International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| Volume 6 Issue 4 PP 218-221, 2025
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V6I4P126

Original Article

Quantum Computing: Back to the Future

Susmit Sen
Independent Researcher and Industry Expert.

Received On: 16/10/2025 ***Revised On: 29/10/2025*** ***Accepted On: 20/11/2025*** ***Published On: 12/12/2025***

Abstract *- Quantum computing represents a paradigm shift in computational capabilities, promising to solve complex problems that remain intractable for classical architectures. Tracing its roots from the theoretical propositions of the 1980s to the Noisy Intermediate-Scale Quantum (NISQ) era of the present, the field is rapidly transitioning from academic curiosity to industrial reality. This manuscript explores the historical trajectory of quantum computing, examining foundational milestones such as Shor's and Grover's algorithms. It evaluates the current state of hardware platforms, including superconducting circuits, trapped ions, and photonic systems, highlighting the persistent challenges of decoherence and quantum error correction. Furthermore, the paper analyzes the future trajectory of the technology, focusing on the race toward large-scale fault-tolerant quantum computing (FTQC) and the critical transition to post-quantum cryptography. By synthesizing current roadmaps and industry projections, this study underscores that while significant technical hurdles remain, the realization of scalable quantum advantage will fundamentally disrupt sectors ranging from drug discovery to global cybersecurity.*

Keywords *- Decoherence, Fault-Tolerant Quantum Computing, Post-Quantum Cryptography, Qubits, Quantum Advantage, Quantum Error Correction.*

1. Introduction

The evolution of computing has historically been defined by the miniaturization of classical components, governed by Moore's Law. However, as silicon transistors approach the physical limits of atomic scales, classical computing faces insurmountable barriers in solving specific classes of highly complex problems [1]. Quantum computing offers a profound departure from this classical paradigm by leveraging the fundamental principles of quantum mechanics namely superposition, entanglement, and interference to process information in multidimensional computational spaces.

The conceptual foundation of quantum computing was laid in the early 1980s when physicist Richard Feynman proposed that simulating quantum physical systems would require a computer built on quantum principles [2]. This theoretical vision remained largely abstract until 1994, when Peter Shor introduced a quantum algorithm capable of factoring large integers exponentially faster than any known classical algorithm. Shor's discovery demonstrated that a functional quantum computer could break widely used public-key cryptographic systems, instantly elevating quantum computing from an academic niche to a matter of global strategic importance [3].

Today, the industry resides in the Noisy Intermediate-Scale Quantum (NISQ) era. Current quantum processors possess tens to hundreds of physical qubits but lack the error-correction capabilities necessary for sustained, complex calculations [4]. Despite these limitations, the field is accelerating rapidly. Major technology firms and national research laboratories are executing aggressive roadmaps aimed at achieving fault-tolerant quantum computing (FTQC) by the end of the decade. According to industry analyses, the successful commercialization of quantum technologies could unlock substantial economic value across multiple sectors, including pharmaceuticals, materials science, and financial modeling [5].

This manuscript provides a comprehensive overview of quantum computing, bridging its historical origins with its future trajectory. Section II traces the historical milestones of the field. Section III examines the current landscape of quantum hardware and the challenge of decoherence. Section IV discusses the imperative of quantum error correction. Section V explores the looming impact on cybersecurity and post-quantum cryptography, and Section VI concludes the paper.

2. Historical Foundations

The journey of quantum computing is characterized by punctuated breakthroughs in both theoretical computer science and experimental physics. Table II summarizes the critical milestones that have defined the trajectory of the field.

Table 1: Key Milestones in Quantum Computing History

Milestone	Decade	Significance
Feynman's Proposal	1980s	Conceptualized simulating quantum physics using quantum systems.
Shor's Algorithm	1990s	Demonstrated exponential speedup for integer factorization.
First Quantum Gate	1990s	Physical realization of controlled-NOT gate using trapped ions.

Quantum Supremacy	2010s	Google demonstrated computation impossible for classical supercomputers.
Fault-Tolerant Roadmaps	2020s	Industry focus shifted from NISQ to logical qubits and error correction.

2.1. Theoretical Breakthroughs

Following Feynman's initial proposition, David Deutsch developed the concept of the quantum Turing machine in 1985, proving that a quantum computer could theoretically simulate any physical process [6]. The field gained immense momentum in the 1990s with the introduction of two foundational algorithms. Shor's algorithm (1994) provided an exponential speedup for prime factorization, directly threatening RSA encryption. Shortly after, Lov Grover introduced a quantum search algorithm (1996) that offered a quadratic speedup for searching unstructured databases [7]. These algorithms proved that quantum computers could solve specific, highly valuable problems significantly faster than classical machines.

2.2. The Transition to Hardware

The transition from mathematical theory to physical hardware began in the late 1990s. In 1995, researchers successfully demonstrated the first quantum logic gate using trapped ions [8]. Over the subsequent two decades, various physical systems were explored to isolate and control qubits. The defining moment of the modern era occurred in 2019 when Google announced "quantum supremacy," demonstrating that their 53-qubit Sycamore processor performed a specific sampling calculation in 200 seconds a task that would theoretically take a state-of-the-art classical supercomputer thousands of years to complete [9]. While the practical utility of the specific calculation was limited, it served as an undeniable proof of concept for quantum advantage.

3. Current Hardware Landscape

Unlike classical computing, which universally relies on silicon-based CMOS transistors, the quantum computing industry has not yet converged on a single hardware architecture. Multiple competing modalities are currently being developed in parallel, each with distinct physical characteristics. Table I provides a comparative analysis of the leading hardware platforms.

Table 2: Comparison Of Quantum Hardware Platforms

Hardware Platform	Key Advantages	Primary Challenges
Superconducting Qubits	Fast gate speeds, leverage existing semiconductor manufacturing techniques, scalable 2D arrays.	High susceptibility to noise (decoherence), requires extreme cryogenic cooling.
Trapped Ions	Long coherence times, identical qubits, high-fidelity gate operations.	Slower gate speeds, difficulty scaling to thousands of qubits in a single trap.
Photonic Qubits	Operates at room temperature, excellent for quantum networking and communication.	Difficult to generate deterministic multi-qubit entanglement, high photon loss rates.
Neutral Atoms	Highly scalable in 3D arrays, long coherence, flexible connectivity.	Complex laser control systems required, relatively slow gate operations.

3.1. Superconducting Circuits

Superconducting qubits are currently the most widely adopted platform among major technology companies, including IBM and Google. These systems utilize lithographically printed circuits cooled to near absolute zero (milliKelvin temperatures) to exhibit macroscopic quantum behaviors [10]. The primary advantage of superconducting qubits is their rapid gate execution speeds and their compatibility with existing semiconductor fabrication infrastructure. However, they are highly sensitive to environmental noise, resulting in short coherence times and high error rates.

3.2. Trapped Ions and Neutral Atoms

Trapped ion systems, pioneered by companies like IonQ and Quantinuum, use electromagnetic fields to suspend individual charged atoms in a vacuum. Lasers are then used to manipulate their quantum states. Because all ions of a given isotope are perfectly identical, these systems offer exceptionally long coherence times and high-fidelity operations [11]. However, scaling trapped ion systems to thousands of qubits presents significant engineering challenges regarding laser control and trap design.

Similarly, neutral atom arrays utilize optical tweezers to arrange uncharged atoms in highly scalable two- and three-dimensional grids. This modality has recently shown immense promise for analog quantum simulation and flexible qubit connectivity [12].

4. The Challenge of Error Correction

The fundamental fragility of quantum states remains the greatest barrier to realizing the full potential of quantum computing. Qubits are highly susceptible to decoherence the loss of quantum information due to interactions with the external environment, such as thermal fluctuations, electromagnetic radiation, or cosmic rays [13].

4.1. Physical vs. Logical Qubits

To perform complex algorithms like Shor's, a quantum computer must execute millions of operations without failure. Because physical qubits are inherently noisy, the industry must transition from physical qubits to "logical qubits." A logical qubit is an abstract, error-free qubit created by entangling multiple physical qubits together using Quantum Error Correction (QEC) codes [14].

Historically, QEC schemes like the surface code required a massive overhead, demanding hundreds or

thousands of physical qubits to sustain a single logical qubit. Consequently, building a useful fault-tolerant machine was projected to require millions of physical qubits. However, recent breakthroughs in quantum low-density parity-check (qLDPC) codes have significantly reduced this overhead, accelerating the timeline toward scalable fault tolerance [15].

5. Post-Quantum Cryptography

As the hardware matures, the implications for global cybersecurity become increasingly urgent. Modern digital infrastructure relies heavily on public-key cryptography (e.g., RSA, ECC), which secures everything from secure web browsing (HTTPS) to digital banking and secure communications. These cryptographic protocols are based on mathematical problems that are practically impossible for classical computers to solve, but which a sufficiently large fault-tolerant quantum computer could break efficiently using Shor's algorithm [16].

5.1. The 'Store Now, Decrypt Later' Threat

Although a cryptographically relevant quantum computer (CRQC) does not yet exist, the threat is immediate due to "Store Now, Decrypt Later" (SNDL) attacks. Malicious actors are currently harvesting encrypted, highly sensitive data with the intention of storing it until quantum computers become capable of decrypting it [17]. For data requiring long-term confidentiality such as national security intelligence, intellectual property, and healthcare records the quantum threat is already active.

5.2. Transitioning to Quantum-Safe Standards

In response to this existential threat, the National Institute of Standards and Technology (NIST) initiated a multi-year global effort to evaluate and standardize Post-Quantum Cryptography (PQC) algorithms. These new cryptographic algorithms are designed to be secure against both classical and quantum attacks and can be implemented on existing classical hardware [18].

In mid-2024, NIST released its first finalized PQC standards, marking the beginning of a massive global migration effort. Organizations are now tasked with discovering vulnerable cryptographic assets across their networks and transitioning to these quantum-resistant standards. This cryptographic agility is a critical component of modern IT governance, ensuring that digital trust is maintained as we enter the quantum era [19].

6. Conclusion

Quantum computing is transitioning from a theoretical physics discipline into a mature engineering endeavor. The journey "back to the future" realizing the visions proposed by pioneers over forty years ago is accelerating. While the NISQ era has provided valuable proofs of concept, the ultimate utility of quantum computing hinges on the successful implementation of quantum error correction and the realization of fault-tolerant architectures.

As hardware roadmaps target large-scale logical qubits by the end of the decade, the dual nature of quantum technology becomes apparent. It promises unprecedented computational power to solve humanity's most complex challenges in materials science, optimization, and medicine. Conversely, it presents a profound threat to classical cryptographic infrastructure. The concurrent advancement of fault-tolerant hardware and the global adoption of post-quantum cryptography will define the technological landscape of the coming decade, solidifying quantum computing as the next great frontier of human innovation.

Acknowledgment

The author acknowledges the extensive research contributions of the global quantum physics and computer science communities. Special recognition is extended to the National Institute of Standards and Technology (NIST) for their leadership in post-quantum cryptography standardization, and to the foundational theorists whose work established the principles of quantum computation.

References

[1] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," 10th Anniversary Edition, Cambridge University Press, 2010.

[2] R. P. Feynman, "Simulating Physics with Computers," International Journal of Theoretical Physics, vol. 21, no. 6/7, pp. 467–488, 1982.

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, pp. 124–134.

[4] J. Preskill, "Quantum Computing in the NISQ era and beyond," Quantum, vol. 2, p. 79, 2018.

[5] McKinsey & Company, "Quantum Technology Monitor," April 2024. [Online]. Available: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-monitor.

[6] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 400, no. 1818, pp. 97–117, 1985.

[7] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.

[8] C. Monroe et al., "Demonstration of a Fundamental Quantum Logic Gate," Physical Review Letters, vol. 75, no. 25, pp. 4714–4717, 1995.

[9] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, no. 7779, pp. 505–510, 2019.

[10] M. Kjaergaard et al., "Superconducting Qubits: Current State of Play," Annual Review of Condensed Matter Physics, vol. 11, pp. 369–395, 2020.

[11] C. D. Bruzewicz et al., "Trapped-ion quantum computing: Progress and challenges," Applied Physics Reviews, vol. 6, no. 2, 2019.

[12] M. Morgado and S. Whitlock, "Quantum simulation and computing with Rydberg-interacting qubits," AVS Quantum Science, vol. 8, no. 1, 2021.

[13] W. H. Zurek, "Decoherence, einselection, and the quantum origins of the classical," Reviews of Modern Physics, vol. 75, no. 3, pp. 715–775, 2003.
[14] B. M. Terhal, "Quantum error correction for quantum memories," Reviews of Modern Physics, vol. 87, no. 2, p. 025003, 2015.
[15] S. Bravyi et al., "High-threshold and low-overhead fault-tolerant quantum memory," Nature, vol. 627, pp. 778–782, 2024.
[16] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.
[17] World Economic Forum, "Transitioning to a Quantum-Secure Economy," WEF Insight Report, Sep. 2022.
[18] L. Chen et al., "Report on Post-Quantum Cryptography," National Institute of Standards and Technology, NISTIR 8105, 2016.
[19] NIST, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," August 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.