PEER-REVIEWED JOURNAL OF COMPUTER SCIENCE (PRJCS)

ISSN Online : Open Access Scholarly Journal

Quantum Computing: A Beginner's Guide To Future Processing

Rejina P V

Assistant professor, Co-operative Arts And Science College, Madayi, Pazhayangadi, Kannur, India.

Article information

Received: 12th January 2026
Received in revised form: 19th January 2026
Accepted: 4th February 2026
Available online: 9th February 2026

Volume: 1
Issue: 2
DOI: https://doi.org/10.5281/zenodo.18919206

Abstract

Quantum computing represents a fundamentally different computational paradigm that harnesses quantum mechanical phenomena to process information in ways that classical computers cannot efficiently replicate. This paper provides an accessible introduction to quantum computing for IT professionals and developers seeking to understand the technology's principles, current state, and practical implications. The paper covers the foundational concepts of qubits, superposition, entanglement, and quantum gates, followed by an examination of prominent quantum algorithms and their applications. A comparative analysis of current quantum hardware approaches, including superconducting circuits, trapped ions, and photonic systems, contextualizes the engineering challenges that remain. The paper also addresses the implications of quantum computing for cryptography and outlines the emerging field of post-quantum cryptography. Market analysis and industry investment patterns suggest that while general-purpose quantum advantage remains years away, specific domain applications in chemistry, optimization, and financial modeling are approaching practical viability.

Keywords: Entanglement, Post-quantum cryptography, Quantum algorithms, Quantum computing, Qubits, Superposition

I. INTRODUCTION

Classical computers encode information in binary digits (bits) that exist in one of two states: 0 or 1. Every computation, from simple arithmetic to complex simulations, reduces to operations on these binary values. This model has driven six decades of exponential progress described by Moore's Law, but physical limits on transistor miniaturization and the inherent inefficiency of classical algorithms for certain problem classes have motivated the search for alternative computational paradigms [1].

Quantum computing offers such an alternative. First proposed by Richard Feynman in 1982 and formalized by David Deutsch in 1985, quantum computers exploit the principles of quantum mechanics, specifically superposition, entanglement, and interference, to perform computations that would require exponential time on classical machines [2][3]. The field has progressed from theoretical curiosity to experimental reality, with IBM, Google, and other organizations demonstrating processors exceeding 1,000 qubits [4].

This paper provides a structured introduction to quantum computing intended for IT professionals who need to understand the technology's capabilities, limitations, and timeline without requiring a background in quantum physics.

II. FUNDAMENTAL CONCEPTS

A. Qubits and Superposition

The quantum bit, or qubit, is the fundamental unit of quantum information. Unlike a classical bit, which must be either 0 or 1, a qubit can exist in a superposition of both states simultaneously. Mathematically, the state of a qubit is

described as a linear combination of the basis states |0> and |1>, with complex probability amplitudes that determine the likelihood of measuring each outcome [5]. When measured, the qubit collapses to one of the basis states, but prior to measurement, computations can operate on all superposed states in parallel.

B. Entanglement

Quantum entanglement is a correlation between qubits such that the state of one qubit is directly linked to the state of another, regardless of the physical distance between them. Einstein famously described this as 'spooky action at a distance,' and Bell's theorem later confirmed that entanglement represents a genuinely non-classical phenomenon [6]. In quantum computing, entanglement enables operations on one qubit to instantly influence the state of its entangled partner, providing a mechanism for parallel information processing that has no classical equivalent.

C. Quantum Gates and Circuits

Quantum gates manipulate qubits in a manner analogous to classical logic gates but operate on the continuous probability amplitudes of quantum states. Common gates include the Hadamard gate (which creates superposition), the CNOT gate (which creates entanglement between two qubits), and the Pauli gates (which perform rotations in the qubit state space) [7]. Quantum circuits, composed of sequences of gates applied to qubits, define quantum algorithms.

Table 1. Comparison of Classical and Quantum Computing Concepts

Concept	Classical Computing	Quantum Computing
Basic Unit	Bit (0 or 1)	Qubit (superposition of 0 and 1)
Operations	Logic gates (AND, OR, NOT)	Quantum gates (Hadamard, CNOT, Pauli)
Parallelism	Multiple processors	Superposition and entanglement
Error Handling	Error correction codes	Quantum error correction (overhead)
Memory	Deterministic	Probabilistic until measured

III. QUANTUM HARDWARE APPROACHES

Several physical implementations of qubits are under active development, each with distinct advantages and engineering challenges. The three most advanced approaches are superconducting circuits, trapped ions, and photonic systems.

A. Superconducting Qubits

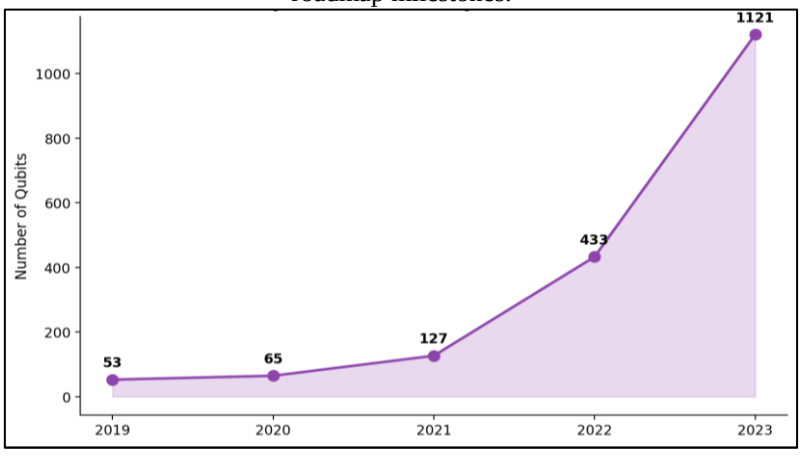
Superconducting qubits, used by IBM and Google, encode quantum information in the energy states of circuits cooled to approximately 15 millikelvin, colder than outer space. These qubits operate at nanosecond gate speeds, enabling rapid computation, but suffer from relatively short coherence times, the duration for which quantum information is preserved before environmental noise corrupts it [8]. IBM's roadmap envisions scaling to significantly larger qubit counts through modular architectures in the coming decade through modular architectures that link multiple processor chips.

B. Trapped Ion Qubits

Trapped ion systems, developed by companies including IonQ and Quantinuum, use individual atoms suspended in electromagnetic fields as qubits. Trapped ions offer significantly longer coherence times and higher gate fidelities than superconducting systems, but their gate operations are slower, operating on microsecond timescales [9]. The ability to achieve all-to-all qubit connectivity, where any qubit can directly interact with any other, reduces the circuit depth required for many algorithms.

C. Photonic Qubits

Figure. 1. IBM quantum processor qubit count progression, 2019-2023 [4]. Qubit counts based on published IBM roadmap milestones.



Photonic quantum computers, pursued by Xanadu and PsiQuantum, encode information in properties of light particles (photons). Photonic systems operate at room temperature, eliminating the extreme cooling requirements of superconducting systems, and are well-suited to quantum networking applications [10]. However, creating deterministic interactions between photons, which naturally do not interact with each other, remains an engineering challenge.

IV. Key Quantum Algorithms

The practical value of quantum computing depends on algorithms that exploit quantum properties to outperform classical approaches. Several foundational algorithms have been identified, though their practical implementation requires hardware capabilities that are still under development.

A. Shor's Algorithm

Peter Shor's 1994 algorithm for integer factorization demonstrated that a sufficiently large quantum computer could break RSA encryption by factoring the large prime products on which it depends in polynomial time, compared to the sub-exponential time required by the best known classical algorithms [11]. This result is the primary driver behind the development of post-quantum cryptography standards.

B. Grover's Algorithm

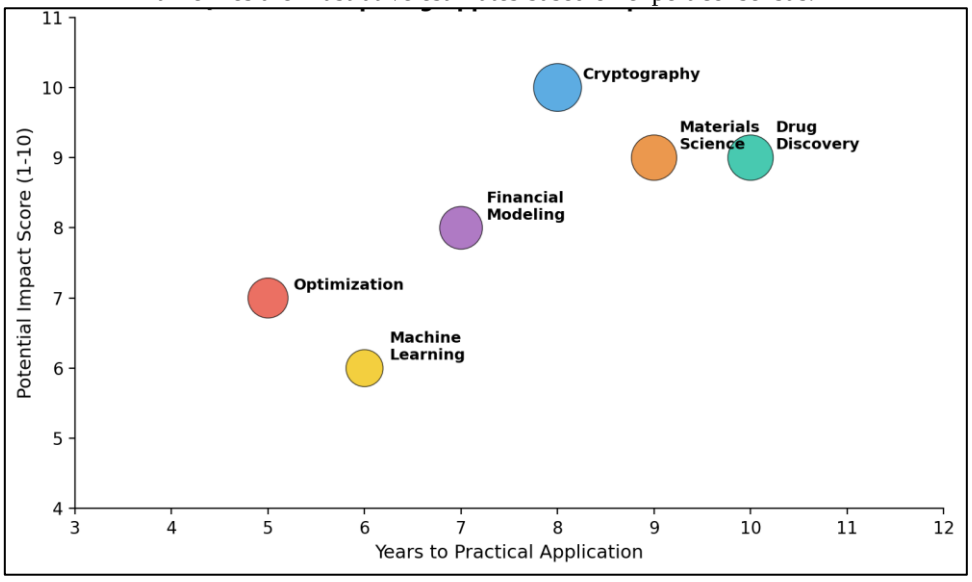
Lov Grover's 1996 search algorithm provides a quadratic speedup for unstructured search problems, reducing the number of queries required to find a target item in an unsorted database from N to the square root of N [12]. While less dramatic than Shor's exponential speedup, Grover's algorithm has broad applicability to optimization and constraint satisfaction problems.

C. Variational Quantum Eigensolver (VQE)

VQE is a hybrid quantum-classical algorithm designed for near-term quantum hardware. It uses a quantum processor to prepare and measure quantum states while a classical optimizer adjusts parameters to minimize energy functions. VQE has particular relevance to computational chemistry and materials science, where it can simulate molecular properties that are computationally intractable for classical systems [13].

V. APPLICATIONS AND IMPACT

Figure. 2. Quantum computing application areas: potential impact versus estimated timeline [14]. Impact scores and timelines are illustrative estimates based on expert consensus.



Drug discovery and materials science represent the most promising near-term applications for quantum computing. Simulating molecular interactions at the quantum level could accelerate the identification of new pharmaceutical compounds and advanced materials by orders of magnitude compared to classical simulation methods [14]. Financial institutions are exploring quantum algorithms for portfolio optimization, risk assessment, and derivative pricing, where the combinatorial complexity of the problem space aligns with quantum computational strengths [15].

Table 2. Quantum Computing Application Domains and Timeline

Domain	Application	Quantum Advantage	Estimated Timeline
Chemistry	Molecular simulation	Exponential speedup	5-10 years
Cryptography	Code breaking / QKD	Exponential speedup	10-15 years (breaking RSA)
Finance	Portfolio optimization	Quadratic speedup	5-8 years
Logistics	Route optimization	Quadratic speedup	5-7 years
Materials	Catalyst design	Exponential speedup	7-12 years

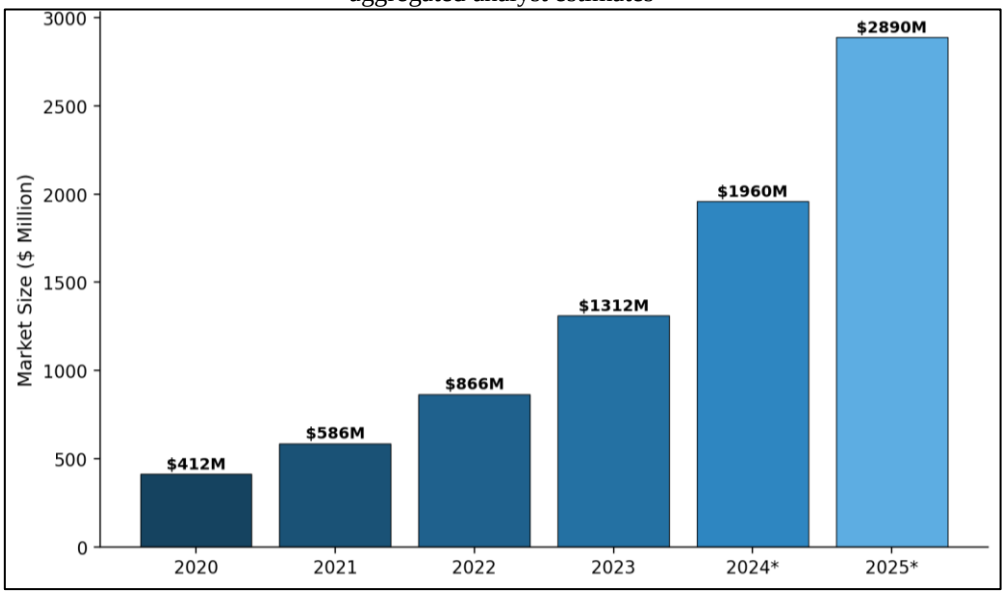
VI. IMPLICATIONS FOR CRYPTOGRAPHY

The threat that quantum computers pose to current cryptographic systems has driven significant investment in post-quantum cryptography (PQC). In 2022, NIST selected four algorithms for standardization: CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures [16]. These algorithms are based on mathematical problems believed to be resistant to both classical and quantum attacks, including lattice-based and hash-based constructions.

Organizations should begin planning for the transition to post-quantum cryptography now, even though large-scale quantum computers capable of breaking current encryption are likely a decade or more away. The 'harvest now, decrypt later' threat model, where adversaries collect encrypted data today intending to decrypt it when quantum computers become available, makes proactive cryptographic migration essential for data with long-term sensitivity [17].

VII. MARKET AND INVESTMENT LANDSCAPE

Figure. 3. Global quantum computing market size and projections [18]. Market projections are illustrative based on aggregated analyst estimates



The quantum computing market has attracted substantial investment from both private and public sectors. Boston Consulting Group estimates that quantum computing could create $450 billion to $850 billion in economic value by 2040 [18]. Government programs in the United States, European Union, China, and Japan have committed billions of dollars to quantum research infrastructure. Cloud-based quantum computing services from IBM, Amazon, Microsoft, and Google allow organizations to experiment with quantum algorithms without investing in specialized hardware.

VIII. CONCLUSION

Quantum computing stands at an inflection point between scientific demonstration and practical utility. The fundamental principles of superposition, entanglement, and quantum interference enable computational approaches that are provably beyond the reach of classical systems for specific problem classes. While current hardware remains limited by qubit counts, error rates, and coherence times, the pace of progress, from 53 qubits in 2019 to over 1,000 in 2023, indicates that practically useful quantum computers are approaching. IT professionals should familiarize themselves with quantum concepts, monitor developments in post-quantum cryptography, and identify problems within their domains that may benefit from quantum computational approaches as the technology matures.

References

[1] M. M. Waldrop, "The Chips Are Down for Moore's Law," Nature, vol. 530, pp. 144-147, Feb. 2016.
[2] R. P. Feynman, "Simulating Physics with Computers," International Journal of Theoretical Physics, vol. 21, no. 6-7, pp. 467-488, Jun. 1982.
[3] D. Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," Proc. Royal Society of London A, vol. 400, pp. 97-117, 1985.
[4] IBM, "IBM Quantum Development Roadmap," IBM Research, Yorktown Heights, NY, USA, 2023.
[5] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," 10th Anniversary ed. Cambridge, UK: Cambridge University Press, 2010.
[6] J. S. Bell, "On the Einstein Podolsky Rosen Paradox," Physics Physique Fizika, vol. 1, no. 3, pp. 195-200, 1964.
[7] E. Rieffel and W. Polak, "Quantum Computing: A Gentle Introduction," Cambridge, MA, USA: MIT Press, 2011.
[8] F. Arute et al., "Quantum Supremacy Using a Programmable Superconducting Processor," Nature, vol. 574, pp. 505-510, Oct. 2019.

[9] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, "Trapped-Ion Quantum Computing: Progress and Challenges," Applied Physics Reviews, vol. 6, no. 2, 2019.
[10] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated Photonic Quantum Technologies," Nature Photonics, vol. 14, pp. 273-284, 2020.
[11] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in Proc. 35th Annual Symp. Foundations of Computer Science, IEEE, 1994, pp. 124-134.
[12] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in Proc. 28th ACM Symp. Theory of Computing, 1996, pp. 212-219.
[13] A. Peruzzo et al., "A Variational Eigenvalue Solver on a Photonic Quantum Processor," Nature Communications, vol. 5, p. 4213, Jul. 2014.
[14] McKinsey & Company, "Quantum Technology Monitor," McKinsey Digital, New York, NY, USA, 2023.
[15] S. Orus, S. Mugel, and E. Lizaso, "Quantum Computing for Finance: Overview and Prospects," Reviews in Physics, vol. 4, p. 100028, 2019.
[16] NIST, "Post-Quantum Cryptography: Selected Algorithms 2022," National Institute of Standards and Technology, Gaithersburg, MD, USA, 2022.
[17] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, Sep./Oct. 2018.
[18] Boston Consulting Group, "The Next Decade in Quantum Computing and How to Play," BCG Henderson Institute, Boston, MA, USA, 2023.