in the AI 100 and Digital Health 150 cohorts for 2020, is already using contemporary quantum computers to help anticipate how proteins will fold in the body. For traditional computers, this is a notoriously tough process. However, addressing the problem using quantum computing might make creating potent protein-based treatments easier in the long run. Quantum computing might eventually lead to more customized medicine by enabling speedier genetic analysis to determine personalized treatment strategies unique to each patient.

Genome sequencing generates a lot of data, therefore interpreting a person's DNA takes a lot of processing power. Companies are already lowering the cost and resources required to sequence the human genome; but, a powerful quantum computer might filter through this data considerably faster, making genome sequencing more efficient and scalable.

Pharmaceutical businesses such as Merck and Biogen have collaborated with quantum computing startups.

Finance and quantum computing

Computational models that incorporate probability and assumptions about how markets and portfolios will perform are frequently used by financial analysts. Quantum computers might assist by processing through data faster, running better forecasting models, and balancing opposing alternatives more precisely. They might also assist in resolving complicated optimization problems such as portfolio risk optimization and fraud detection.

Monte Carlo simulations – a probability simulation used to analyze the impact of risk and uncertainty in financial forecasting models – are another area of finance where quantum computers might have an influence. Last year, IBM presented research on a strategy for gauging financial risk that employed quantum algorithms to outperform traditional Monte Carlo simulations.

RBS, the Commonwealth Bank of Australia, Goldman Sachs, Citigroup, and many other financial institutions have invested in quantum computing firms.

Quantum computing in cybersecurity

Quantum computing has the potential to disrupt cybersecurity. Quantum computers have the potential to break cryptography systems such as RSA encryption, which are currently employed to protect sensitive data and electronic communications. Shor's Algorithm, a quantum algorithm hypothesized in the 1990s by Peter Shor, a researcher at Nokia's quantum computing hub, Bell Laboratories, foreshadows this possibility. This method explains how a sufficiently strong quantum computer – which some predict will appear around 2030 – may determine the prime factors of huge numbers relatively rapidly, a task that classical computers struggle with. To safeguard data being sent over the internet, RSA encryption relies on this same difficulty.

However, multiple quantum computing firms are forming to combat this danger by inventing new encryption methods known as "post-quantum cryptography." These approaches are created to be more resistant to quantum computers, frequently by posing a challenge that even the most powerful quantum computer is unlikely to be able to answer. Isara and Post Quantum are two companies in the space, among many more. The National Institute of Standards and Technology (NIST) in the United States supports the concept and plans to adopt a post-quantum cryptography standard by 2022.

Quantum key distribution (QKD), a developing quantum information technique, may provide some relief from quantum computers' code-breaking ability. Encryption keys are transferred via entangled qubits in QKD. It's possible to detect if an eavesdropper has intercepted a QKD communication since quantum systems are affected when measured. If done correctly, even quantum computer-equipped hackers would have a difficult time stealing data.

Blockchain and cryptocurrency quantum computing

The danger of quantum computing to encryption extends to blockchain technology and cryptocurrencies such as Bitcoin and Ethereum, which use quantum-susceptible encryption algorithms to complete transactions.

Though quantum risks to blockchain-based applications differ, the consequences might be disastrous. According to a Deloitte investigation, around 25% of bitcoins (now worth $173 billion) are kept in such a way that they might be readily stolen by a quantum computer-equipped burglar. Another concern is that quantum computers will one day grow strong enough to decode and meddle with transactions before they are validated by other network members, jeopardizing the decentralized system's integrity. That's only for Bitcoin. Blockchain technology is increasingly being utilized in asset trading, supply networks, identity management, and many other areas.

A lot of stakeholders are working to make blockchain technology safer, alarmed by the serious hazards posed by quantum computers. Established networks like Bitcoin and Etherum are experimenting with quantum-resistant approaches for future iterations; a new blockchain protocol called the Quantum Resistant Ledger was created specifically to counter quantum computers, and startups like QuSecure and Qaisec say they're working on quantum-resistant blockchain tech for businesses.

Quantum-resistant blockchains may not completely develop in the next years as post-quantum cryptographic standards become more firmly defined. In the meantime, people in charge of blockchain initiatives will be watching quantum computing developments anxiously.

Quantum computing in artificial intelligence

The ability of quantum computers to filter through large data sets, simulate complicated models, and solve optimization issues efficiently has sparked interest in artificial intelligence applications. Google, for example, says it's working on machine learning tools that integrate classical and quantum computing, and that it expects these techniques to function with quantum computers before long. In a recent statement, quantum software firm Zapata indicated that quantum machine learning is one of the highest potential commercial uses for quantum computers in the near future. Though quantum-assisted machine learning may soon provide some economic benefits, quantum computers in the future might push AI considerably further.

Quantum computing-based AI might improve computer vision, pattern recognition, speech recognition, machine translation, and other technologies.

Quantum computing may eventually aid in development of AI systems that behave more human-like. Allowing robots to make better judgments in real time and adapt more rapidly to changing conditions or new scenarios, for example.

Logistics and quantum computing

Quantum computers excel at optimizing things. A complicated optimization issue which would take a classical supercomputer thousands of years to complete may theoretically be solved in minutes by a quantum computer. Quantum computing might be well-positioned to assist in handling tough logistical issues, given the tremendous complexity and unpredictability involved in international shipping routes and coordinating supply chains.

Quantum computers are already being considered by DHL, a leading global logistics company, to aid in more effective packing of shipments and optimization of worldwide delivery routes. The business hopes to improve service speed all while making it simpler to adjust to changes like cancelled orders or postponed delivery.

Others aim to use quantum computers to improve traffic flow, a technology that may allow delivery vans to reach more destinations in less time.

Manufacturing and industrial design using quantum computing

Big players interested in manufacturing and industrial design are also interested in quantum computing. For example, in 2015, Airbus, a multinational aerospace company, launched a quantum computing unit and funded quantum software startup QC Ware and quantum computer manufacturer IonQ.

Quantum annealing for digital modelling and materials sciences is one of the areas the organization is looking into. For example, a quantum computer may assist discovery of the most efficient wing design for an aero plane by filtering through innumerable factors in only a few hours.

Manufacturing has also been recognized as a potential market for IBM's quantum computers, with fields such as materials science, improved analytics for control operations, and risk modelling highlighted as significant applications.

Agriculture and quantum computing

Quantum computers might aid agriculture by making fertilizer production more efficient. Ammonia is utilized in nearly all fertilizers used in agriculture across the world. Fertilizers would be cheaper and less energy-intensive if ammonia (or a substitute) could be produced more effectively. As a result, improved access to better fertilizers may be able to assist in feeding the world's rising population. According to CB Insights' Industry Analyst Consensus, ammonia is in great demand and will be a $77 billion worldwide market by 2025.

Because the number of conceivable catalyst combinations that may help us manufacture or replace ammonia is extraordinarily huge, little recent progress has been made on enhancing the process – meaning we effectively still rely on an energy-intensive approach from the 1900s known as the Haber-Bosch Process. Identifying the ideal catalytic combinations to generate ammonia with today's supercomputers would take centuries.

A powerful quantum computer, on the other hand, might be used to examine alternative catalyst combinations much more effectively – another use of modelling chemical processes – and aid in the discovery of a better way to manufacture ammonia.

Furthermore, we know that bacteria in plant roots use a chemical called nitrogenase to produce ammonia every day at a very inexpensive energy cost. This molecule is beyond our finest supercomputers' ability to mimic and so better comprehend, but a future quantum computer may be able to do so.

National security and quantum computing

Governments across the world are pouring money into quantum computer research, ostensibly to increase national security. Quantum computers might be used for a variety of defense applications, including code cracking for espionage, performing war simulations, and developing better materials for military vehicles, to name a few. For example, the US government stated earlier this year that it will invest about $625 million in quantum technology research institutions sponsored by the Department of Energy, with Microsoft, IBM, and Lockheed Martin contributing a total of $340 million to the programme.

Similarly, China's government has invested billions of dollars on a variety of quantum technology initiatives, and a Chinese team recently claimed to have made a quantum computer breakthrough.

Though it is unclear when quantum computing will play a significant role in national security, there is little doubt that no government wants to fall behind its competitors' capabilities. Already, a new "weapons race" has begun.

Quantum Data Center Transformations

Quantum computing on a large scale for data centers

Quantum computers deployed at scale in data center infrastructures will change data center design in terms of networking and security, resulting in creation of the quantum network and quantum security.

Quantum networking will achieve the ability to interact directly with quantum computers' vast computational power and enable information flow while remaining within the quantum domain. Data teleportation and entanglement, for example, would enable highly scalable and energy-efficient networking while still ensuring data security at each physical layer via quantum encryption. These designs will transform data centers not just in terms of processing capability, but also in terms of enabling use cases that aren't achievable in the traditional arena, allowing for vast computational, storage, and information sharing capabilities.

It's important to note that the quantum internet will not replace the classical internet – even Local Operations and Classical Communication (LOCC) operations depend on classical communications – but rather will coexist with it to create a new hybrid internet. This bright future brings with it some significant obstacles, as well as new standardizations and alignments between classical and quantum internet standards, which will fuel efforts and new definitions in the coming decades. It's vital to start planning now so that you're ready when these technologies become widely available.

Making quantum computing a reality in data centers

Quantum computing for data centers is thought to be ten years distant, according to industry consensus. While some claim it will be ready in three years, this is a highly sophisticated technology that will need time to evolve. "The future is already here – it's just not evenly distributed," science fiction novelist William Gibson once quipped. While quantum computing is still a few years away, businesses should begin planning for it now since it is no longer a question of if, but when we will use it.

Making a plan for the company and identifying the major areas where quantum computing might be used will help shape the roadmap for new quantum-enabled infrastructure and future goods. It's never too early to start thinking about how quantum computing may be used in organizations. Set up a dedicated team that investigates and creates concepts on a regular basis to assist movement of the technology to commercial use cases.

One of the most ignored, if not the most crucial, elements of the quantum stack is the conversion of classical data into quantum data. By ignored, we mean that investors aren't paying enough attention to it. Sure, qubit quality and the Quantum Processing Unit are critical, but ignoring the control hardware that regulates those qubits is akin to ignoring the gearbox of a car and focusing solely on the engine.

To construct the world's first Quantum Data Center, we first should understand why control systems are so critical.

Quantum Control Systems

The illustration below shows that the quantum processor, or QPU for short, is housed in its own enclosure box. And there's a complete rack of old modules in a different enclosure or rack. In many respects, this rack is as crucial as the QPU itself because it houses the QPU's control mechanisms. This behemoth of a system is responsible for converting traditional data into quantum data and vice versa. You'll have a hard time connecting your quantum computer to an ethernet port without it.

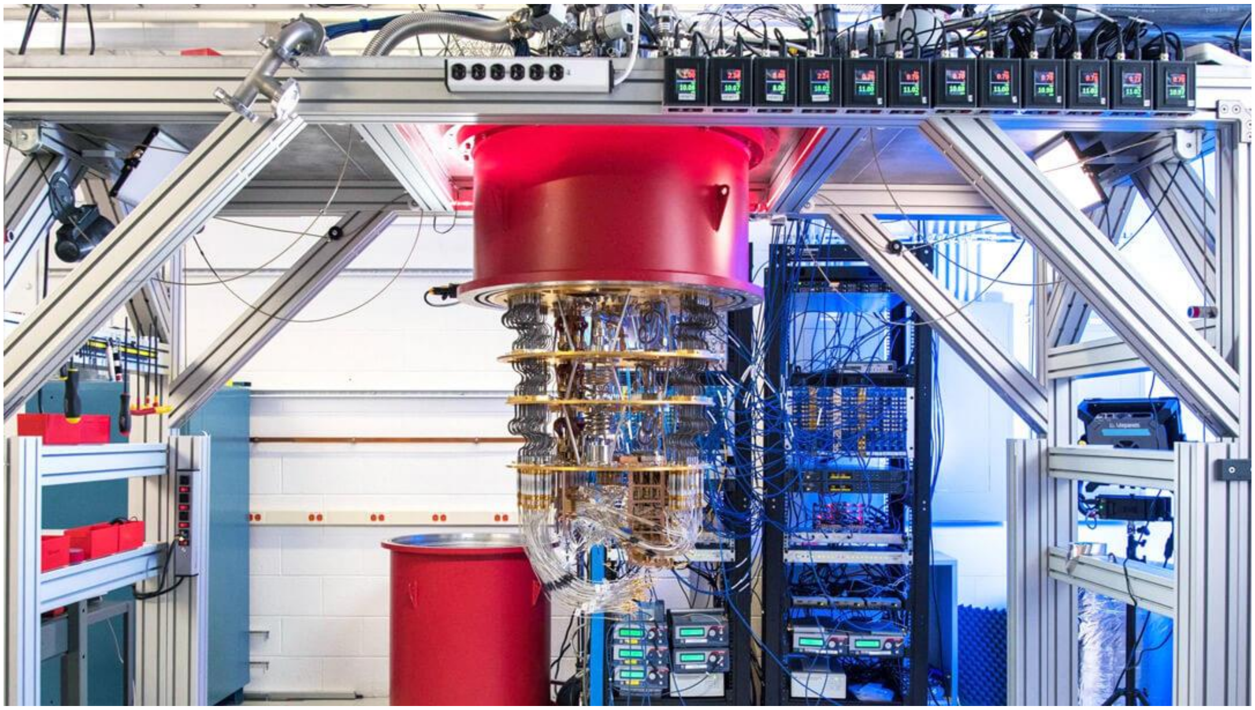


Image Source - https://quantumai.google/

We need to create new ASICs that are specifically designed for transmission and reception quantum information, as well as new control algorithms to decrease disturbances in magnetic fields, external disturbances, optical noise, and other factors.

This rack is also required so that the remainder of your datacenter can communicate with a quantum computer.

Quantum computing should be simple to implement

As control hardware is gradually becoming standardized, the software layer that specifies the device's interface is all that remains. In essence, a "Docker Container" of sorts is required, which allows any user to connect to any Quantum Device on the ARTIQ SINARA platform. It is possible for the Quantum Device to be physically located in the data center or to be located remotely. All the user has to do is provide the device's IP address, and you've got yourself a Quantum Data Center at your fingertips.

It Should Be Intuitive to Write Quantum Applications

Users who want to use this machine for algorithms should only be concerned with how effectively their algorithms are designed, not whether parts of the algorithm are executed on quantum vs. conventional devices. Another significant problem in today's Noisy Intermediate Scale Quantum Computing (NISQ) era is that users of quantum computers must optimize their algorithms to ensure that the instructions are delivered appropriately to the appropriate hardware. Even in Hybrid Quantum Classical Regimes, this results in a poor user experience and a significant barrier of entry. Quantum algorithms must be simple to write and deploy so that users can quickly embrace them.

Finally, businesses must decide how to gain access to and integrate with strategic resources via a cloud-enabled link to a quantum-enabled data center. To fully leverage the potential benefits, cybersecurity, low latency, and high-speed/high-capacity connections will be needed, as well as a new software layer and application. While quantum computing may be a decade away, planning forward and preparing for future data centers will be critical if we are to fully reap the potential of the technology.

Conclusion

Quantum computing has a great deal of promise.

Quantum computing is still very much in its early stages. As we've seen, technology is still in its infancy and difficult to master, with many unknowns. However, quantum computers' present and future use may alter our perceptions of the universe.

Quantum computing is indeed disrupting sectors, despite remaining a mystery to many. This technology will only grow more powerful and accessible as leading firms continue to develop, opening the path for unforeseen advantages. Quantum computing is the next great step in the data-driven revolution. While the future of this technology is yet unknown, these businesses are the most likely to usher it in.

The race to demonstrate a viable quantum gadget that can solve a problem that no conventional computer can solve in any reasonable length of time is on. The leap to the next generation of computing has always been measured in terms of speed – and long-term viability.

Quantum computers offer a lot of possibilities, from precise models and simulations to substantially quicker problem solutions. However, it remains to be seen whether we will be able to completely achieve that promise. Because companies like Google and IBM are significantly involved in the technology, we expect to see more improvements and creation of multiple Quantum Data centers in the future, if nothing else.

References

- 15 Things Everyone Should Know About Quantum Computing – [Bernard Marr]
- What is quantum computing? Essential concepts and uses – [FutureLearn]
- Introduction to Quantum Computing Online Class – [LinkedIn]
- IBM | What is Quantum Computing? – [Chris Fisher]
- Quantum computing - Wikipedia – [Wikipedia]
- Quantum Computing Memory And Storage – [Tom Coughlin]
- 'Quantum supremacy' and the threat it poses to data storage, digital economy – [Rohan Abraham]
- What Is Quantum Computing? Definition, Industry Trends & Benefits Explained – [CB Insights Research]
- Optical Quantum Memory and its Applications in Quantum Communication Systems – [Lijun Ma, Oliver Slattery, and Xiao Tang]
- Quantum Computing Threat – PQSecure Technologies – [Pqsecurity.com]
- What to Expect as the Era of Data Center Quantum Computing Nears – [Domenico Di Mola]
- The Quantum DataCenter — What it is and Why We're Building It. – [Dominik Andrzejczuk]
- Quantum computing history and background - Azure Quantum – [Docs.microsoft.com]
- 27 Milestones In The History Of Quantum Computing – [Gil Press]
- Top Quantum Computing Companies for 2022 | CIO Insight – [Devin Partida]
- How Do Quantum Computers Work? – [ScienceAlert]
- The Map of Quantum Computing | Quantum Computers Explained – [DoS - Domain of Science]