Mrs M.Kalavathi, 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Quantum Computing: Current Progress, Challenges and Future Directions

[1]Mrs M.Kalavathi, [2]S.Aarthi, [3]M.Aimuga Venkatmathi, [4]K.Narmaladevi, [5]G.Abirami, [6]M.Indhumathi

[1]Assistant Professor J.P.College of Engineering,Ayikudy,,
Tenkasi, Affiliated to Anna University,Chennai
[2]Student, Department of Information Technology, J.P.College of Engineering, Ayikudy,
Tenkasi, Affiliated to Anna University Chennai
[3]Student, Department Of Information Technology, J.P.College of Engineering, Ayikudy,
Tenkasi, Affiliated to Anna University Chennai
[4]Student, Department of Information Technology, J.P.College of Engineering, Ayikudy,
Tenkasi, Affiliated to Anna University Chennai
[5]Student, Department of Information Technology, J.P.College of Engineering, Ayikudy,
Tenkasi, Affiliated to Anna University Chennai
[6]Student, Department of Information Technology, J.P.College of Engineering, Ayikudy,
Tenkasi, Affiliated to Anna University Chennai

Abstract- Quantum computing is an emerging computational paradigm that uses the principles of quantum mechanics, including superposition, entanglement, and quantum interference, to process information in fundamentally different ways from classical computers. During the last decade, quantum computing has progressed from theoretical research toward experimental and cloud-accessible systems. Recent developments have focused on increasing the number and quality of qubits, reducing gate errors, developing quantum error correction, improving quantum software, and integrating quantum processors with classical high-performance computing systems. Despite significant progress, practical large-scale quantum computing remains challenging because quantum states are extremely sensitive to environmental disturbances, resulting in decoherence and computational errors. Other challenges include limited qubit coherence time, gate fidelity, scalability, cryogenic requirements, quantum error correction overhead, hardware connectivity, programming complexity, and the difficulty of demonstrating useful quantum advantage for real-world applications. Recent developments from major research organizations indicate a shift from simply increasing physical qubit counts toward building reliable logical qubits and fault-tolerant quantum systems. Google has reported progress toward error-corrected logical qubits, while IBM's roadmap focuses on increasingly complex processors, modular architectures, quantum-classical integration, and fault-tolerant systems. Microsoft is pursuing a topological-qubit approach aimed at scalable quantum computing. This paper reviews the current state of quantum computing, examines major technological and scientific challenges, analyzes current research directions, and identifies future opportunities in drug discovery, materials science, optimization, cryptography, artificial intelligence, finance, and scientific simulation. The study concludes that the most realistic future is likely to involve quantum-centric computing, in which quantum processors work together with classical CPUs, GPUs, high-performance computing systems, and quantum networks rather than completely replacing classical computers.

Keywords— Quantum Computing, Qubit, Superposition, Entanglement, Quantum Error Correction, Quantum Algorithms, Quantum Machine Learning, Fault-Tolerant Quantum Computing, Quantum Advantage, Quantum Networking.

I. INTRODUCTION

Classical computers represent information using bits whose values are either 0 or 1. Modern classical computers have achieved remarkable performance through improvements in semiconductor technology, parallel processing, GPUs, cloud computing, and artificial intelligence. However, some computational problems remain extremely difficult because their computational complexity increases rapidly with problem size.Quantum computing introduces a different model of computation based on quantum mechanics. Instead of classical bits, quantum computers use quantum bits or qubits. A qubit can exist in a combination of the states |0⟩ and |1⟩ through a property called superposition.

A simplified representation of a qubit is:

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

where α and β represent probability amplitudes and:

$$|\alpha|^2 + |\beta|^2 = 1$$

Another important quantum property is entanglement, in which the states of two or more qubits become correlated in ways that cannot be described independently. Quantum algorithms exploit these properties together with quantum interference to perform certain computational tasks differently from classical algorithms.

Important quantum algorithms include:

- Shor's algorithm for integer factorization.
- Grover's algorithm for unstructured search.
- Quantum phase estimation.
- Variational Quantum Eigensolver (VQE).
- Quantum Approximate Optimization Algorithm (QAOA).
- Quantum simulation algorithms.
- Quantum machine-learning algorithms.

The field has moved rapidly from theoretical proposals to experimental processors available through cloud platforms. Research has increasingly shifted toward Noisy Intermediate-Scale Quantum (NISQ) devices and, more recently, toward fault-tolerant quantum computing. Google has reported progress in quantum error correction with its Willow processor, while Microsoft is developing a topological-qubit approach. Therefore, quantum computing should not be considered simply as a faster replacement for classical computers. Instead, it is better understood as a specialized computational technology that can cooperate with classical computing systems to address selected problems that are difficult for classical machines.

II. LITERATURE REVIEW

1. Early Foundations of Quantum Computing

The theoretical foundations of quantum computing emerged from the recognition that quantum systems could be used to represent and manipulate information. Feynman proposed the idea of quantum simulation as a way of efficiently representing quantum physical systems, while Deutsch developed a universal quantum computational model.These foundational contributions established the possibility of creating computational systems based on quantum mechanical principles.Deutsch's work demonstrated that quantum computation could be described using a universal quantum computer model, providing an important theoretical foundation for subsequent quantum algorithms.

2. Shor's Algorithm

Shor introduced a quantum algorithm for integer factorization and discrete logarithms.

The importance of Shor's algorithm comes from its potential impact on public-key cryptographic systems such as RSA and elliptic-curve cryptography.For a sufficiently large fault-tolerant quantum computer, Shor's algorithm could theoretically solve integer factorization much more efficiently than known classical algorithms.

This has created a major motivation for:

- Quantum-resistant cryptography.
- Post-quantum cryptographic standards.
- Quantum-safe communication.
- Cryptographic migration planning.

3. Grover's Algorithm

Grover proposed a quantum search algorithm that provides a quadratic speedup for searching an unstructured database.

If a classical algorithm requires approximately:

$$O(N)$$

operations for an unstructured search, Grover's algorithm requires approximately:

$$O(\sqrt{N})$$

quantum operations.

Although this is not an exponential speedup, it demonstrates an important advantage of quantum computation for specific problem classes.

4. NISQ Computing

Preskill introduced the concept of Noisy Intermediate-Scale Quantum (NISQ) computing to describe quantum processors with tens to thousands of imperfect qubits that operate before fully fault-tolerant quantum computers become available.

NISQ systems have encouraged research into:

- Variational algorithms.
- Quantum machine learning.
- Quantum chemistry.
- Optimization.
- Error mitigation.
- Hybrid quantum-classical algorithms.

However, NISQ systems are limited by noise and relatively short circuit depths.

5. Quantum Hardware Development

Several hardware approaches are being investigated, including:

- Superconducting qubits.
- Trapped-ion qubits.
- Neutral-atom qubits.
- Photonic qubits.
- Topological qubits.
- Silicon spin qubits.

Superconducting processors have received substantial industrial investment, while trapped-ion and neutral-atom approaches offer alternative advantages in fidelity, connectivity, or scalability.IBM has continued to develop superconducting processors and modular architectures, with its roadmap increasingly emphasizing quantum-classical integration and fault-tolerant computation. Google has concentrated on superconducting quantum processors and quantum error correction. Its reported results with Willow demonstrated below-threshold error correction, representing progress toward long-lived logical qubits. Microsoft is pursuing topological qubits and a roadmap that progresses from noisy physical qubits to reliable logical qubits and ultimately to scalable quantum supercomputers.

6. Recent Research Progress

Recent research indicates that the quantum computing field is entering a transition period.

The emphasis is changing from:

- “How many physical qubits can be built?” to:
- “How many reliable logical operations can be performed?”

This is an important distinction because a quantum computer containing a large number of noisy physical qubits may be less useful than a smaller machine containing high-quality logical qubits.IBM's roadmap identifies milestones involving increasingly complex circuits, modular processors, quantum-classical workflows, and fault-tolerant architectures.Google's recent work similarly emphasizes error correction and logical-qubit development.Academic research also continues to evaluate quantum processors, software stacks, algorithms, and future applications. A 2025 review in The Journal of Supercomputing examined the evolution of IBM quantum systems and future directions for quantum computing.

III. METHODOLOGY

This study uses a Systematic Narrative Review Methodology to analyze the current development, challenges, and future directions of quantum computing.

1. Research Design

The research follows five major stages:

Stage 1 – Literature Identification

Research papers, technical reports, institutional publications, and quantum-computing roadmaps were identified from academic and authoritative sources.

Stage 2 – Literature Classification

The collected literature was classified into:

- Quantum hardware.

- Quantum algorithms.
- Quantum error correction.
- Quantum software.
- Quantum applications.
- Quantum networking.
- Quantum security.
- Future directions.

Stage 3 – Comparative Analysis

Different quantum computing approaches were compared according to:

- Qubit scalability.
- Error rates.
- Connectivity.
- Coherence.
- Hardware complexity.
- Software maturity.
- Application potential.

Stage 4 – Challenge Analysis

The major barriers to practical quantum computing were analyzed, including:

- Noise.
- Decoherence.
- Error correction.
- Scalability.
- Cost.
- Infrastructure.
- Algorithmic limitations.
- Lack of proven commercial advantage.

Stage 5 – Future Direction Analysis

Emerging research areas were analyzed to identify likely future directions.

IV. MAIN RESULTS

1. Current Progress of Quantum Computing

The review indicates that quantum computing has progressed substantially in five major areas:

Increasing Qubit Quality

Quantum hardware research has moved beyond simply increasing qubit counts. Researchers are increasingly focusing on:

- Gate fidelity.
- Coherence time.
- Connectivity.
- Readout accuracy.
- Error rates.
- Logical-qubit quality.

Quantum Error Correction

Quantum error correction is one of the most important developments in the field.A classical bit can be copied easily for redundancy. Quantum information cannot simply be copied because of the no-cloning theorem.Instead, quantum error-correction codes distribute quantum information across multiple physical qubits.

The basic idea is:

Google's reported Willow results demonstrated below-threshold quantum error correction, an important step toward practical logical qubits.

Quantum-Classical Hybrid Computing

Current quantum computers are not isolated machines.

A realistic architecture combines:

CPU + GPU + QPU + Cloud + HPC

The classical computer prepares the problem, controls the quantum circuit, processes measurements, and optimizes parameters.

The quantum processor performs specific quantum operations.

Classical Computer

IBM's current strategy explicitly emphasizes quantum-centric computing in which CPUs, GPUs and QPUs work together.

2. Major Challenges

Challenge 1: Decoherence

Quantum states are highly sensitive to environmental disturbances.

Interaction with:

- Heat.
- Electromagnetic radiation.
- Vibrations.
- Material defects.

can cause quantum information to decay.

Challenge 2: Quantum Errors
Quantum operations are not perfectly accurate. Errors may occur during:

- State preparation.
- Quantum gates.
- Measurement.
- Qubit interactions.

Therefore, error correction is essential.

Challenge 3: Scalability
Building a system with thousands or millions of high-quality physical qubits is extremely difficult.
Scaling requires:

- Advanced fabrication.
- Control electronics.
- Cryogenic infrastructure.
- High-quality materials.
- Efficient qubit connectivity.
- Advanced software.

IBM's roadmap highlights the infrastructure and engineering challenges involved in scaling fault-tolerant systems.

Challenge 4: Quantum Error-Correction Overhead
A single logical qubit may require many physical qubits depending on the hardware error rate and error-correction code.

Therefore:

Physical Qubits ≠ Logical Qubits
This is one of the most important concepts for understanding quantum computing scalability.

Challenge 5: Lack of Broad Quantum Advantage
A quantum computer is not automatically faster than a classical computer.

Quantum advantage depends on:

- The problem.
- Algorithm design.
- Hardware quality.
- Circuit depth.
- Classical baseline.
- Input/output overhead.

Therefore, meaningful quantum advantage must be demonstrated against strong classical alternatives.
Challenge 6: High Infrastructure Cost

Some quantum hardware requires extremely specialized environments, including:

- Dilution refrigerators.
- Vacuum systems.
- Laser systems.
- Microwave electronics.
- Shielding.
- Precision control systems.

This increases development and operational costs.

V. COMPARATIVE ANALYSIS OF QUANTUM TECHNOLOGIES

Technology	Major Advantage	Major Challenge	Current Potential
Superconducting	Fast gates and mature fabrication ecosystem	Cryogenic cooling and noise	High
Trapped Ion	High gate fidelity	Slow operations and scaling	High
Neutral Atom	Large arrays and flexible connectivity	Control complexity	High
Photonic	Natural networking potential	Photon generation/detection challenges	High
Topological	Potentially strong error protection	Technology is still developing	Long-term
Silicon Spin	Potential compatibility with semiconductor industry	Precise control and scaling	Promising

Interpretation: No single qubit technology has yet been established as the universally dominant approach. Different architectures may ultimately serve different applications.

VI. QUANTUM COMPUTING APPLICATIONS

1. Drug Discovery
Quantum computers may simulate molecular interactions more naturally than classical systems.

Potential applications include:
- Molecular simulation.
- Protein-ligand interactions.
- Drug candidate screening.
- Chemical reaction modeling.

2. Materials Science
Quantum simulation could help researchers investigate:
- New battery materials.
- Superconducting materials.
- Catalysts.
- Solar-cell materials.
- Advanced semiconductor materials.

3. Optimization
Potential applications include:
- Transportation routing.
- Supply-chain optimization.
- Scheduling.
- Portfolio optimization.
- Resource allocation.

Algorithms such as QAOA are being studied for these types of problems.

4. Artificial Intelligence and Machine Learning
Quantum machine learning combines quantum computing with machine-learning techniques.

Possible research areas include:
- Quantum neural networks.
- Quantum kernels.
- Quantum classifiers.
- Hybrid quantum-classical models.
- Quantum optimization for machine learning.

However, practical advantages over highly optimized classical machine learning remain an open research question.

5. Cybersecurity
A sufficiently powerful fault-tolerant quantum computer could threaten some widely used public-key cryptographic systems.

Therefore, organizations are increasingly preparing for post-quantum cryptography (PQC).

6. Finance
Possible applications include:
- Portfolio optimization.
- Risk analysis.
- Derivative pricing.
- Fraud detection.
- Financial optimization.

VII. MAIN FINDINGS TABLE

Research Area	Current Progress	Major Limitation	Future Direction
Qubits	Increasing quality and scale	Noise	High-quality logical qubits
Error Correction	Below-threshold demonstrations and active development	Large overhead	Fault-tolerant computing
Algorithms	Many algorithms developed	Limited practical advantage	Application-specific algorithms
Hardware	Multiple competing architectures	Scaling complexity	Modular quantum systems
Software	Cloud platforms and SDKs available	Programming complexity	Automated quantum software
AI	Hybrid quantum-ML research	Advantage not yet established broadly	Quantum-enhanced ML
Chemistry	Strong theoretical potential	Hardware limitations	Large-scale molecular simulation

Research Area	Current Progress	Major Limitation	Future Direction
Optimization	QAOA and hybrid methods	Classical competition	Industry-specific quantum optimization
Networking	Early experimental progress	Loss and connectivity	Quantum internet
Security	PQC transition underway	Cryptographic migration complexity	Quantum-safe infrastructure

Future Directions

Fault-Tolerant Quantum Computing

The most important future direction is the development of fault-tolerant quantum computers. Future systems must achieve:

High-quality physical qubits → Logical qubits → Fault tolerance → Large-scale computation

IBM's roadmap currently targets fault-tolerant architectures as a major long-term milestone.

Quantum Internet

Quantum networking could eventually connect quantum computers over long distances.

Potential benefits include:

- Quantum communication.
- Distributed quantum computing.
- Quantum-secure communication.
- Quantum teleportation.
- Networked quantum processors.

Microsoft's roadmap also identifies quantum networking as an important long-term direction.

Quantum Machine Learning

Future research may investigate whether quantum processors can provide measurable benefits for selected machine-learning workloads.

Future directions include:

- Quantum deep learning.
- Quantum reinforcement learning.
- Quantum kernels.
- Hybrid quantum-classical neural networks.
- Quantum generative models.

Quantum Computing and Artificial Intelligence

AI can also help quantum computing.
Machine learning can be used for:

- Quantum error mitigation.
- Circuit optimization.
- Qubit calibration.
- Noise prediction.
- Quantum control.
- Automated circuit generation.

Thus, the relationship is bidirectional:
Quantum Computing → AI
and
AI → Quantum Computing

The literature shows that quantum computing has entered a significant transition from experimental demonstrations toward utility-oriented development. Earlier research primarily focused on proving that quantum computation was theoretically possible. Current research increasingly concentrates on making quantum computers reliable, scalable, programmable, and economically useful. One important observation is that qubit count should not be used as the only measure of quantum-computer performance. Gate fidelity, circuit depth, connectivity, error rates, logical-qubit lifetime, and useful computational throughput are equally important. Another major observation is the increasing importance of hybrid computing. Quantum processors are expected to work as specialized accelerators within larger classical computing environments rather than independently replacing CPUs and GPUs. Current roadmaps from IBM, Google, and Microsoft illustrate different technological strategies toward this objective. IBM emphasizes modular superconducting systems and quantum-centric integration, Google emphasizes superconducting processors and error correction, and Microsoft focuses on topological qubits and protected quantum states. Consequently, the future of quantum computing is likely to be heterogeneous, with several hardware technologies potentially coexisting.

VIII. CONCLUSION

Quantum computing represents one of the most significant emerging technologies in computer science. It introduces a fundamentally different computational model based on quantum mechanical principles such as superposition, entanglement, and interference. The review shows that substantial progress has been made in quantum hardware, software, error correction, cloud access, algorithms, and quantum-classical integration. Recent developments have particularly emphasized the transition from noisy physical qubits toward reliable logical qubits and fault-tolerant quantum computation. However, several challenges remain. Decoherence, gate errors, limited coherence time, scalability, quantum error-correction overhead, infrastructure requirements, high development costs, and the difficulty of demonstrating practical quantum advantage continue to limit widespread adoption. The future direction of quantum computing is therefore not simply to build a larger number of qubits. The central objective is to build high-quality, error-corrected logical qubits capable of executing long and useful quantum circuits.

Future quantum systems are expected to combine:

Quantum Processors + Classical Computing + AI + HPC + Quantum Networks

Such systems could eventually provide valuable capabilities in drug discovery, materials science, optimization, cybersecurity, finance, artificial intelligence, and scientific simulation.In conclusion, quantum computing is not yet a universal replacement for classical computing. Rather, it is evolving toward a complementary computational paradigm. The most important milestone for the field will be the transition from experimental quantum processors to reliable, scalable, fault-tolerant systems that demonstrate repeatable and economically meaningful advantages for real-world problems.

REFERENCES

1. Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21, 467–488.
2. Deutsch, D. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London A, 400, 97–117.
3. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124–134.
4. 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.
5. Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.
6. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press.
7. AbuGhanem, M. (2025). IBM quantum computers: evolution, performance, and future directions. The Journal of Supercomputing, 81, Article 687.
8. IBM Quantum. (2025). IBM Quantum Roadmap. IBM Technology Atlas.
9. IBM Quantum. (2026). Quantum Roadmap: Diversify quantum advantage and entangle fault-tolerant modules. IBM Technology Atlas.
10. Google Quantum AI. (2025). Google hardware is powering quantum breakthroughs. Google Research.
11. Microsoft Quantum. (2026). Our Quantum Roadmap. Microsoft Quantum.
12. IBM Quantum. (2025). What is fault-tolerant quantum computing? IBM Quantum Computing.
13. IBM Quantum. (2025). Scaling beyond our roadmap with networked quantum computers. IBM Quantum Computing Blog.
14. Google Quantum AI. (2025). The road to useful quantum computing applications. Google Research.
15. IBM. (2025). 2025 Development & Innovation Roadmap. IBM Quantum.