

Archives available at [journals.mriindia.com](http://journals.mriindia.com)

## International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526

Volume 14 Issue 01, 2025

### A Comprehensive Study of Quantum Computing: Principles, Applications and Its Impact on Future Technologies

Jayshree Tarare<sup>1</sup>, Harshika Chimankar<sup>2</sup>, Minakshi Janbandhu<sup>3</sup>, Chetna Turkar<sup>4</sup>, Mr. Ajay nanwatkar<sup>5</sup>

Department of MCA, Suryodaya College of Engineering & Technology (SCET), Nagpur, (MS)-India

<sup>1</sup>tararejayshree2002@gmail.com, <sup>2</sup>chimankarharshika3@gmail.com, <sup>3</sup>minakshijanbandhu2000@gmail.com,

<sup>4</sup>chetnatarkar321@gmail.com, <sup>5</sup>ajay.nanwatkar10@gmail.com

Peer Review Information	Abstract
<p>Submission: 11 Feb 2025 Revision: 20 Mar 2025 Acceptance: 22 April 2025</p> <p><b>Keywords</b></p> <p>Quantum Computing Real-Time Systems Program Processors</p>	<p>"Quantum computing" marks a ground breaking change in the field of computing by using quantum mechanics, like superposition and entanglement, to process data. Quantum computing represents a contemporary method of computation grounded in the principles of quantum mechanics and its astonishing phenomena. It is an exquisite fusion of physics, mathematics, computer science, and information theory. It offers significant computational capability, reduced energy usage, and exponential speeds compared to traditional computers by manipulating the behaviour of tiny physical entities, such as microscopic particles including atoms, electrons, photons, and so on. It reveals the potential of quantum computers that can affect our lives from different perspectives such as cyber security, traffic management, healthcare, artificial intelligence, and numerous others.</p>

#### Introduction

In today's computing processors translate information into binary digits 0's and 1's, and logic gates that rely on switching transistors are utilized to handle them. These computers' function based on sequential principles where tasks are completed in an orderly fashion until results are produced. At present, computing is directed by the laws of classical physics until the size of semiconductor transistors nears atomic dimensions. In 1975, Gordon Moore forecasts that the number of transistors in integrated circuits will double every eighteen months.[1] It is anticipated that by 2024, it will become difficult for Moore's law to persist as the size of conventional classical bits nears the scale of an atom [2]. In such scenarios, material particles cannot be accurately described by classical physics, and a new computer model may become necessary

by then. Therefore, achieving computation at atomic dimensions that adheres to non-traditional physics known as quantum mechanics is crucial. In addressing the challenges presented, one potential solution is the quantum computer, which may hold promise. Quantum computing is garnering increasing interest from industrial sectors, including not only large corporations like Microsoft or Google but also firms more traditionally associated with nanoelectronics and nanotechnology (e. g., IBM and Intel [3]. The field of quantum computing was established in the 1980s. In 1999, the first quantum computer was created from superconductors by D-Wave Systems, a Canadian company.[4] Quantum computers are not limited to just two states; they represent data using quantum bits, known as qubits, which can take the value

of 0 or 1, or both 0 and 1 simultaneously in a phenomenon called superposition. When considering the atomic level, quantum computers can be physically constructed using atoms, photons, ions, or electrons, along with their respective control devices that function together to serve as both processor and memory. At the level of fundamental research, many alternative physical realizations of qubits have been suggested and investigated. Recently, solid-state implementations have gained significant attention due to their ability to scale to large quantities of qubits.[5]

### History Of Quantum Computing

Advancements in one area of science and technology result in the emergence of another. Within a century, the research and advancement of effective computing technologies have transformed science, technology, and nations significantly. The initial practical computer from the 20th century could not perform mathematical computations independently. Practical devices require a strong physical realization of theoretical ideas. Today, computers resolve issues immediately and precisely, given that the input is pertinent and a specific set of instructions is provided.

Quantum computing possesses a captivating history that traces back to the early 20th century when quantum mechanics emerged as a revolutionary domain, thanks to the contributions of physicists like Max Planck, Albert Einstein, and Niels Bohr.[6] These trailblazers established the groundwork for comprehending the behaviour of particles at both atomic and subatomic scales, which subsequently inspired the idea of quantum computing. In the 1980s, Richard Feynman suggested the idea of employing quantum computers to emulate quantum systems, emphasizing their advantages over classical computers in certain tasks.[7] David Deutsch further refined the notion of a universal quantum computer that could efficiently carry out any computation.[8] The creation of quantum algorithms, such as Shor's algorithm in 1994, demonstrated the vast potential of quantum computing in fields like cryptography by surpassing classical approaches[9]. As the concept developed, researchers began taking experimental actions in the 1990s, constructing small-scale quantum processors and investigating qubit technologies like trapped ions and superconducting

circuits. Gradually, technology leaders like IBM and

Google entered the competition to create practical quantum systems, resulting in substantial progress in scaling and minimizing error rates. In 2019, Google asserted that it had reached "quantum supremacy," solving a problem quicker than a classical computer for the first time. Presently, quantum computing has progressed beyond theoretical investigation and is poised to transform industries such as artificial intelligence, materials science, and cryptography. Although its promising potential is evident, quantum computing continues to encounter challenges related to stability, scalability, and error correction, but its journey thus far lays the groundwork for ground breaking impacts in the future.[10]

### New Kind Of Computing

Today's computers are more compact, less expensive, faster, significantly efficient, and even more powerful in comparison to the early computers that used to be large, expensive, and more energy-consuming. This advancement is possible due to enhancements in architecture, hardware components, and the software operating on them. The electronic circuits used in computers are shrinking day by day. Transistors are tiny semiconductor devices that function to amplify and switch electrical or electronic signals. They used to be manufactured on a piece of silicon. The circuit was formed by linking these transistors together on a single silicon surface. The configuration of circuits in an integrated circuit (IC) was printed simultaneously across all layers of silicon. This process takes the same duration even if the number of transistors in the circuit increases. The production cost of an IC was determined by the size of silicon rather than the quantity of transistors. This decrease in cost led to lower product prices, which in turn boosted the manufacturing and selling of ICs, enhancing both benefits and sales. From the concept of connecting individual transistors to the aggregation of these transistors (Logic Gates) and finally, the assemblage of these Logic Gates into a single integrated circuit (IC). Nowadays, a single IC can even encapsulate small computers onto it. Gordon Moore, Intel's co-founder, discovered in 1965 that the number of transistors on a silicon microprocessor chip had doubled every year while the prices were halved since their inception. This observation is known as

Moore's Law. Moore's Law is significant because it implies that computers and their computing power become progressively smaller and faster over time. Although this law is currently slowing down, the progress in traditional computers is not as it once was. This leads to the concept of the smallest computer by minimizing the size of the circuit down to the dimensions of an atom. However, at this scale, these circuits would be unable to function as a switch since electrons within an atom can become undetectable on one side of a barrier and reappear on the other side, meaning they can exist in multiple locations simultaneously. This phenomenon is known as "Quantum Tunneling" in quantum mechanics. It illustrates that the dimensions of classical computer circuits have reached their limit after 5-7 nano-meters. The representation and processing capabilities of these computers can be described by classical physics laws, which provide a deterministic explanation of the Universe. Yet, it falls short in predicting all observable phenomena occurring in nature, leading to the development of quantum mechanics, the most significant transformation in physics. Therefore, there is a necessity for new computing methods beyond traditional classical computing to encode its state into some physical information rather than a circuit. As quantum phenomena impose more constraints on computer design, the search for new models continues [11].

### Need For Quantum Computing

Quantum computers are capable of solving any computational problem that classical computers can handle. The Church-Turing thesis suggests that the reverse is also applicable, meaning classical computers can address all quantum computer problems as well. This implies that, in terms of computability, they do not offer any additional advantages over classical computers; however, there exist some intricate and unsolvable problems that current conventional computers cannot resolve within a practical timeframe. These problems require greater computational power. Quantum computers can address such issues in a reasonably and exponentially reduced time complexity, a phenomenon referred to as "Quantum Supremacy" [12].

In 1993, Peter Shor demonstrated that quantum computers can assist in solving these problems significantly more efficiently, often within seconds, without overheating. He created

algorithms that factor large numbers swiftly [13]. Their computations are founded on the probability of an atom's state before it becomes definitively known. They possess the capability to handle data in an exponentially vast volume. This indicates that a functional quantum computer could potentially break cryptographic secret codes. This could jeopardize the security of encrypted communications and data [14]. It could reveal confidential and protected secret information. Nonetheless, the benefits of quantum computers are considered to substantially outweigh their drawbacks. Therefore, they remain essential, and ongoing research is directed toward a promising future.

Quantum computing, on the other hand, harnesses the principles of quantum mechanics, including superposition and entanglement, allowing qubits to exist in multiple states simultaneously. This enables quantum computers to process vast amounts of information in parallel, drastically improving efficiency for specific tasks. Applications that benefit from quantum computing include drug discovery [15]

### PRINCIPLES OF QUANTUM COMPUTING

The principles of quantum computing revolve around the application of quantum mechanics to process information in ways that surpass classical computing capabilities. Here are the core concepts:

**1. Superposition:** Superposition is a quantum phenomenon where a qubit, unlike a classical bit, can exist in a combination of states simultaneously. A classical bit has a definite value of 0 or 1. However, a qubit can be in a state that is 0, 1, or a combination of 0 and 1 (a weighted probability of both). This means that a quantum computer with multiple qubits can perform a vast number of calculations in parallel. For example, with just 2 qubits, we can represent and compute four states (00, 01, 10, 11) simultaneously, while a classical system would have to handle each state one at a time. In practice, superposition enables quantum computers to explore multiple solutions to a problem simultaneously, providing significant speedups for certain computations [16].

**2. Entanglement:** Entanglement is a unique and deeply non-intuitive property of quantum mechanics, where two or more qubits become interconnected such that the state of one qubit instantly reflects changes in the state of the other, even if they are separated by large distances. This interconnection allows qubits to share and

process information in ways classical bits cannot. For quantum computing, entanglement is a powerful tool because it enables qubits to work together as a system, exponentially increasing computational efficiency. For example, when entangled qubits are manipulated, the results reflect the entire system of qubits, creating possibilities for solving highly complex problems [17].

**3. Quantum Interference:** Quantum interference plays a crucial role in quantum algorithms. When qubits exist in a superposition state, their probabilities interfere with one another. By carefully designing quantum operations, we can amplify the probabilities of desired solutions while canceling out unwanted outcomes. This "wave-like" property of quantum mechanics is a key reason why quantum algorithms, like Grover's algorithm for search problems, can achieve speedups over classical ones [18].

**4. Quantum Parallelism:** Quantum parallelism arises from the concept of superposition. Because qubits can process multiple possibilities at once, quantum computers can perform many calculations simultaneously. For instance, a quantum computer with (n) qubits can represent and compute ( $2^n$ ) states simultaneously. This is why quantum computing holds promise for solving problems that are practically unsolvable with classical computers, such as factoring extremely large numbers or optimizing complex systems [19].

### Applications Of Quantum Computing

Below are some of the main applications that we will encounter shortly in the forthcoming era:

**Cryptography:** Quantum computers can break existing cryptographic techniques like RSA through algorithms such as Shor's algorithm [20].

**Optimization Problems:** Quantum algorithms can optimize problems more efficiently than classical methods, including molecular simulations and traffic optimization [21].

**Artificial Intelligence:** Quantum computing can enhance AI models by handling large datasets and improving training accuracy [16].

### Architecture Of Quantum Computers

Architecture can be viewed as a schematic. The architecture of the quantum computer consists of a blend of classical and quantum elements, and it can be categorized into 5 layers.

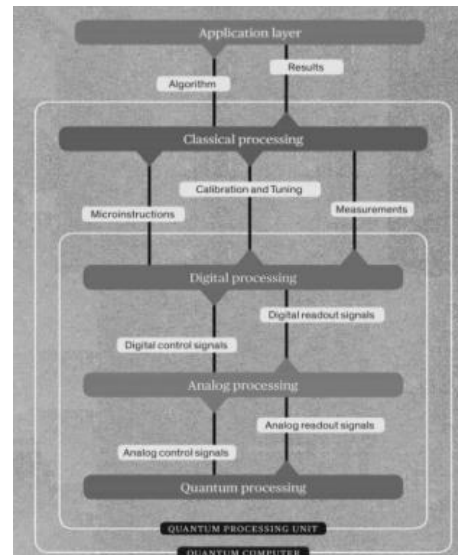


Fig.1. architecture of quantum computers [27]

**Application Layer** - This layer is not a component of a quantum computer. It serves to represent a user interface, the operating system for a quantum computer, a coding environment, etc., which are necessary for developing appropriate quantum algorithms. It is independent of hardware.

**Classical Layer** - This layer optimizes and compiles the quantum algorithm into microinstructions. Additionally, it processes the quantum-state measurement that is returned from the hardware in the lower layers and provides it to a classical algorithm to generate results.

**Digital Layer**- It translates microinstructions into signals (pulses) required by qubits that function as quantum logic gates. It serves as the digital representation of the needed analogy pulses in the subsequent layers. Additionally, it provides quantum measurement as feedback to the upper classical layer in order to integrate the quantum results into the final outcome.

**Analog Layer**- It generates voltage signals which possess phase and amplitude modulations similar to waves, for transmitting them to the lower layer so that qubit operations can be carried out.

**Quantum Layer**- It is combined with both the digital and analogy processing layers on the same chip. It is utilized for maintaining qubits and is kept at room temperature (absolute). Error correction is managed at this level. This layer assesses the performance efficiency of the computer.

Quantum Processing Unit (QPU) consists of three layers including the digital processing layer, analogy processing layer, and quantum processing layer. QPU and classical layer collectively form the Quantum Computer.[17]

### Hardware And Software Require for Quantum Computers

Below are the main categories of quantum computing hardware:

**Superconducting Qubits:** Superconducting qubits represent one of the most commonly employed technologies for constructing quantum computers. They utilize superconducting circuits, which can conduct an electrical current without resistance when cooled to extremely low temperatures. These circuits generate qubits that can occupy quantum states [18].

**Trapped Ions:** Trapped-ion quantum computers utilize ions (charged atoms) that are confined and controlled with electromagnetic fields. Lasers are employed to manipulate the state of each ion, enabling the creation of qubits [19].

**Photonic Qubits:** Photonic quantum computing employs photons as qubits, usually encoded in characteristics such as polarization or phase. Photons are controlled using optical components like beam splitters and wave plates [20].

**Quantum Dots:** Quantum dots consist of semiconductor materials capable of trapping a limited number of electrons. The configurations of these electrons are used to signify qubits. Quantum dots are governed by electric or magnetic fields [21].

### Software Of Quantum Computers

Quantum computing software consists of programming languages, algorithms, and tools utilized to design, control, and optimize quantum operations.

**Quantum Programming Languages:** In order to create programs for quantum computers, developers utilize specific quantum programming languages. These languages enable users to articulate quantum operations, such as gate sequences, and manipulate qubits in manners that take advantage of quantum properties.

**Qiskit (IBM):** An open-source framework based on Python for quantum computing that allows users to write quantum algorithms,

simulate them, and execute them on IBM's quantum processors [16].

**Cirq (Google):** A Python library created by Google for the development, simulation, and execution of quantum circuits on quantum hardware [19].

### Limitations Of Quantum

The exponential computational capabilities of quantum computers can be achieved by evaluating and addressing any type of design constraint, which aids in preventing their quality decline. There are four primary design constraints. The first constraint is that the number of coefficients in Dirac notation, which describes the state of a quantum computer, increases exponentially with the increase in the number of qubits, specifically when all the qubits become entangled with one another [22]. To unlock the full capability of quantum computing, qubits must adhere to the principle of entanglement, implying that the state of one qubit has to be connected with the states of other qubits [23]. Direct attainment of this is not feasible since establishing a direct connection between qubits is challenging. However, it can be broken down into

a series of straightforward fundamental operations, directly supported by the hardware. Additionally, one can engage in indirect coupling, which is recognized as an overhead in classical computing machines and is vital during the initial phases of development, especially when qubits and gate functions are restricted.

The second constraint is that replicating an entire quantum system is impossible due to a principle referred to as the no-cloning principle [24]. There exists the danger of arbitrary information being deleted from the original qubits since the state of qubits or a set of qubits transfers to another set of qubits instead of being copied. The creation and retention of copies of intermediate states or partial results in memory is a crucial element in classical computing. However, quantum computers require an alternate approach. Certain quantum algorithms facilitate access to classical bits from storage, enabling the identification of which bits are loaded and queried in the memory of the quantum system to execute their functions effectively [26].

The third constraint stems from the lack of noise protection in qubit operations. Minor imperfections in gate operations or input signals accumulate over time, disturbing the

system's state because they are not eliminated by the fundamental gate operations.

### Future Scope of Quantum Computing

A considerable level of effort is still required before a functional quantum computer can

be introduced. Certain future developments are necessary. Some of the upcoming requirements include enabling a Quantum Error Correction algorithm that necessitates minimal overhead and lowers the error rates in qubits, creating additional algorithms with fewer qubits for problem-solving, minimizing circuit thickness to allow NISQ computers to function, progressing methods that can verify, debug, and emulate quantum computers, scaling the number of qubits per processor in such a manner that the error rate is sustained or significantly improved if feasible, interleaving operations within a qubit, identifying more algorithms that can shorten computation time, and establishing input-output for the quantum processor. Such 'Quantum games' are anticipated in the future, offering unforeseen

scenarios and outcomes that players can encounter, as quantum computers will randomly incorporate all possible operations into the game due to their quantum characteristics such as superposition and entanglement of qubits. It will present an endless experience.

'Quantum computing in Cloud' holds the potential to surpass business endeavors like other emerging technologies, including cryptography and artificial intelligence. Given that the classical simulation of fifty qubits is equivalent to one Petabyte of memory, which doubles with each additional qubit added, the memory needed must also be substantial enough to create an environment for application development and testing for numerous developers to simulate quantum computers utilizing appropriate shared resources. AI and machine learning challenges could be resolved in practical time frames that could decrease from hundreds of thousands of years to mere seconds. Several quantum algorithms have been concocted, such as Grover's algorithm for searching and Shor's algorithm for factoring large numbers. More quantum algorithms are expected to emerge soon. Google has also announced its intention to create a functional quantum computer within the next five years, utilizing a 50-qubit quantum computer and achieving quantum supremacy. IBM will soon

present commercial quantum computers as well. The advancement of development in the domain of quantum computers relies on numerous elements. Interest and financial backing from the private sector can facilitate the creation of commercial applications for NISQ computers. It hinges on the evolution of quantum algorithm development, the availability of sufficient investment in the quantum technology sector from the government, and the exchange of ideas among researchers, scientists, and engineers. To clarify the limitations of quantum technology, a defensive outcome is also advantageous. It can assist in overcoming these negative results.

### Conclusion

By resolving intricate issues that traditional computers are unable to handle, quantum computing has the potential to completely transform a number of industries. Quantum computers may execute several calculations at once by utilizing the concepts of superposition and entanglement. This capability will result in exponential speedups in fields such as artificial intelligence, material science, and encryption. Hardware stability, error correction, and scalability issues still exist, although they are gradually being resolved by continued study and technical developments. As quantum computing develops, it has the potential to unleash hitherto unheard-of potential, stimulating creativity and offering answers to some of the world's most important problems.

### Reference

Moore, G.E. (1975). "Progress in Digital Integrated Electronics." IEEE.

Waldrop, M.M. (2016). "The Chips Are Down for Moore's Law." Nature.

National Institute of Standards and Technology (NIST). (2020). "Quantum Computing: Progress and Prospects."

D-Wave Systems Inc. (1999). "Quantum Computing Technologies."

IBM Quantum. (2021). "Quantum Systems and Qubit Implementations."

Planck, M. (1901). "On the Law of Distribution of Energy in the Normal Spectrum." Annalen der Physik.

Feynman, R.P. (1982). "Simulating Physics with Computers." International Journal of Theoretical Physics.

Deutsch, D. (1985). "Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer." *Proceedings of the Royal Society A*.

Shor, P.W. (1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*.

Google AI Quantum. (2019). "Quantum Supremacy Using a Programmable Superconducting Processor." *Nature*.

National Physical Laboratory (NPL). (2020). "Quantum Tunneling and Its Applications."

John Preskill, "Quantum Computing and the Entanglement Frontier," 2012.

Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," 1994.

Rainer Blatt and David Wineland, "Entangled States of Trapped Atomic Ions," 2008.

Scott Aaronson, "Quantum Computing Since Democritus," 2013.

IBM Research, "Qiskit Documentation," 2021.

David Wineland, "Quantum Information Processing with Trapped Ions," 2003.

Lov Grover, "A Fast Quantum Mechanical Algorithm for Database Search," 1996.

Google AI Quantum Team, "Cirq Documentation," 2020.

Jeremy O'Brien, "Photonic Quantum Technologies," 2009.

Leo Kouwenhoven, "Quantum Dots: A Doorway to Advanced Electronics," 1997.

Nielsen, M.A., & Chuang, I.L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. *Quantum*, 2, 79.

Arute, F., Arya, K., Babbush, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505-510.

Shor, P.W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5), 1484–1509.

Grover, L.K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212–219.

<https://www.intechopen.com/chapters/73811>