IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, June 2024

Quantum Computing: A Paradigm Shift in Computational Powder

Abres Siddique and Sheetal Waghmare
Students, Department MCA
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Quantum computing represents a transformative leap in computational capabilities, promising to solve problems deemed intractable for classical computers. This paper provides an in-depth analysis of the principles underlying quantum computing, explores key quantum algorithms, evaluates the current state of quantum hardware, and discusses the implications for various fields. By examining both theoretical foundations and practical advancements, this paper aims to highlight the paradigm shift brought about by quantum computing.*

Keywords: Quantum Computing, Quantum Algorithms, Quantum Hardware, Quantum Advantage, Quantum Information Theory

I. INTRODUCTION

Quantum computing leverages the principles of quantum mechanics to process information in fundamentally new ways. Unlike classical computing, which uses bits to represent data as 0s or 1s, quantum computing uses qubits that can exist in superposition of states. This property, along with entanglement and quantum interference, enables quantum computers to perform certain computations exponentially faster than classical computers. The potential applications of quantum computing span numerous fields, including cryptography, drug discovery, optimization, and machine learning.

II. THEORETICAL FOUNDATIONS

Quantum mechanics describes the behaviour of particles at the atomic and subatomic levels. Key principles relevant to quantum computing include:

A. Superposition

Superposition is a fundamental concept in quantum mechanics where a quantum system such as a qubit can exist in multiple states simultaneously. In classical computing, a bit can be either in state 0 or state 1. However, a qubit can exist in a linear combination of these states, represented mathematically as:

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$$

where$|\alpha|^2+|\beta|^2=1$, ensuring normalization. This means the qubit is in a superposition of states $|0\rangle$and $|1\rangle$with probability amplitudes α and βrespectively. The physical state is determined only upon measurement, collapsing to either $|0\rangle$ or $|1\rangle$with probabilities $|\alpha|^2$ and $|\beta|^2$.

Superposition is pivotal in quantum computing because it allows quantum computers to process vast amounts of information simultaneously, potentially solving certain problems exponentially faster than classical computers.

B. Entanglement

Entanglement is a unique quantum phenomenon where two or more qubits become correlated with each other in such a way that the state of one qubit is instantly related to the state of another, regardless of the distance between them. This correlation persists even if the entangled qubits are spatially separated by large distances, violating classical intuitions about locality.

Entanglement is established through quantum interactions and persists until the entangled qubits are measured or interact with their environment, causing their entangled state to collapse. This property is crucial for quantum

DOI: 10.48175/568

computing because it allows for parallelism and simultaneous processing of information, enabling quantum computers to perform certain tasks with unprecedented efficiency.

C. Quantum Interference

Quantum interference is a phenomenon where quantum states can constructively or destructively interfere with each other, depending on their phase relationships. This interference is a consequence of the wave-like nature of quantum particles and is exploited in various quantum algorithms to enhance desirable outcomes and suppress undesirable ones.

In quantum computing, quantum interference plays a significant role in algorithms such as Grover's algorithm, where it helps amplify the probability of finding the correct solution while damping incorrect ones. This ability to manipulate interference is one of the factors that contribute to the potential computational superiority of quantum computers over classical ones for certain problem types.

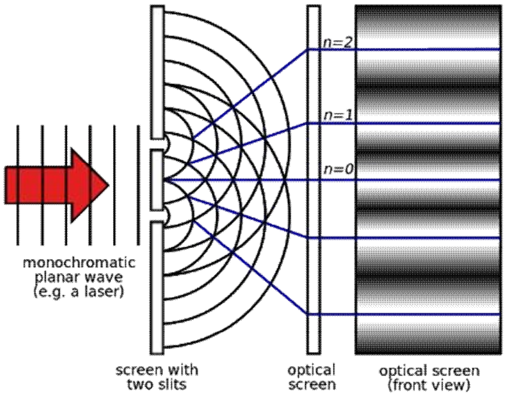

Figure 1: Quantum Mechanics Principles

D. Qubits and Quantum Gates

A qubit is the fundamental unit of quantum information. Quantum gates manipulate qubits, similar to how logic gates manipulate bits in classical computing. Common quantum gates include:

- Pauli-X, Y, Z Gates: Basic single-qubit operations corresponding to rotations around the x, y, and z axes.
- Hadamard Gate: Creates super positions.
- CNOT Gate: A two-qubit gate that entangles qubits.

Gate	Symbol	Function
Pauli-X	X	Flips the state of a qubit.
Pauli-Y	Y	Rotates the qubit around the Y-axis.
Pauli-z	Z	Flips the phase of the qubit.
Hadamard	H	Creates a superposition state.
CNOT	CX	Entangles two qubits.

Table 1: Common Quantum Gates and Their Functions

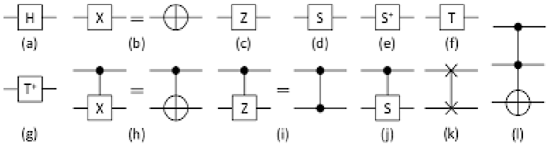

Figure 2: Basic Quantum Gates.

DOI: 10.48175/568
ISSN 2581-9429 IJARSCT

III. QUANTUM ALGORITHMS

Quantum algorithms exploit quantum mechanics to solve specific problems more efficiently than classical algorithms. Leveraging phenomena such as superposition, entanglement, and interference, these algorithms can offer significant computational speedups for certain types of problems. This section examines two of the most well-known quantum algorithms: Shor's algorithm and Grover's algorithm.

A. Shor’s Algorithm

Shor's algorithm, developed by Peter Shor in 1994, revolutionized the field of quantum computing by demonstrating that quantum computers could solve specific problems exponentially faster than classical computers. Specifically, Shor's algorithm can factor large integers in polynomial time, posing a significant threat to classical encryption methods such as RSA, which rely on the computational difficulty of factoring large numbers for security.

Shor's algorithm uses two key quantum components: the Quantum Fourier Transform (QFT) and period finding. The algorithm can be broken down into the following steps:

Quantum Fourier Transform (QFT): The QFT is applied to a superposition of states to transform the quantum state into a form that reveals periodicity. This step is crucial for identifying the period of the function that will lead to the factorization of the integer.

$$QFT|x\rangle = -\,{}^{1}\sqrt{N}\sum_{k-0}^{N-1} e^{2\pi i}\frac{km}{N}|k\rangle$$

Where $|x\rangle$ *and* $|k\rangle$ *are quantum states, N is the number to be factored, and n is the integer whose period is to be found.*

Period Finding: Using the QFT, the algorithm identifies the period r of a function related to the number Nto be factored. The periodicity of this function is key to finding the factors of N’s.

$$\downarrow$$

$$r = \text{Period of } f(x) = a^{x} \bmod N$$

Classical Computation: Once the period r is found, classical algorithms use this period to compute the factors of the number N. This involves some additional steps, including checking for the greatest common divisor (GCD) to obtain the factors.

$$gcd(a^{r/2} \pm 1, N)$$

The combination of quantum and classical computations in Shor's algorithm enables it to factorize integers exponentially faster than the best-known classical algorithms. This capability poses a potential risk to current cryptographic systems, driving the need for quantum-resistant encryption methods.

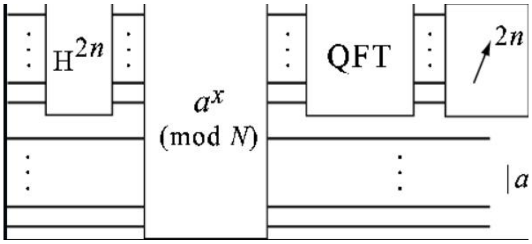

Figure 3: Shor's Algorithm Process.

B. Grover’s Algorithm

Grover’s algorithm, introduced by Lov Grover in 1996, provides a quadratic speedup for unstructured search problems, significantly improving search efficiency over classical methods.

Algorithm steps:

Initialization: Prepare a superposition of all possible states by applying a Hadamard transform, creating an equal superposition of N states.

DOI: 10.48175/568

$$|\psi\rangle = {}^{1}\sqrt{N} \sum_{k=0}^{N-1} |x\rangle$$

Oracle Application: Utilizes an oracle to mark the solution by inverting the amplitude of the correct state, without collapsing the superposition.
The oracle $U f$ *applies a phase shift to the state* $|x\rangle$ *if* x *is the solution:*
$U f|x\rangle = (-1)^{f(x)}|x\rangle$
where $f(x) = 1$ *for the correct* x *and* $f \downarrow = 0$ *otherwise.*
The oracle $U f$ *applies a phase shift to the state* $|x\rangle$ *if* x *is the solution:*
$U f|x\rangle = (-1)^{f(x)}|x\rangle$
where $f(x) = 1$ *for the correct* x *and* $f(x) = 0$ *otherwise.*
Amplitude Amplification: Enhance the probability amplitude of the correct answer using the Grover iteration, which consist of the oracle followed by a diffusion transform. The diffusion transform amplifies the probability of the correct solution state.

$$D = 2|\psi\rangle\langle\psi| - I$$

Where I is the identify matrix.

Measurement: Measures the state to obtain the solution after a sufficient number of Grover iterations (about$\overline{N}$ *), maximizing the probability of identifying the correct solution.*
Grover's algorithm demonstrates quantum computing's efficiency in solving search problems and finds applications in database search, cryptography, and optimization.

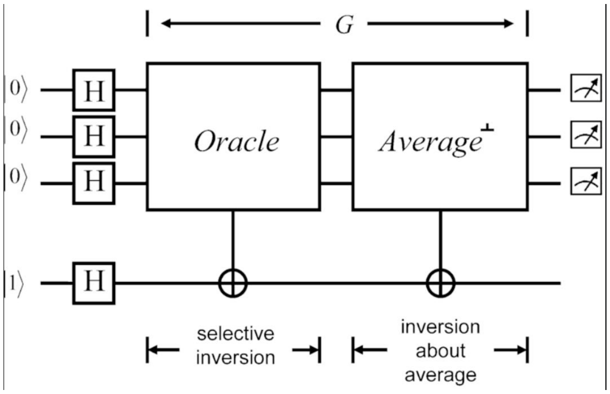

Figure 4: Grover's Algorithm Process.

IV. QUANTUM HARDWARE

Quantum hardware is the backbone of quantum computing, with various technologies being developed to build scalable and reliable quantum computers. Each approach has its own set of advantages and challenges, contributing to the diverse landscape of quantum hardware. This section explores three leading quantum hardware approaches: superconducting qubits, trapped ion qubits, and photonic qubits.

Superconducting Qubits:

Superconducting qubits are circuits made from superconducting materials, which are cooled to cryogenic temperatures to maintain quantum coherence. These qubits are fabricated using advanced lithography techniques, similar to those used in classical integrated circuits, but they operate on the principles of quantum mechanics. Companies like IBM and Google have made significant advancements in this area, demonstrating quantum supremacy with certain computational tasks.

The operation of superconducting qubits relies on Josephson junctions—nonlinear inductors that allow for the superposition and entanglement of quantum states. The Josephson junction is formed by sandwiching a thin layer of insulating material between two superconductors, enabling the tunnelling of Cooper pairs (pairs of electrons bound together at low temperatures). This tunnelling effect is essential for creating the quantized energy levels that define the qubit states.

One of the key advantages of superconducting qubits is their relatively fast operation speeds, which are essential for executing complex quantum algorithms within the coherence time of the qubits. Moreover, advancements in error correction and qubit connectivity have led to significant improvements in the scalability and reliability of superconducting qubit systems.

However, superconducting qubits face challenges such as maintaining coherence at scale and managing the large amounts of cryogenic infrastructure required. Researchers are continuously working on improving coherence times and developing more efficient cooling methods to address these issues.

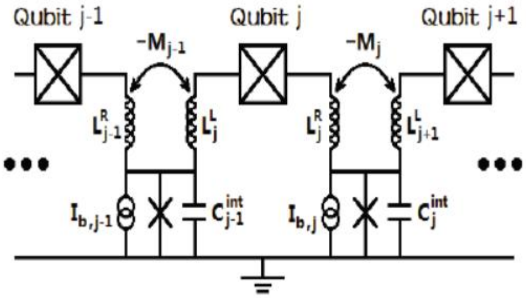

Figure 5: Superconducting Qubits Setup.

Trapped Ion Qubits

Trapped ion qubits use individual ions confined in electromagnetic fields and manipulated using lasers. This technology is renowned for its long coherence times and high-fidelity operations, making it a strong candidate for building scalable quantum computers. Companies like IonQ are at the forefront of developing trapped ion technology.

The primary advantage of trapped ion systems is their ability to maintain qubit states for extended periods, significantly reducing de-coherence issues. Each ion represents a qubit, and quantum information is stored in the electronic states of the ions. Lasers are used to perform operations on the qubits, including initialization, manipulation, and measurement.

Trapped ion qubits also benefit from high connectivity, as ions in a trap can interact with each other through Coulomb interactions, enabling entanglement and complex multi-qubit operations. Additionally, trapped ions can be transported between different zones of a trap, facilitating modular and scalable quantum computing architectures.

Despite these advantages, trapped ion systems face challenges related to the complexity of laser control and the scalability of trapping and manipulating large numbers of ions. Advances in laser technology and ion trap design are crucial for overcoming these hurdles and making trapped ion quantum computers more practical.

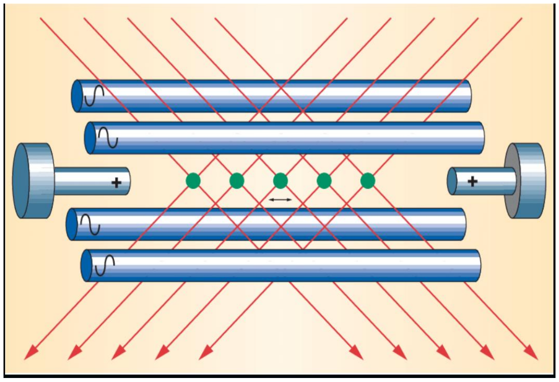

Figure 6: Trapped Ion Qubits Setup.

Photonic Qubits

Photonic qubits utilize photons as the carriers of quantum information. Photons offer several advantages, including high speed and compatibility with existing fibre-optic communication infrastructure. Photonic quantum computing leverages the properties of light particles, such as polarization and phase, to encode information.

One of the main advantages of photonic qubits is their robustness against de-coherence, as photons do not interact with their environment as strongly as other quantum systems. This makes them particularly suitable for quantum communication and networking applications, where maintaining quantum information over long distances is critical.

Photonic quantum computing can be implemented using various approaches, such as linear optical quantum computing (LOQC), which uses beam splitters, phase shifters, and photon detectors to perform quantum operations. Another approach involves using integrated photonic circuits, which can be fabricated using techniques similar to those used in classical photonics.

However, photonic qubits face challenges in scalability, primarily due to the probabilistic nature of photon sources and the need for efficient photon detection. Research is ongoing to develop deterministic single-photon sources and more efficient photonic quantum gates to address these issues.

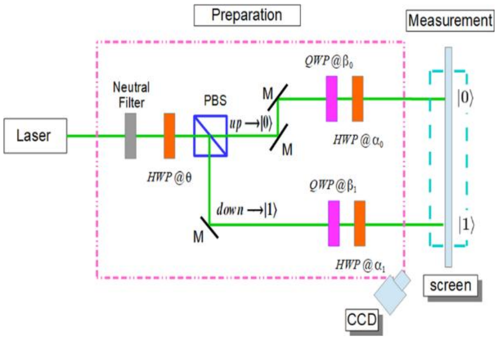

Figure 7: Photonic Qubits Setup.

V. DE-COHERRENCE AND NOISE

Qubits are highly susceptible to de-coherence and noise, which can cause the loss of quantum information. De-coherence occurs when a qubit interacts with its environment, leading to the loss of its quantum properties. Noise in quantum systems can arise from various sources, including thermal fluctuations and electromagnetic interference.

Developing error correction methods and fault-tolerant quantum computing is critical to mitigate these challenges. Quantum error correction (QEC) techniques aim to encode logical qubits into multiple physical qubits to detect and correct errors. However, implementing effective QEC requires overcoming significant technical hurdles due to the sensitivity of quantum states to environmental interactions.

Scalability

Scaling quantum systems to thousands or millions of qubits while maintaining control and coherence is a significant engineering challenge. As the number of qubits increases, the complexity of managing their interactions grows exponentially. Precise control over each qubit is essential for maintaining coherence and enabling reliable quantum computation.

Achieving scalability involves addressing several technical issues:

- Qubit Connectivity: Ensuring that qubits can reliably interact with each other over long distances without losing coherence.
- Error Rates: Minimizing errors that arise from imperfect operations and environmental factors.
- Fabrication Processes: Developing scalable fabrication techniques to manufacture qubits with high fidelity and uniformity.

DOI: 10.48175/568

Quantum Error Correction

Quantum error correction (QEC) is indispensable for achieving fault-tolerant quantum computing. QEC techniques involve encoding logical qubits into multiple physical qubits in such a way that errors can be detected and corrected without disturbing the quantum information excessively. However, implementing QEC faces several challenges:

- High Overhead: Many QEC techniques require a large number of physical qubits to encode a single logical qubit, resulting in significant overhead.
- Complex Implementation: Techniques like the surface code, which uses a 2D grid of qubits, offer high fault-tolerance but are complex to implement and operate.
- Error Types: Correcting both bit-flip and phase-flip errors effectively without introducing additional errors is a non-trivial task.

Technique	Description	Challenges
Shor Code	Corrects bit-flip and phase-flip errors.	High overhead in number of qubits.
Stene Code	A type of stabilizer code, corrects multiple errors.	Complex implementation.
Surface Code	Uses a 2D grid of qubits, highly fault-tolerant.	Requires many physical qubits for one logical qubit.

Table 2: Quantum Error Correction Techniques

These challenges underscore the ongoing need for interdisciplinary research and technological innovation to overcome barriers and realize the full potential of quantum computing in practical applications.

VI. IMPLICATIONS FOR VARIOUS FIELD

Quantum computing has the potential to revolutionize numerous fields by providing unprecedented computational power. This section explores the implications of quantum computing in cryptography, drug discovery, optimization problems, and machine learning.

6.1 Cryptography

Quantum computing poses both opportunities and threats to cryptography. On one hand, it can break widely used encryption schemes, presenting a significant challenge to data security. Shor's algorithm, for instance, can efficiently factorize large integers, rendering classical encryption methods like RSA and ECC (Elliptic Curve Cryptography) vulnerable. These encryption methods rely on the computational difficulty of factoring large numbers or computing discrete logarithms, tasks that classical computers find infeasible but quantum computers can accomplish in polynomial time.

On the other hand, quantum computing also enables the development of quantum-safe cryptographic methods. Quantum Key Distribution (QKD) is a notable example. QKD leverages the principles of quantum mechanics, such as the no-cloning theorem and quantum entanglement, to provide a secure communication method that is theoretically immune to eavesdropping. Any attempt at interception can be detected by the legitimate communicating parties, ensuring the integrity of the transmitted information.

Further, post-quantum cryptography is an active area of research aiming to develop classical cryptographic algorithms that are resistant to quantum attacks. These algorithms are designed to be secure against both quantum and classical adversaries, ensuring long-term data security as quantum computing technology advances.

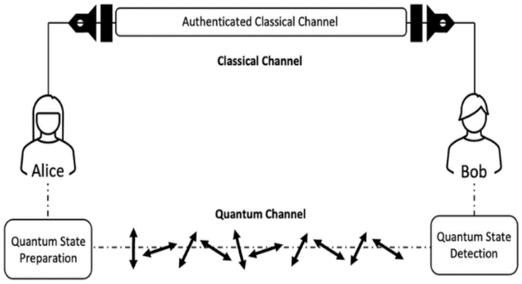

Figure 8: Quantum-Safe Cryptography.

6.2 Drug Discover

Quantum computing promises to transform the field of drug discovery by enabling the simulation of complex molecular interactions with unprecedented accuracy. Classical computers struggle with simulating large quantum systems because the required computational resources grow exponentially with system size. Quantum computers, however, can naturally simulate quantum phenomena, making them well-suited for modelling molecular structures and chemical reactions.

Quantum simulations can provide detailed insights into molecular behaviour, potentially accelerating the identification of drug candidates and the understanding of reaction mechanisms. This capability can lead to the discovery of new drugs and materials much faster than current methods allow. For example, simulating the interactions of proteins with potential drug molecules can reveal binding affinities and optimal configurations, guiding the design of more effective therapeutic agents.

Moreover, quantum computing can aid in the exploration of new materials for drug delivery systems and other biomedical applications. By accurately predicting the properties of complex molecules, quantum simulations can facilitate the development of materials with specific desired characteristics, enhancing the efficacy and safety of medical treatments.

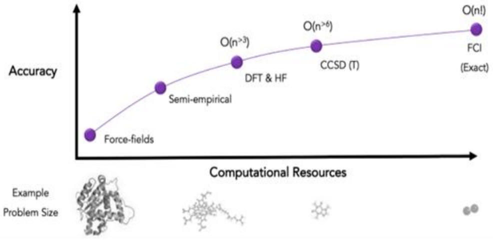

Figure 9: Quantum Drug Discovery Process.

6.3 Optimization Problems

Optimization problems are prevalent across various industries, including logistics, finance, and artificial intelligence. These problems often involve finding the best solution from a vast number of possible configurations, a task that becomes computationally intensive as the problem size grows. Quantum algorithms offer the potential to solve these optimization problems more efficiently than classical algorithms.

For example, the traveling salesman problem, which seeks the shortest possible route visiting a set of cities, can benefit from quantum speedups. Similarly, portfolio optimization in finance, which aims to allocate assets to maximize returns while minimizing risk, can be enhanced using quantum algorithms. In artificial intelligence, training neural networks often involves optimizing a large number of parameters, a process that can be expedited by quantum computing.

Quantum annealing, a technique used by quantum computers like those developed by D-Wave, is particularly suited for solving optimization tasks. It leverages quantum tunnelling to escape local minima and find global optima, offering a significant advantage over classical methods that might get stuck in suboptimal solutions. This ability to explore and optimize complex landscapes efficiently can lead to improved decision-making and operational efficiencies in various fields.

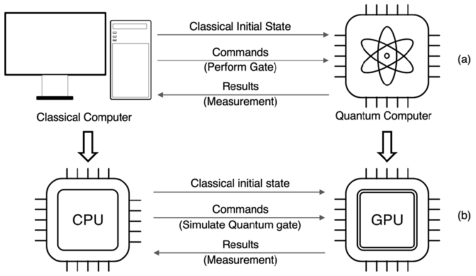

Figure 10: Optimization with Quantum Computing

6.4 Machine learning

Quantum machine learning has the potential to enhance data processing and pattern recognition capabilities, leading to more powerful and efficient AI systems. Quantum algorithms, such as the quantum support vector machine (QSVM) and quantum neural networks, can process high-dimensional data more effectively than classical algorithms. These quantum algorithms leverage the principles of superposition and entanglement to explore large solution spaces and identify patterns with greater accuracy.

For instance, quantum computers can perform certain linear algebra operations, such as matrix inversion and eigenvalue decomposition, exponentially faster than classical counterparts. These operations are fundamental to many machine learning algorithms, including those used for classification, clustering, and regression tasks. By accelerating these computations, quantum computing can significantly reduce the time required to train and deploy machine learning models.

Moreover, quantum-enhanced machine learning can improve the performance of AI systems in areas such as image and speech recognition, natural language processing, and predictive analytics. By enabling more efficient data processing and model training, quantum computing can drive advancements in AI, leading to smarter and more adaptive systems.

Quantum machine learning frameworks are being developed to integrate quantum computing capabilities with classical machine learning techniques, creating hybrid models that leverage the strengths of both paradigms. This integration can result in more robust and versatile AI applications, capable of solving complex problems that are currently beyond the reach of classical methods.

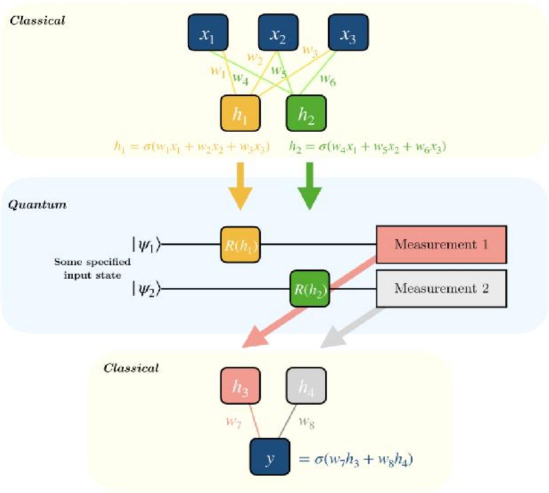

Figure 11: Quantum Machine Learning Framework.

VII. FUTURE DIRECTIONS

The field of quantum computing is rapidly evolving, with ongoing research focused on overcoming current limitations and exploring new applications. This section discusses hybrid quantum-classical computing, quantum networks, and quantum metrology and sensing as promising future directions.

Hybrid Quantum-Classical Computing

Hybrid quantum-classical computing approaches are emerging as practical solutions for near-term applications, leveraging the strengths of both quantum and classical processors to optimize overall performance. These hybrid systems utilize quantum processors for specific tasks that benefit from quantum speedups, while relying on classical processors for other tasks where classical methods are more efficient.

One prominent example of a hybrid algorithm is the variation Quantum Eigen solver (VQE). VQE is used for solving eigenvalue problems, which are crucial in quantum chemistry and material science. In VQE, a quantum processor is employed to prepare a trial wave function and measure its energy, while a classical processor optimizes the parameters of the wave function to minimize the energy.

Another important hybrid algorithm is the Quantum Approximate Optimization Algorithm (QAOA), which is designed for solving combinatorial optimization problems. QAOA alternates between applying a quantum operator to create a superposition of solutions and a classical optimizer to adjust the parameters for better solutions. This hybrid approach leverages quantum parallelism to explore many solutions simultaneously, while classical optimization refines the results.

Hybrid quantum-classical computing represents a realistic pathway to achieving quantum advantage in the near term, as it mitigates some of the challenges associated with building large-scale, fault-tolerant quantum computers. By combining the best of both worlds, these systems can tackle complex problems more efficiently than classical or quantum processors alone.

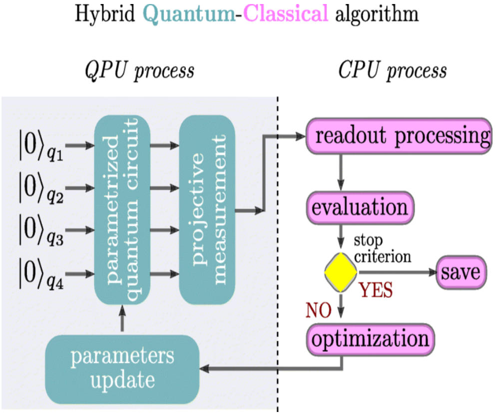

Figure 12: Hybrid Quantum-Classical Computing.

Quantum Networks

Developing quantum networks and quantum internet infrastructure is a crucial direction for the future of quantum computing and communication. Quantum networks utilize principles such as entanglement and quantum teleportation to transmit quantum information across distances securely and efficiently. This infrastructure will enable a variety of advanced applications, including secure communication, distributed quantum computing, and networked quantum sensors.

Quantum networks rely on entanglement to establish connections between distant nodes. Once entangled, quantum bits (qubits) can be teleported from one location to another using quantum teleportation protocols, ensuring that the information is transmitted without being intercepted or corrupted. This property makes quantum networks inherently secure, as any attempt at eavesdropping can be detected through changes in the entangled state.

One significant application of quantum networks is secure communication through Quantum Key Distribution (QKD). QKD allows two parties to generate a shared, secret key using quantum mechanics principles, which can then be used for encrypting and decrypting messages. This method provides security that is theoretically immune to eavesdropping, offering a robust solution for sensitive communications.

In addition to secure communication, quantum networks will enable distributed quantum computing, where multiple quantum processors are interconnected to share and process information collaboratively. This capability can significantly enhance computational power and efficiency for complex tasks that require substantial resources.

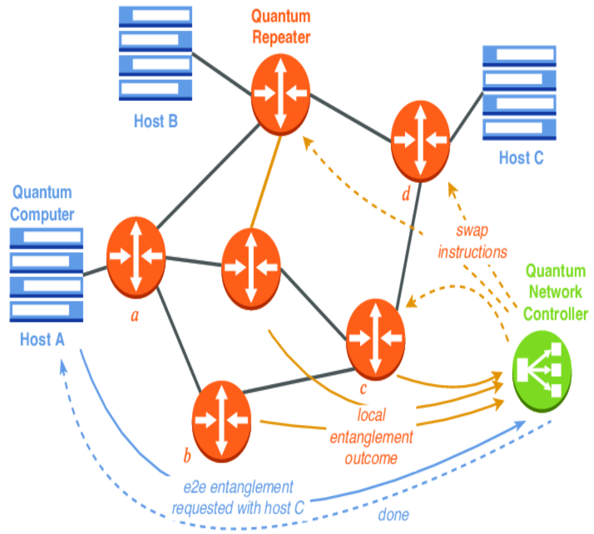

Figure 13: Quantum Network Concept.

Quantum metrology and Sensing

Quantum metrology and sensing represent another exciting frontier in quantum technology, offering unprecedented precision in measurement capabilities that can impact a wide range of fields from fundamental physics to navigation.

Quantum metrology exploits quantum entanglement and superposition to achieve measurement precision beyond classical limits. By using entangled particles, quantum sensors can measure physical quantities such as time, magnetic fields, and gravitational forces with extreme accuracy.

One notable application of quantum metrology is the development of atomic clocks. Atomic clocks based on quantum technology can achieve timing precision far superior to classical clocks, making them essential for applications in global positioning systems (GPS), telecommunications, and scientific research.

Another significant application is in gravitational wave detection. Quantum sensors can detect minute changes in gravitational fields, contributing to the study of astrophysical phenomena and the verification of general relativity.

Quantum gyroscopes, another example of quantum sensing technology, offer enhanced precision for navigation systems. These devices can provide accurate orientation and rotation measurements, benefiting aerospace, maritime, and autonomous vehicle applications.

Quantum metrology and sensing have the potential to revolutionize numerous industries by providing high-precision tools that enable new discoveries and advancements.

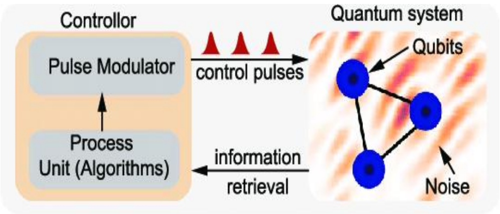

Figure 14: Quantum Sensing Applications.

VIII. CONCLUSION

Quantum computing represents a paradigm shift in computational power, with the potential to solve problems beyond the reach of classical computers. While significant challenges remain, ongoing advancements in quantum algorithms, hardware, and error correction are paving the way for practical quantum computing. The impact of this technology will be profound, reshaping industries and driving new scientific discoveries. As research continues to progress, the realization of a fully functional, large-scale quantum computer becomes increasingly plausible, heralding a new era in computational science.

ACKNOWLEDGMENT

The authors gratefully acknowledge the following individuals and institutions for their contributions to this research:
We extend our sincere appreciation to Sheetal Waghmare for her exceptional mentorship, continuous support, and invaluable feedback throughout this study.
We are grateful to Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application for providing the academic platform and resources essential for pursuing the Master's in Computer Application program.
We also acknowledge the significant contributions of the research institutions and industry partners whose advancements in quantum computing technologies have enriched the scope and depth of this study.
Special thanks go to our families and friends for their unwavering encouragement and understanding throughout this research journey.

REFERENCES

[1] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124-134).
[2] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (pp. 212-219).
[3] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., & Neven, H. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510.
[4] Nielsen, M. A., & Chuang, I. L. (2000). Quantum Computation and Quantum Information. Cambridge University Press.
[5] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.
[6] Brown, K. R., Kim, J., & Monroe, C. (2016). Co-designing a scalable quantum computer with trapped atomic ions. npj Quantum Information, 2, 16034.
[7] Giovannetti, V., Lloyd, S., & Maccone, L. (2004). Quantum-enhanced measurements: beating the standard quantum limit. Science, 306(5700), 1330-1336.