Quantum Computing

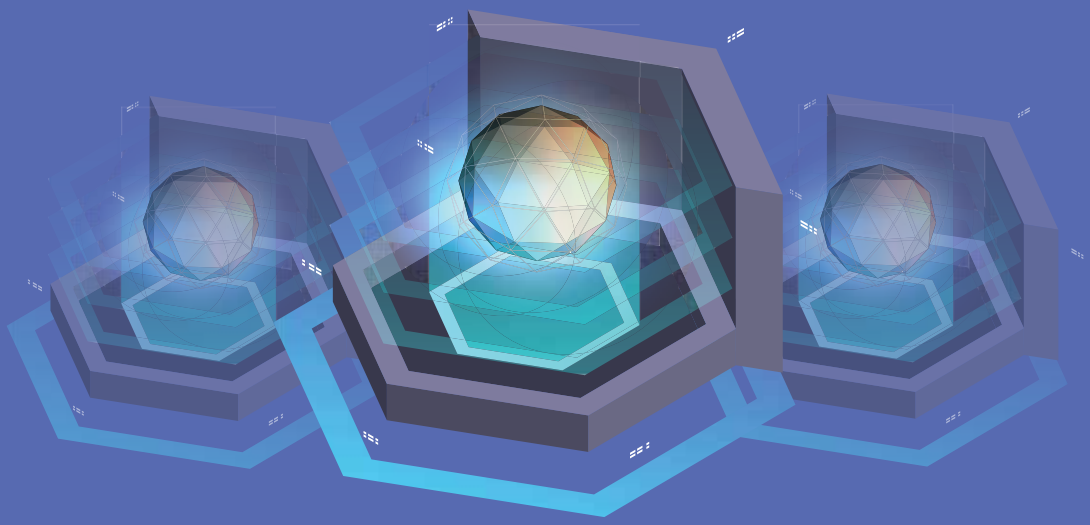
The first spark in quantum computing was ignited in 1981 by the famous physicist and MIT professor Richard Fayman. He proposed his research paper, “Classical computers cannot simulate the evolution of quantum systems efficiently". With this paper, he proposed a quantum computer model, theoretically, which is capable of such type of simulations. Quantum computers harness the behavior of quantum physics and apply it to the field of computation. It accounts for the properties of atomic and subatomic particles.

Quantum computers can create vast multidimensional spaces to represent very large problems. Algorithms that employ quantum wave interference are then used to find solutions in this space and translate them into forms we can use and understand. Several Quantum Properties such as superposition and entanglement make it different from classical computers and make it much faster than any classical computer. Entanglement is important in quantum cryptography and quantum communication.

WHY QUANTUM COMPUTERS DESERVE THE SPOTLIGHT THIS CENTURY

Many tech giants such as Google, IBM are already working in the field of quantum computing.

The first application is cybersecurity which led to the development in the field of quantum computing. Looking at the present and the future, we can see that the world is moving towards Artificial intelligence and machine learning, which require heavy computation and optimization. After many research papers were published on the topic of AI and ML using Quantum Computers, There is a sharp increase of students, researchers, and professors into the field of quantum computing. Other significant applications using quantum computers are financial modeling, drug modeling, and weather forecasting.



Quantum-era cybersecurity will wield power to detect and deflect quantum-era cyber attacks before they cause harm. But it could become a double-edged sword, as quantum computing may also create new exposures, such as the ability to quickly solve the difficult math problems that are the basis of some forms of encryption.

QUANTUM

Quantum computing, and prosaic quantum technology, promise to transform cybersecurity in four major areas.

1. **Generating random numbers using a quantum computer** - Conventional random number generators typically rely on algorithms known as pseudo-random number generators, which are not truly random and thus potentially open to compromise.

2. **Quantum key distribution (QKD)** - Sharing cryptographic keys between two or more parties (to allow them to exchange information privately) is at the heart of secure communications. QKD utilizes aspects of quantum mechanics to enable the completely secret exchange of encryption keys and can even alert the presence of an eavesdropper.

3. The emerging field of quantum machine learning may enable exponentially faster, more time - and energy-efficient machine learning algorithms leading to more effective algorithms for identifying and defeating novel cyberattack methods.

4. The most controversial application of QC is its potential for breaking public-key cryptography, specifically the RSA algorithm, which is at the heart of the nearly $4 trillion e-commerce industry. RSA relies on the fact that the product of two prime numbers is computationally challenging to factor. It would take classical computers trillions of years to break RSA encryption. A quantum computer with around 4,000 error-free qubits could defeat RSA in seconds. Classified financial and national security data is potentially susceptible to being stolen today — only to be decrypted once a sufficiently powerful quantum computer becomes available. But with the development of more powerful Quantum computers, we can increase the encryption making our data safer.

QUANTUM

QUANTUM ALGORITHMS

Quantum Algorithms is an algorithm implemented in quantum computers to perform quantum computation. The most common model used for computation is the quantum circuit model. Like classical algorithms is a finite sequence of instructions or step-by-step procedures where instructions are implemented one at a time. The quantum algorithm follows the same procedure, but quantum computers support parallelism, i.e., multiple instructions can execute simultaneously.

The first major qc algorithm - In 1994, Peter Shor developed his algorithm allowing quantum computers to efficiently factorize large integers exponentially quicker than the best classical algorithm on traditional machines. Theoretically, the Shor algorithm is capable of breaking many of the cryptosystems used today. The possibility to break cryptosystems in hours rather than millions of years using quantum computers lit a fire of interest for quantum computing and its applications.

How did Shor develop the first major qc algorithm - Peter Shor was a student at Caltech, where Richard Feynmann was the professor. In Feynman's lecture, he presented his paper on negative probability. The idea for this paper came to him first after viewing Bell's theorem, which stated the EPR paradox. He tried to find in his writings, but he got into a hidden assumption that probability lies between 0 & 1, which made him release his papers on negative probability to prove Bell's theorem wrong. However, it did not serve the purpose.

In 1992, Umesh Vazirani presented his papers in Bell labs on "Bernstein Vazirani Algorithm," which could work faster on the quantum computer than the classical computer, which was the first motivation for the shot to make an algorithm in the field of quantum computing. Later in the Symposium on Theory of Computing (STOC) conference , Simon presented his algorithm, which the various researchers rejected. However, Shor was motivated by solving Simon's problem that he decided to use those methods to solve a discrete log problem. He presented his work at the National institute of standards and technology (NIST) conference which was specifically organized to understand the factoring algorithm. In the next few weeks, he solved the prime factorization problem with quantum algorithms with the concepts used similarly in discrete log problems. Finding the algorithm for the factorizing problem brought him glory worldwide; since the old encryption system works based on discrete log problems, modern-day encryptions are possible using Shor's algorithm's help.

This interested other people and made the students and researchers work in this field.

WHAT DOES THE RISE IN QC MEAN FOR OUR ECONOMY ?

Quantum computing can be used for innovations and calculations across all industries that were not possible with classical computers and have the potential to benefit society in various ways, including making smarter investment decisions, developing drugs and vaccines faster, and revolutionizing transportation.

HealthCare

With the rise of quantum computing, the healthcare industry will benefit from the increase in the speed of vaccines and pharmaceuticals. Drug development is a slow process since scientists have to test the interactions with other molecules. However, Quantum computers will give scientists high-speed and exact simulations for every single drug molecule.

Finance

Quantum computing would easily calculate outcomes in stock markets that were previously too random and numerous since investors need more accurate risk assessments. Additionally, when calculating loans and portfolios, quantum computers will offer more precise calculations of credit, which will enable better lending decisions.

Additionally, quantum computers may help quicken the development of autonomous vehicles, which must be trained through AI. It can take weeks or months with the world's fastest computers to train AI algorithms, but with quantum computers, development could be exponentially faster.