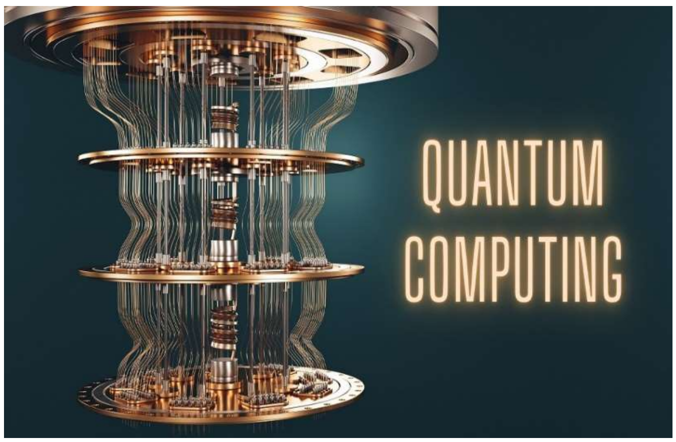
QUANTUM COMPUTING

Quantum computing is a multidisciplinary field comprising aspects of computer science, physics, and mathematics that utilizes quantum mechanics to solve complex problems faster than on classical computers. The field of quantum computing includes hardware research and application development. Quantum computers are able to solve certain types of problems faster than classical computers by taking advantage of quantum mechanical effects, such as superposition and quantum interference.



HISTORY OF QUANTUM COMPUTING :

Quantum computers were first proposed in the 1980s by Richard Feynman and Yuri Manin. The intuition behind quantum computing stemmed from what was often seen as one of the greatest embarrassments of physics: remarkable scientific progress faced with an inability to model even simple systems. Quantum mechanics was developed between 1900 and 1925 and it remains the cornerstone on which chemistry, condensed matter physics, and technologies ranging from computer chips to LED lighting ultimately rests. Yet despite these successes, even some of the simplest systems seemed to be beyond the human ability to model with quantum mechanics. This is because simulating systems of even a few dozen interacting particles requires more computing power than any conventional computer can provide over thousands of years!

In 1980, Paul Benioff introduced the quantum turning machine, which uses quantum theory to describe a simplified computer. When digital computers became faster, physicists faced a exponential increase in overhead when stimulating quantum dynamics prompting Yuri Manin and Richard Feynman to independently suggest that hardware based on quantum phenomena might be more efficient for computer simulation. In a 1984 paper, Charles

Bennett and Gilles Brassard applied quantum theory to cryptography protocols and demonstrated that quantum key distribution could enhance information security.

Quantum algorithms then emerged for solving oracle problems, such as Deutsch's algorithm in 1985,[15] the Bernstein–Vazirani algorithm in 1993,[16] and Simon's algorithm in 1994.[17] These algorithms did not solve practical problems, but demonstrated mathematically that one could gain more information by querying a black box with a quantum state in superposition, sometimes referred to as *quantum parallelism*.[18] Peter Shor built on these results with his 1994 algorithms for breaking the widely used RSA and Diffie–Hellman encryption protocols,[19] which drew significant attention to the field of quantum computing.[20] In 1996, Grover's algorithm established a quantum speedup for the widely applicable unstructured search problem.[21][22] The same year, Seth Lloyd proved that quantum computers could simulate quantum systems without the exponential overhead present in classical simulations,[23] validating Feynman's 1982 conjecture.

Over the years, experimentalists have constructed small-scale quantum computers using trapped ions and superconductors. In 1998, a two-qubit quantum computer demonstrated the feasibility of the technology,[26][27] and subsequent experiments have increased the number of qubits and reduced error rates.[25] In 2019, Google AI and NASA announced that they had achieved quantum supremacy with a 54-qubit machine, performing a computation that is impossible for any classical computer.

WHY QUANTUM COMPUTING ?

Deutsch invented the idea of the quantum computer in the 1970s as a way to experimentally test the "Many Universes Theory" of quantum physics the idea that when a particle changes, it changes into all possible forms, across multiple universes.

UNLOCKING THE POWER OF QUANTUM COMPUTING

Quantum Computing uses the laws of quantum mechanics to solve complex problems efficiently due to its phenomenal processing power. This ability to process information faster opens disruptive possibilities in fundamental research and optimization for automotive, aerospace, and pharmaceutical industries among others. As the quantum industry continues to grow at an unprecedented pace, businesses must understand the roadmap to investment and commercialization to capitalize on this emerging technology.

Advancements in quantum error correction techniques and fault-tolerant quantum computing pave the way for more reliable and scalable quantum processors with higher qubits and quantum gate fidelity. Such innovations have resulted in investments of over $40 billion from corporations and governments into Quantum. The market for quantum enabled applications is projected to grow by 36.89 from 2023 to 2030 and reach $123bn, as quantum clearly emerges as the next in-line-tech.

PRINCIPLES OF QUANTUM COMPUTING:

Qubits

To implement a computational model as a physical device, the computer must be able to adept different internal states, provide means to perform the necessary transformations on them and to extract the output information. The correlation between the physical and the logical state of the machine is arbitrary (as long it is consistent with the desired transformations) and requires interpretation.

In an ordinary RAM module, the common quantum state of thousands of electrons is interpreted as only one bit. The logical state is determined by the expectation value of its register contents (e.g. tension of a capacitor) The interpretation as (classical) bits is performed by comparing the measured value to a defined threshold, while the great number of particles guarantees that the uncertainty of the measurement is small enough ($O(1/\sqrt{n})$) to make errors practically impossible.

In a quantum computer, information is represented directly as the common quantum state of many subsystems. Each subsystem is described by a combination of two ``pure'' states interpreted as $|0\rangle$ and $|1\rangle$ (quantum bit, qubit). This can e.g., be realised by the spin of a particle, the polarisation of a photon or by the ground state and an excited state of an ion.

Entanglement of States

Due to the one-to-one relation between logical and physical state in a quantum computer, a quantum register containing more than one qubit can not be described by simply listing the states of each qubit. In fact, the ``state of a qubit'' becomes a meaningless term

Given an isolated system of two qubits, its state can be described by four complex amplitudes $a|0,0\rangle + b|1,0\rangle + c|0,1\rangle + d|1,1\rangle$. You can define the expectation value for the first qubit, which is $\sqrt{bb^* + dd^*}$ but there is no isolated state for the first qubit anymore like e.g. $(a+c)|0\rangle + (b+d)|1\rangle$ since $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$ does not implicate that $|a+c|^2 + |b+d|^2 = 1$.

Therefore, manipulations on a single qubit effect the complex amplitudes of the overall state and have a global character. To describe the combined state $|\psi\rangle$ of n entangled qubits, 2^n complex numbers are necessary.

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i\,|i\rangle \quad \text{with} \quad \sum_{i=0}^{2^n-1} c_i^* c_i = 1 \quad \text{and} \quad c_i \in \mathbf{C}$$

Reversibility

To keep the computation coherent, quantum registers must be kept isolated, to avoid entanglement with the environment. The entropy of such a system has to remain constant since no heat dissipation is possible, therefore state changes have to be adiabatic, which requires all computations to be reversible.

Every reversible operation can be described by a *unitary* operator U which matches the condition $U^{-1} = U^\dagger$. Compositions of unitary operators are also unitary since $(UV)^{-1} = V^\dagger U^\dagger$. The restriction to unitary operators can also be directly derived for the operator of temporal propagation $U = e^{-iHt/\hbar}$. Since the Hamilton operator H is an observable it has only real eigenvalues and $({}^\dagger U) = U^{-1} = e^{iHt/\hbar}$.

A general unitary transformation in the two-dimensional Hilbert space $\mathbf{C}^2$ can be defined as follows:

$$U(\theta,\delta,\sigma,\tau) = \begin{pmatrix} e^{i(\delta+\sigma+\tau)}\cos\frac{\theta}{2} & e^{-i(\delta+\sigma-\tau)}\sin\frac{\theta}{2} \\ -e^{i(\delta-\sigma+\tau)}\sin\frac{\theta}{2} & e^{i(\delta-\sigma-\tau)}\cos\frac{\theta}{2} \end{pmatrix} \quad \text{with} \quad \theta,\delta,\sigma,\tau \in \qquad (1.5)$$

If this operator can be applied to arbitrary 2-dimensional subspaces of $\mathcal{H}$, then any unitary transformation can be constructed by composition. If only subspaces corresponding to a subset of qubits are allowed, which is the case for many proposed architectures, among them also the linear ion trap (*Cirac-Zoller gate*), then an additional 4-dimensional 2-qubit operator is needed to obtain a mixing between separate qubits .

One possibility for this operator is the 2-qubit XOR which is defined as $XOR : |x, y\rangle \rightarrow |x, x \oplus y\rangle$ or in matrix notation:

$$XOR = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

A quantum computer which is capable of performing general single qubit and XOR operations can therefore perform any possible operation and is in this sense universal.

Initialisation

To set a quantum computer to the desired input state $|\psi\rangle$, it suffices to provide means to initially ``cool'' all qubits to $|0\rangle$ and then apply a unitary transformation U which matches the condition $U|0\rangle = |\psi\rangle$. One might think of U as a base transformation which trivially exists for any desired $|\psi\rangle$.

Measuring States

Measuring n qubits reduce the dimensionality of $\mathcal{H}$ by a factor of 2^n. The outcome of the measurement is biased by the probability amplitude for a certain bit configuration. Consider two quantum registers with n and m qubits in the state

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^m-1} c_{i,j}|i,j\rangle \quad \text{with} \quad \sum_{i,j} c_{i,j}^* c_{i,j} = 1$$

The base-vectors $|i, j\rangle$ are interpreted as a pair of binary numbers with $i < 2^n$ and $j < 2^m$. The probability $p(I)$ to measure the number I in the first register and the according post measurement state $|\psi_I'\rangle$ are given by

$$p(I) = \sum_{j=0}^{2^m-1} c^*_{I,j} c_{I,j}, \quad \text{and} \quad |\psi'_I\rangle = \frac{1}{\sqrt{p(I)}} \sum_{j=0}^{2^m-1} c_{I,j} |I, j\rangle$$

BACKGROUND INFORMATION ON CLASSICAL COMPUTING LIMITATIONS:

Quantum computers typically must operate under more regulated physical conditions than classical computers because of quantum mechanics. Classical computers have less compute power than quantum computers and cannot scale as easily. They also use different units of data -- classical computers use bits and quantum computers use qubits.

Units of data: Bits and bytes vs. qubits

Classical computers use bits -- eight units of bits is referred to as one byte -- as their basic unit of data. Classical computers write code in a binary manner as a 1 or a 0. Simply put, these 1s and 0s indicate the state of on or off, respectively. They can also indicate true or false or yes or no, for example.

This is also known as serial processing, which is successive in nature, meaning one operation must complete before another one follows. Lots of computing systems use parallel processing, an expansion of classical processing, which can perform simultaneous computing tasks. Classical computers also return one result because bits of 1s and 0s are repeatable due to their binary nature.

Power of classical vs. quantum computers

Most classical computers operate on Boolean logic and algebra, and power increases linearly with the number of transistors in the system -- the 1s and 0s. The direct relationship means in a classical computer, power increases 1:1 in tandem with the transistors in the system. Because quantum computers' qubits can represent a 1 and 0 at the same time, a quantum computer's power increases exponentially in relation to the number of qubits. Because of superposition, the number of computations a quantum computer could take is 2^N where N is the no of qubits.

ADVANTAGES OF QUANTUM COMPUTING :

The advantages od quantum computing are as follows :-

1. Fastest Calculations: A quantum computer is capable of solving problems faster than other computers. For instance, it can solve highly complicated mathematical problems in a matter of seconds that would take a classical computer thousands of years to do. This is what is meant by the term quantum speed-up. Because of this speed-up, quantum computers have made it possible to break some of the most complex encryption codes.

2. Storing and Retrieving Data: A quantum computer can store, retrieve, and process large amounts of information in a fraction of the time needed by digital computers. It is possible to do this because a quantum computer deals with qubits instead of bits. There is another advantage of storing information in a quantum computer. It is that information cannot be altered or hacked by anybody. This is because a quantum computer uses the phenomenon of superposition to interrelate the two states, which makes it impossible for an unauthorized third party to know exactly how the states are related. It is also processed with huge and complex amounts of data. This makes it possible for a quantum computer to simulate millions of molecules and atoms before it is needed.

3. **They Can Solve Complex Problems:** A quantum computer is a faster and more powerful technology than any other conventional computer. To use a classical computer to solve a problem, it is necessary to break it down into many different parts. Though this makes it possible to solve the problem, it requires more time than is necessary. By using quantum computers, complex problems can be solved instantly and in a few steps. The harder a problem is to solve, even for a supercomputer, the more complicated it is. When a classic computer fails, it’s usually because it’s very complicated and has a lot of parts that interact with each other. But because of the ideas of superposition and entanglement, quantum computers can figure out a solution that takes into account all of these variables and complexities.

4. Faster Computations: A quantum computer can perform faster calculations than a classical computer. This is because they are able to process data in parallel and do it much more efficiently. They also need less time to do computations than classical computers, making them significantly faster.

5. Google Search: Quantum computers also use google search for searching information. Quantum computers can make complex calculations much faster than any other conventional computer. This is because they use the effects of quantum superposition to perform these calculations. One of the examples is Google asking NASA to develop a quantum computer.

6. New Technologies: A quantum computer is a new technology with various features that are yet to be explored in its development. Quantum computers have the potential to make the world significantly more efficient, secure, and energy-efficient than ever before.

7. HIGH PRIVACY: A Quantum computer is highly confidential and secure. It uses the phenomenon of superposition to form the supercomputer that makes hacking impossible. They are also ideal for storing and managing passwords and cryptographic keys without fear of being hacked or intercepted by hackers.

8. THEY CAN RUN COMPLEX SIMULATIONS: Because of their high computational power and the speed of their operations, quantum computers can simulate things that are too complex for today's computers. They can even simulate a bunch of atoms or molecules in order to determine how they will react with other substances.

Due to the speed and complexity of quantum computing, a quantum computer could, in theory, simulate many complex systems and help us figure out some of life's biggest mysteries.

DISADVATAGES OF QUANTUM COMPUTING

Quantum computing is a complicated and controversial technology that has the potential to revolutionize computing in the future. Quantum computers are systems that will allow for extraordinarily powerful computations. There are disadvantages of quantum computing such as follows:

1. ALGORITHM CREATION: It has to write a new algorithm for each type of computation. Quantum computers can't work like traditional computers, they need special algorithms to do tasks in their environment. The problem that quantum computers will solve is the problem of algorithm creation.The algorithms of quantum computers are strange and often in contrast to the logic of classical computing. A classical computer has a processor, memory, and software. There are no such things in quantum computing.

2. THE LOW TEMPERATURE NEEDED: Quantum computers require extreme temperatures that are hard to keep. It can't be isolated from its environment because it has to interact with the environment. If it interacts with the environment, it will lose its quantum nature. This is why quantum computers need to operate at incredibly low temperatures. Since there is a lot of processing going on in these computers, they need to be at a temperature of -460°F. This is the coldest place in the universe, and it is very hard to keep it this way.

3. NOT OPEN TO PUBLIC: Quantum computers are not open for public use. As of now, they are not available commercially. Even if they were, no one would be able to use them because there is no software or algorithms to run on them. They can't be used by the public because they cost too much. Also, these types of computers make a lot of mistakes because they are still being developed. When there are 10 qubits, quantum computers work fine, but when there are more qubits, like 70 qubits, the accuracy isn't right. There are already tests being done to make sure that the results from these computers are accurate.

4. Internet Security: The internet is the main way that we send and receive information. Quantum computers will take over the security of the internet and this could destroy the world. If the internet shuts down, so does our economy. No one will be able to get any money or food. Scientists think that if a quantum computer is built in the best way, it will break the security of the whole internet. This is because all the codes on the internet can be broken by these computers.

5. Heating Problems: Quantum computers are very fragile, and they break easily because of their environment. The smallest amount of heat can destroy the computer, and this is an issue. When the information is saved and retrieved, it needs to be very accurate. If there is any change in the information, it needs to be rewritten because it won't work with the same software.

6. They are difficult to build: It is difficult to build a quantum computer because the researchers need to find a way to get the qubits accurate. Quantum computers cannot be run on traditional computers. Software, algorithms, and programmers are needed to work with these computers. There is a lot of work that needs to be done for the computer to run correctly.

7. Low Precision: Quantum computers have a low level of precision. Scientists have to create their own qubits, which is difficult. They are hard to find and even harder to control. Also, they have to be stable because if they aren't stable, the computer will constantly shut down or malfunction.

8. They are high-maintenance: Quantum computers are very expensive to maintain. They have to be monitored constantly because they can easily break. They have to be programmed, and when they start, they may not work at all.

SOME TOPICS OF QUANTUM COMPUTING

- ***QUANTUM PARALLELISM:***

  Quantum parallelism is a concept that lies at the heart of quantum computing. It refers to the ability of quantum systems to perform multiple calculations simultaneously, thereby enabling a tremendous speed-up over classical computing. This speed-up is achieved through the use of quantum superposition, which allows quantum bits (or "qubits") to exist in a superposition of states, rather than just the two states of classical bits (0 or 1).

- ***QUANTUM SUPERPOSITION:***

  Quantum superposition is a fundamental principle of quantum mechanics. In classical mechanics, things like position or momentum are always well-defined. We may not know what they are at any given time, but that is an issue of our understanding and not the physical system. In quantum mechanics, a particle can be in a superposition of different states. However, a measurement always finds it in one state, but before and after the measurement, it interacts in ways that can only be explained by having a superposition of different states.

- ## ***SHOR'S ALGORITHM:***

Shor's algorithm is a quantum computer algorithm for finding the prime factor of an integer. It was developed in 1994 by the American mathematician Peter Shor. On a quantum computer, to factor an integer , Shor's algorithm runs in polylogarithmic time meaning the time taken is polynomial in , the size of the integer given as input. Specifically, it takes quantum gates of order using fast multiplication, or even utilizing the asymptotically fastest multiplication algorithm currently known due to Harvey and Van Der Hoven, thus demonstrating that the integer factorization problem can be efficiently solved on a quantum computer and is consequently in the complexity class BQP.

GROVER'S ALGORITHM:

Classically, searching an unsorted database requires a linear search which is *O(N)* in time. Grover's algorithm, which takes *O(N1/2)* time, is the fastest possible quantum algorithm for searching an unsorted database. It provides "only" a quadratic speedup, unlike other quantum algorithms, which can provide exponential speedup over their classical counterparts. However, even quadratic speedup is considerable when *N* is large. Like all quantum computer algorithms, Grover's algorithm is probabilistic, in the sense that it gives the correct answer with high probability. The probability of failure can be decreased by repeating the algorithm.

- ## ***QUANTUM CRYPTOGRAPHY:***

Quantum cryptography is a method of encryption that uses the naturally occurring properties of quantum mechanics to secure and transmit data in a way that cannot be hacked. Cryptography is the process of encrypting and protecting data so that only the person who has the right secret key can decrypt it.

REQUIREMENTS FOR IMPLEMENTING QUANTUM COMPUTING

1. Long Coherence Time:

Long qubit coherence times are a prerequisite for quantum computing. Coherence time is the time duration over which the qubit states is considered to be notvarying. How long can a quantum superposition state survive? That length of time is called the coherence time. As long as there exists a definite phase relation between different qubit states, the system is said to be coherent. When, the pahse r elation is broken, the system is said to be decoherent.

2. High Scalability

In quantum computing scalability refers to ability to handle increased computing demands. The quantum computers must be able operate in a Hilbert space whose dimensions may be grown exponentially without an exponential cost in resources(such as time, space or energy). Successful development of quantum computer swill require not only further quantum computing hardware development, but also the continued theoretical development of algorithms and quantum error correction codes, and the architecture connections between the theory and the hardware Normally, architecture with solid-state qubits provides the route of scalability.

3. High Fault Tolerance and Quantum Error Correction :

By nature, qubits are fragile. They require a precise environment and state to operate correctly, and they're highly prone to outside interference. This interference is referred to as 'noise', which is a consistent challenge and a well-known reality of quantum computing. As a result, error correction plays a significant role. The ability to correct errors using error-prone resources is called fault-tolerance. Fault tolerance has been shown to be theoretically possible for error rates beneath a critical threshold that depends on the computer hardware, the sources of error, and the protocols used forQEC. Quantum error correction (QEC) is used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise. Quantum error correction is challenging because measurements of a quantum state in general disrupt the delicate superpositions that they are supposed to protect. However, many new codes, techniques, and methodologies have been developed to implement error correction for large scale quantum algorithms. This can be overcome by using Peter Shor's quantum error correcting code. Essentially the use of entanglement helps detect and correct errors while keeping the state of a qubit intact.

4. Ability to Initialize Qubits:

As a computation begins, the initial set of qubits in the quantum computer are referred to as ‘physical qubits’. . Initialization refers to the ability to quickly cool quantum system into a low-entropy state; for example, the polarization of a spin intoits ground state. Normally, the models of quantum computation are based on performing some operations on a state of qubit and finally measuring/reading out the result, a procedure that is dependent on the initial state of the system. In most of the cases the approach to initialise a state is to let the system anneal into the ground state and then we can start the computation. This is of particular importance when you consider Quantum Error Correction, a procedure to perform quantum processes that are robust to certain types of noise, that requires a large supply of fresh initialised qubits.

5. Universal quantum gates:

The system must have available a universal set of quantum logic gates. The large Hilbert space must be accessible using a finite set of control operations; the resources for this set must also not grow exponentially. In the case of qubits, it issufficient to have available any “analog” single qubit gate (e.g. an arbitrary rotation ofa spin-qubit), and almost any “digital” two-qubit logic operation, such as the controlled-NOT gate. Quantum logic gates are reversible, unlike many classical logic gates.

6. Efficient Qubit-state Measurement Capability:

Measurement is at the corner of all quantum algorithms. Measurement refers to the ability to quickly determine the state of a qubit with the accuracy allowed by quantum mechanics. After the measurement, the system is in the measured state! That is, further measurements will always yield the same value. We can only extract one bit of information from the state of a qubit.

7. Faithful transmission of flying qubitsand interconversion between stationary and “flying” qubits:

These two conditions are necessary when considering quantum communication protocols such as quantum key distribution that involve exchange of coherent quantum states or exchange of entangled qubits. When creating pairs of entangled qubits in some experimental set up usually these qubits are ‘stationary’ and cannot be moved from the laboratory. If these qubits can be teleported to flying qubits such as encoded into the polarisation of a photon then we can consider sending entangledphotons to a third party and having them extract that information, leaving twoentangled stationary qubits at two different locations. The ability to transmit the flyingqubit without decoherence is major problem. Several attempts have been made toproduce a pair of entangled photons and transmit one of the photons to some otherpart of the world by reflecting off of a satellite or by use optical fibres.

COMPANIES PROVIDING QUANTUM COMPUTING

AMAZON

Amazon is a more recent player joining the race to build a quantum computer. In 2021, Amazon announced the opening of the AWS centre for Quantum Computing in Pasadena, Calif. It has partnered with the California Institute of Technology to foster the next generation of quantum scientists and fuel their efforts to build a fault-tolerant quantum computer. In addition to these efforts, Amazon offers a quantum computing service called Amazon Bracket, which provides developers access to quantum computers and tools from third-party partners. This service enables customers to speed up their own quantum computing research, build quantum projects and run quantum algorithms.

GOOGLE

Google's Quantum AI lab has been developing a programmable superconducting processor. A recent iteration is Sycamore, a 54-qubit processor composed of high-fidelity quantum logic gates.In 2019, Google claimed Sycamore had achieved quantum supremacy. Quantum supremacy is the point at which a quantum device can solve a problem exponentially faster than a classical processor. In this case, Sycamore took about 200 seconds to sample one instance of a quantum circuit 1 million times -- something that would have taken a classical supercomputer nearly 10,000 years to do.

IBM

In November 2022, IBM held the Quantum Summit, where it unveiled a development roadmap detailing its plans and timeline for progressing quantum computing through 2025. Its primary goal is to go beyond using single processors, and by 2025, it plans to combine multichip processors into what it has name Kookaburra processors. Compared to IBM's latest processor, Osprey, which has 433 qubits, IBM plans for the multichip Kookaburra processor to have 4,158 qubits. These plans are ambitious, but IBM has a strong history in quantum development. In 2019, it launched a commercial quantum computer, the IBM Quantum System One. It's currently developing the IBM Quantum System Two to better serve Osprey and future quantum processors

MICROSOFT

Microsoft is currently developing its own scalable, full-stack quantum machine with a unique approach that's focused on topological qubits. The research team at Microsoft has invented a control chip, called Gooseberry, and a cryo-compute core that are key to this approach. In short, the chip and core work together to maintain a stable cold environment that enables the quantum stack to send and receive information to and from every qubit. Achieving this task is no simple feat; however, if Microsoft can pull it off, it will result in a highly scalable quantum computer that can support even larger, more complex applications. While development is still ongoing for this hardware, Microsoft also offers a portfolio of quantum computers from other hardware providers as part of its Azure Quantum platform. This service provides an open development environment for researchers, businesses and developers that enables the flexibility to tune algorithms and explore today's quantum systems.

INTEL

Like IBM, INTEL has a storied history in the semiconductor industry, having been founded in Mountain View, California, in 1968 by Gordon Moore of "Moore's law" fame and Robert Noyce, a physicist and co-inventor of the integrated circuit.Leading the charge is Intel's Director of Quantum Hardware, James Clarke. Intel Labs, the R&D arm of the company, is leveraging its expertise in high-volume transistor manufacturing to develop 'hot' silicon spin-qubits, much smaller computing devices that operate at higher temperatures. Second, the Horse Ridge II cryogenic quantum control chip provides tighter integration. And third, the cryoprober enables high-volume testing that is helping to accelerate commercialization. Intel is working on both superconducting and spin qubits, though research on superconducting seems to be limited to their academic affiliations at Qutech (Delft university), whereas spin qubits are the main focus with activities at Qutech and in-house.

There are also many more companies nowadays in the market who are using quantum computing mechanism in the industry and in also technical field they are *Rigetti, IonQ, D-Wave, Alibaba, Tencent, Huawei, and Xanadu.*

USECASES AND REAL WORLD EXAMPLE

- ### MEDICINE CREATION

Quantum computers can create new medicines and vaccines to fight diseases. They can help cure diseases that have so far been unable to be cured. Quantum computing makes it possible for medical researchers to run simulations on millions of different factors with a high level of accuracy. The medical field can use these kinds of computers better. They can find diseases and figure out how to make medicines. Using these computers, scientists can diagnose and test for different kinds of diseases in labs.

- ### USED IN ARTIFICIAL INTELLIGENCE

Recent developments in quantum physics show that quantum computers will play a crucial role in future artificial intelligence developments. Quantum computer systems can provide the basis for solving some of the most challenging problems in artificial intelligence.When it comes to artificial intelligence, these kinds of computers do well. Normal computers can't make decisions as well as they can. When scientists use these computers, they can do better research.

- ### MACHINE LEARNING

Quantum computers are used in machine learning. It is a computer science approach that's based on the idea of artificial intelligence. Computer scientists use this technology to perform image recognition, speech processing, computational linguistics, and pattern recognition. Most of all, scientists hope that quantum computers will make a big step forward in artificial intelligence (AI). These could then take over tasks like analyzing data or making predictions in a safe and reliable way.Using machine learning techniques is a good way to use quantum computing. Users can write less code and use a process called "machine learning" to improve results.

- ### DEEP LEARNING

Deep learning is a type of machine learning that aims to mimic the way neurons interact in the brain. This is a very powerful form of computing, much more powerful than traditional computing based on binary language.Quantum computers can perform deep learning algorithms much faster and more accurately. In this way, quantum computers will play a vital role in the development of future technologies.

- ### COMPUTATIONAL CHEMISTRY

Quantum computers will also find new ways to solve problems in computational chemistry. This is because they can help us to model the chemical interactions between electrons and atoms in a computer model. Once these interactions are known, it is easier to study their properties and possibilities.

- ## THE TECHNOLOGY OF LIFE

Quantum computers will also find new relationships between atoms and molecules. These molecules could be used to create new medicines, such as vaccines. This technology will help us to identify the roles of all molecules in the body that are essential for life.

- ## HEALTHCARE

Quantum computing can speed up making vaccines and medicines, help doctors figure out what's wrong with a patient sooner, and customize treatment. Creating new drugs is a slow process, and the coronavirus vaccine showed that current methods can only speed it up so much. Part of the reason it takes so long is that scientists have to make molecules to see how they react with other molecules; Scientists will be able to test molecules, though, if they have quantum computers. Scientists will be able to run simulations of even single molecules on quantum computers that are very accurate.

- ## FINANCE

Some studies say that in the short term, the finance industry stands to gain the most from quantum computers. The first benefit of quantum computing for finance is that it lets us figure out stock market outcomes that were too random and too many to figure out before. Quantum computers will be able to handle the fact that investors want more accurate risk assessments for different possible scenarios. Quantum computers will also be better at figuring out credit when calculating loans and portfolios, which will help people make better lending decisions.

- ## CLIMATE FORECASTING

Quantum computers might also be able to tell what the weather will be like. In an interview with PBS, an MIT professor said, "Right now, it might take a classical computer longer to predict the weather than it takes for the weather to change."This could help a lot of other industries that depend on the weather, such as transportation, food production, and more. In the United States, the weather has a direct or indirect effect on nearly 30% of the GDP. Also, being able to predict the weather would give people more time to get ready for disasters.

- ## TRAVEL AND TRANSPORTATION

When AI is combined with quantum computing, it will help with travel and transportation in many ways, such as improving traffic signals, making self-driving cars, controlling air traffic, and more. Quantum computers could change the transportation industry in a big way, but it might take a few years before they are useful.Quantum computers will be able to quickly figure out the best routes for traffic, which will cut down on traffic jams and speed up the delivery of goods. Companies like Amazon and FedEx could make up to 600% more money if they were more efficient.

Quantum computers could also help speed up the development of self-driving cars, which need to be trained by AI. Even with the fastest computers in the world, it can take weeks or months to train AI algorithms. With quantum computers, this could happen a lot faster.

Quantum computers will also have an effect on media and entertainment, consumer goods, and insurance, among other fields. But quantum computers will also change privacy and cybersecurity in ways that could be very bad for organizations that aren't ready.

CHALLENGES IN QUANTUM COMPUTING

- **Building scalable and stable quantum hardware**: One of the main challenges in quantum computing is building a device that can handle a large number of qubits while maintaining stability and coherence.

- **Dealing with noise and errors in quantum systems:** Quantum systems are highly sensitive to noise and errors, which can disrupt computation and lead to inaccurate results.

- **Developing efficient algorithms for quantum computation**: As the capabilities of quantum computers are expanding, so is the need for new algorithms that can take advantage of the unique properties of quantum systems.

- **Implementing error correction and error mitigation methods**: Error correction and error mitigation are crucial for building a useful quantum computer, but the methods used to accomplish this are still in the early stages of development.

- **Designing and implementing quantum communication and networking**: Quantum communication and networking technologies, such as quantum key distribution and quantum teleportation, are still in the early stages of development, and there are many challenges to be overcome before they can be implemented on a large scale.

- **Addressing the lack of skilled professionals**: The field of quantum computing is relatively new and there is a shortage of professionals with the necessary skills and knowledge to work with quantum devices and software.

- **Addressing the lack of integration of quantum technology with classical technology**: It is still a challenge to seamlessly integrate quantum technology with existing classical technology, making it difficult to use quantum computing for practical applications.

- **Developing robust software and programming languages for quantum computing**: There are currently limited software and programming languages that can be used for quantum computing, and these are still in the early stages of development.

- **Addressing the lack of standardization**: There is currently a lack of standardization in the field of quantum computing, which makes it difficult to compare different devices and technologies.

- **Addressing the cost-effectiveness of quantum computing**: Building and operating a quantum computer is still very expensive, and this is a major barrier to the widespread adoption of quantum computing

CONCLUSION

Quantum computers have the potential to revolutionize computation by making certain types of classically intractable problems solvable. While no quantum computer is yet sophisticated enough to carry out calculations that a classical computer can't, great progress is under way.

THANK YOU