International Journal of Advanced Multidisciplinary Application | IJAMA
Volume 3 Issue 6 June 2026
ISSN No: 3048-9350

Quantum Computing The Next Technological Frontier and Its Impact on Science, Security, and Society

Lalika Singh
Centre for Quantum Technologies

Abstract
Quantum computing represents one of the most profound technological transitions in human history — a shift from the binary logic of classical computation to the probabilistic, superposition-driven mechanics of quantum physics. Where a classical bit must be either 0 or 1, a qubit can exist in both states simultaneously, and entangled qubits can encode exponentially more information than their classical equivalents. After decades of theoretical promise, quantum hardware has entered a phase of rapid, measurable progress: qubit counts are doubling annually, error rates are falling toward fault-tolerance thresholds, and the first demonstrations of "quantum advantage" — the ability of quantum systems to outperform the best classical supercomputers on specific tasks — have been achieved. This article provides a comprehensive overview of quantum computing principles, hardware modalities, applications across industry and science, global investment dynamics, and the profound implications for cryptography and national security.

1. From Classical to Quantum: A Fundamental Shift

The computers that underpin modern civilization — from smartphones to supercomputers — all operate on the same fundamental principle articulated by Alan Turing in 1936: information is encoded in binary bits (0s and 1s), and computation proceeds through deterministic logical operations on those bits. This architecture, refined over eight decades into the transistor-dense microprocessors of today, has delivered extraordinary advances, driving Moore's Law and the exponential growth of digital capability that defines the modern era.

Yet classical computing faces fundamental physical limits. Transistors are approaching atomic scale — Intel's latest process nodes place transistors just 2 nanometres apart, a distance of roughly 10 silicon atoms. Quantum tunnelling effects at this scale cause electrons to leak through transistor walls, generating heat and errors. The era of classical scaling is not over, but its pace is slowing, and for certain categories of problem — those involving the simulation of quantum systems, optimisation across vast search spaces, and cryptographic operations — even the most powerful classical supercomputers are fundamentally inadequate.

Quantum computing offers a fundamentally different approach. By exploiting the quantum mechanical phenomena of superposition, entanglement, and interference, quantum computers can in principle solve certain classes of problems exponentially faster than any conceivable classical system. The operative word is "certain": quantum computers are not universally faster. They are, rather, profoundly better for specific problem types that happen to include some of the most consequential computational challenges in science, security, and industry.

2. The Hardware Landscape: Building a Qubit

2.1 Competing Physical Implementations

The central engineering challenge of quantum computing is building qubits that are simultaneously well-isolated from environmental noise (which causes "decoherence" — the collapse of quantum states) and precisely controllable for computation. No single hardware approach has yet emerged as definitively superior, and a vibrant competition among several physical modalities is underway.

Superconducting qubits, pioneered by IBM, Google, and Rigetti, use tiny circuits of superconducting material cooled to temperatures near absolute zero (approximately 15 millikelvin — colder than deep space). Operations are performed

by microwave pulses applied to the circuit. This approach currently leads in qubit count and has produced the most celebrated demonstrations of quantum advantage. Trapped-ion systems, developed by IonQ, Quantinuum, and others, use individual atomic ions suspended in electromagnetic fields as qubits, manipulated by precisely tuned laser pulses. Trapped-ion qubits offer lower intrinsic error rates and longer coherence times than superconducting qubits, but are currently more difficult to scale.

Photonic quantum computers use individual photons — particles of light — as qubits, offering room-temperature operation and natural compatibility with optical telecommunications infrastructure. Neutral atom platforms, recently commercialised by companies such as QuEra and Pasqal, trap thousands of neutral atoms in programmable arrays using laser "tweezers" — a highly scalable approach that attracted significant attention following landmark results in 2023–2025. Topological qubits, the long-term ambition of Microsoft's quantum programme, encode information in the non-local properties of exotic quasiparticles called Majorana fermions, theoretically offering inherent protection against decoherence — though experimental demonstration remains elusive.

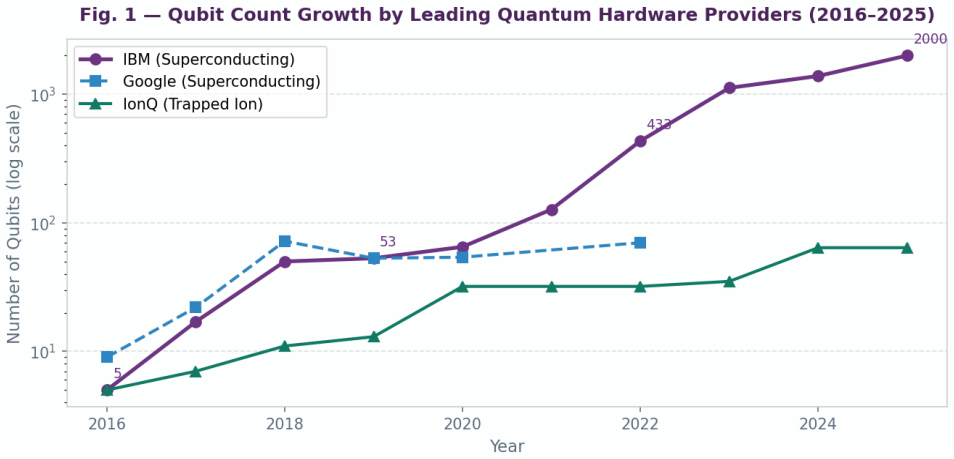

Fig. 1 — Qubit count growth by leading quantum hardware providers (2016–2025, logarithmic scale). IBM's superconducting platform has led in absolute qubit count, while trapped-ion systems have demonstrated superior qubit quality metrics. Source: Company disclosures, Nature, Science.

2.2 The Error Problem and the Road to Fault Tolerance

The most significant obstacle between today's "noisy intermediate-scale quantum" (NISQ) devices and practically useful quantum computers is error. Quantum gates — the operations that manipulate qubits — are imperfect, and qubits are fragile: they decohere due to thermal fluctuations, electromagnetic interference, and manufacturing imperfections. Current two-qubit gate error rates across leading hardware platforms range from 0.07% to 0.5% — far too high for the sustained, complex computations required for most commercially valuable applications.

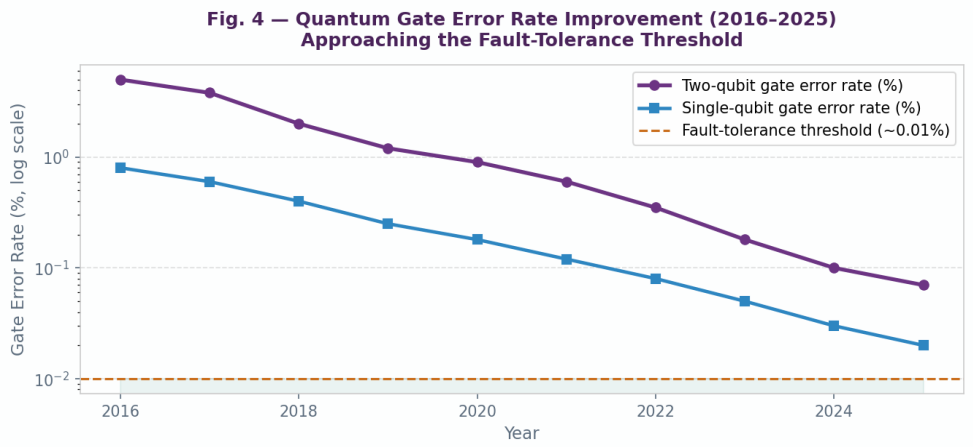

Fig. 4 — Quantum gate error rate improvement across leading hardware platforms (2016–2025, logarithmic scale). Two-qubit gate errors have fallen by roughly two orders of magnitude over a decade. The dashed orange line indicates the approximate fault-tolerance threshold (~0.01%), below which quantum error correction becomes sustainable. Source: IBM Research, Google Quantum AI, IonQ, academic literature.

Achieving fault-tolerant quantum computation requires quantum error correction (QEC) — encoding logical qubits across many physical qubits so that errors can be detected and corrected without directly measuring (and thus collapsing) the quantum state. The leading error correction code, the surface code, requires approximately 1,000 physical qubits per logical qubit to achieve error rates suitable for general computation. A fault-tolerant machine capable of running Shor's algorithm against RSA-2048 encryption would require an estimated 4,000 logical qubits — or roughly 4 million well-controlled physical qubits.

The distance between today's best devices (IBM's 2025 Heron processor at ~2,000 qubits, Google's Willow at 105 qubits with record error rates) and this target is substantial — but the trajectory of progress, as illustrated in Figure 1, suggests the gap is narrowing at a pace that would have seemed implausible five years ago.

3. Quantum Advantage: What Can Quantum Computers Actually Do?

The term "quantum advantage" (sometimes "quantum supremacy") refers to the demonstration that a quantum computer can solve a specific problem faster than any classical computer. Google's 2019 Sycamore experiment claimed quantum supremacy by completing a random circuit sampling task in 200 seconds that it estimated would take a classical supercomputer 10,000 years. Subsequent classical algorithmic improvements have partially revised that gap — but the principle of quantum advantage for certain problem classes is now firmly established.

The more consequential question for society is not whether quantum computers can win contrived speed competitions, but which practically important problems they will be able to solve better than classical systems — and when.

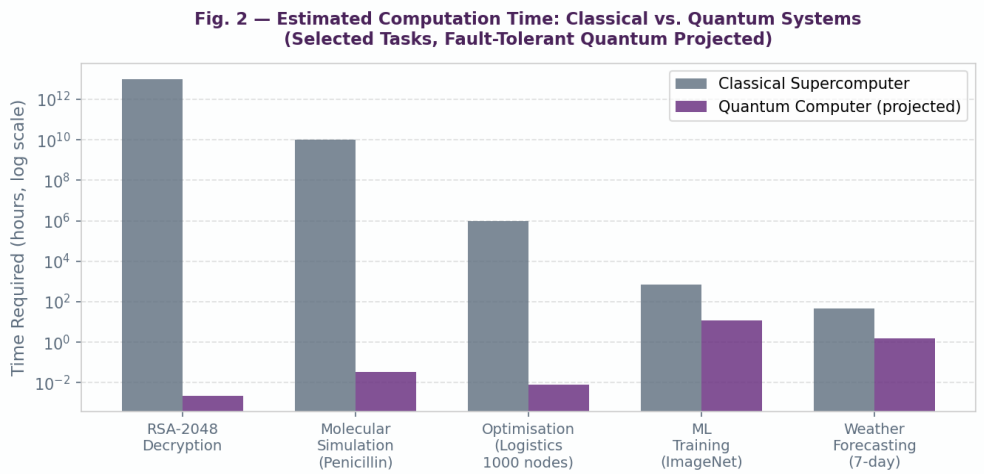

Fig. 2 — Estimated computation time comparison for selected tasks: classical supercomputer vs. projected fault-tolerant quantum computer (logarithmic scale). The quantum advantage is most dramatic for problems involving molecular simulation and cryptography. Note: Quantum projections assume fault-tolerant systems not yet available; timelines are indicative. Source: IBM Research, MIT Lincoln Laboratory, McKinsey Quantum Technology Report 2025.

3.1 Quantum Chemistry and Materials Discovery

Simulating the quantum mechanical behaviour of molecules and materials is perhaps the most natural — and most commercially valuable — application of quantum computing. Classical computers are fundamentally limited in their ability to simulate quantum systems: the computational resources required grow exponentially with the number of electrons involved. A molecule with 50 electrons in superposition requires a classical simulation of 2^{50} states — approximately 10^{15} — rapidly becoming intractable. A quantum computer, by contrast, can simulate quantum systems directly and efficiently. Applications include the design of new catalysts for industrial chemical processes (the Haber-Bosch ammonia synthesis process alone consumes 1–2% of global energy; quantum-optimised catalysts could dramatically reduce this), the simulation of high-temperature superconductors, the discovery of novel battery materials, and the rational design of pharmaceuticals that target specific protein binding sites with atomic precision.

3.2 Optimisation

Many of the most economically important computational problems are optimisation problems: finding the best solution among an astronomically large number of possibilities. The travelling salesman problem, portfolio optimisation, supply chain logistics, drug candidate screening, financial derivatives pricing, and machine learning training all involve searching vast solution spaces. Quantum algorithms — including the Quantum Approximate Optimisation Algorithm (QAOA) and quantum annealing — offer potential speedups for certain classes of these problems, though the practical advantage over the best classical methods remains an active area of research.

4. The Cryptographic Threat: Quantum and Cybersecurity

The most immediately alarming implication of quantum computing for society is its potential to break the cryptographic systems that protect virtually all digital communication, commerce, and infrastructure. Public-key cryptography — the foundation of HTTPS, digital signatures, banking transactions, and secure email — relies on the mathematical difficulty of certain problems for classical computers: factoring large numbers (RSA) and computing discrete logarithms (elliptic curve cryptography).

Peter Shor's 1994 algorithm demonstrated that a sufficiently powerful quantum computer could solve both problems in polynomial time — effectively destroying the security assumptions underpinning RSA and ECC. While a cryptographically relevant quantum computer does not yet exist, the "harvest now, decrypt later" (HNDL) threat is

already active: adversarial actors are collecting encrypted communications today with the intention of decrypting them once capable quantum hardware becomes available. For data with long-term sensitivity — state secrets, medical records, financial data — the threat timeline is measured in years to decades, not generations.

5. Global Investment and the Quantum Race

Quantum computing has become a technology of explicit strategic priority for governments worldwide, driven by its implications for national security, economic competitiveness, and scientific leadership. The scale of public investment is extraordinary, with China's announced government commitment of approximately $15 billion representing the largest single national quantum programme in history.

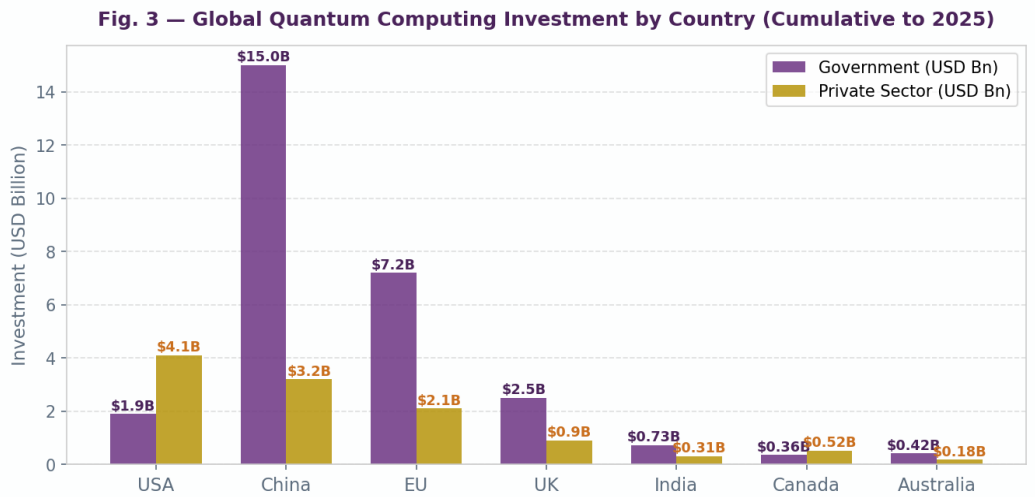

Fig. 3 — Cumulative quantum computing investment by government and private sector, by country/region (to 2025, USD billion). China's government investment dwarfs all others; the United States leads in private sector investment. Source: McKinsey Global Institute, Pitchbook, national government disclosures.

Private sector investment has been equally dramatic. Venture capital and corporate investment in quantum technology companies exceeded $2.4 billion in 2024 alone, with significant rounds raised by IonQ, PsiQuantum, Quantinuum, QuEra, and a new generation of quantum software and algorithm companies. IBM's ten-year, $3 billion quantum investment programme — combined with its open-access IBM Quantum Network — has established it as the world's leading platform for quantum exploration, with over 500,000 registered users running experiments on its cloud-accessible quantum systems.

Country / Region	Govt. Investment	Private Investment	Key Institutions
China	$15.0B	$3.2B	Alibaba DAMO, Baidu, CAS
European Union	$7.2B	$2.1B	Quantum Flagship, Fraunhofer
United States	$1.9B	$4.1B	IBM, Google, IonQ, NIST
United Kingdom	$2.5B	$0.9B	NQCC, Oxford, Cambridge
India	$0.73B	$0.31B	IISc, TIFR, TCS Research

Canada	$0.36B	$0.52B	D-Wave, Xanadu, Perimeter Inst.

Table 1 — Quantum computing investment by country/region (cumulative to 2025). Sources: McKinsey, Pitchbook, national government disclosures.

6. Applications Across Industry Sectors

The potential impact of quantum computing is not confined to any single domain. Expert assessments of quantum advantage potential vary by sector, but the breadth of application is striking — reflecting the fact that quantum speedups apply to mathematical problem classes that appear across many industries.

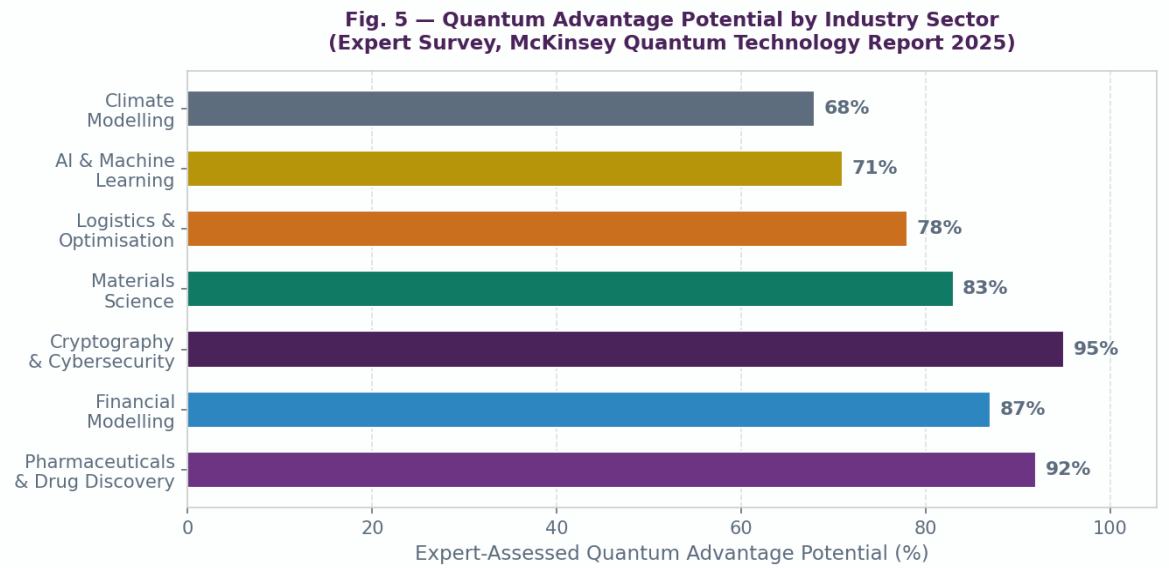

Fig. 5 — Quantum advantage potential by industry sector, based on expert assessment of problem structure alignment with known quantum algorithms. Cryptography and pharmaceuticals rank highest due to the direct applicability of Shor's and simulation algorithms respectively. Source: McKinsey Quantum Technology Report 2025.

6.1 Pharmaceuticals and Drug Discovery

The pharmaceutical industry faces a productivity crisis: the average cost to bring a new drug to market has risen to over $2.6 billion, and failure rates in late-stage clinical trials remain near 90% for oncology. Quantum simulation of molecular interactions at the electronic structure level — impossible for classical computers beyond molecules of modest size — could transform early-stage drug discovery by enabling accurate prediction of binding affinities, toxicity profiles, and metabolic pathways before any wet-lab experiment is conducted.

Companies including Roche, Pfizer, and Merck have active quantum computing research partnerships, and startups such as ProteinQure and Menten AI are developing quantum-native approaches to protein engineering and drug design. The near-term focus is on hybrid classical-quantum algorithms that can run on current NISQ hardware; fault-tolerant systems will eventually enable full quantum simulation of drug-target interactions.

6.2 Financial Services

Financial applications of quantum computing include portfolio optimisation (finding the ideal allocation of assets across thousands of securities subject to complex constraints), derivatives pricing (evaluating path-dependent financial instruments whose value depends on the evolution of underlying assets), risk analysis (Monte Carlo simulations for Value-at-Risk and stress testing), and fraud detection. JPMorgan Chase, Goldman Sachs, and HSBC all have active

quantum research programmes, with JPMorgan publishing quantum algorithms for option pricing and portfolio optimisation that demonstrate theoretical speedups over classical Monte Carlo methods.

7. The Quantum Software and Algorithm Stack

Hardware is only half of the quantum computing story. Realising the potential of quantum processors requires a rich ecosystem of quantum software: programming languages and frameworks, compilers that translate high-level quantum programs into hardware-specific gate operations, error mitigation techniques that extract useful signal from noisy NISQ devices, and a library of quantum algorithms proven to provide advantage over classical methods.

The quantum software landscape has matured significantly. Key quantum programming frameworks include:

- Qiskit (IBM): The most widely adopted open-source quantum computing framework, with over 500,000 registered users, providing tools for circuit construction, transpilation, noise simulation, and cloud execution on IBM Quantum hardware.
- Cirq (Google): Google's open-source framework, optimised for near-term quantum algorithms and tightly integrated with Google's quantum hardware through the Quantum Computing Service.
- PennyLane (Xanadu): A cross-platform library specialising in quantum machine learning and variational quantum algorithms, with automatic differentiation support enabling integration with PyTorch and TensorFlow.
- Amazon Braket and Azure Quantum: Cloud platforms aggregating access to multiple quantum hardware providers (IonQ, Quantinuum, Rigetti, OQC) behind unified APIs, lowering the barrier to quantum experimentation for enterprises.

The dominant near-term algorithmic paradigm is the Variational Quantum Eigensolver (VQE) and the Quantum Approximate Optimisation Algorithm (QAOA) — hybrid classical-quantum approaches that use parameterised quantum circuits optimised by classical gradient descent. These algorithms are designed to extract value from current, noisy hardware by keeping quantum circuit depths short (limiting error accumulation) while delegating optimisation to classical co-processors.

8. Ethical, Regulatory, and Societal Considerations

8.1 Equity and Access

The quantum computing revolution, like previous waves of technological transformation, carries risks of exacerbating existing inequalities. Access to quantum hardware is currently concentrated among well-funded research institutions and large technology companies in a small number of wealthy nations. If the economic benefits of quantum advantage — in drug discovery, financial optimisation, and materials science — accrue primarily to entities in these nations, the technology could deepen global inequality rather than alleviate it.

Cloud-based quantum access, pioneered by IBM Quantum and now offered by Amazon, Microsoft, and Google, represents one pathway to broader participation. The availability of high-quality quantum simulators — classical software that mimics small quantum systems — has been equally important in enabling researchers and students in lower-resource environments to develop quantum expertise without access to physical hardware.

8.2 National Security and Export Controls

Quantum computing's cryptographic implications have elevated it to a matter of explicit national security concern. The United States has imposed export controls on quantum computing components under the Export Administration Regulations (EAR), restricting the transfer of advanced quantum hardware and certain software tools to adversarial nations. The rapidly expanding capabilities of Chinese quantum research — including world-leading achievements in quantum communication and quantum key distribution — have intensified concerns about the strategic implications of quantum technology leadership.

International governance frameworks for quantum technology remain nascent. Unlike nuclear or biological weapons, quantum computers are dual-use technologies — the same hardware that could break encryption also accelerates drug discovery and materials science. Establishing norms for responsible quantum development and deployment, analogous to existing frameworks for AI governance or cybersecurity, is an urgent task for the international community.

9. Conclusion

Quantum computing is no longer a purely theoretical enterprise. The hardware is advancing at a pace that regularly surprises even the most optimistic experts. Qubit counts are growing exponentially, error rates are declining toward the fault-tolerance threshold, and the first genuinely useful quantum applications are beginning to emerge in chemistry simulation, optimisation, and machine learning. The question is no longer whether quantum computers will be transformative, but how rapidly the transition from NISQ-era exploration to fault-tolerant utility will occur, and who will shape its trajectory. For organisations in every sector, the implication is clear: quantum literacy is no longer optional. Understanding which problems in one's domain are structurally amenable to quantum speedup, monitoring the hardware trajectory, participating in early algorithmic experimentation, and — most urgently — beginning the migration to post-quantum cryptographic standards are all actions that responsible leadership demands today, not when fault-tolerant machines arrive.

The history of computing teaches us that the most consequential technologies are routinely underestimated in their early years and overestimated in the short term. Quantum computing, after decades of residing in the "overestimated" category, is now unambiguously entering the era of real-world consequence. The institutions, nations, and researchers that understand this transition earliest — and engage with it most seriously — will be best positioned to shape the extraordinary possibilities, and navigate the profound challenges, that lie ahead.

References

1. Arute, F. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574, 505–510.
2. Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of 35th Annual Symposium on FOCS. IEEE.
3. McKinsey & Company (2025). Quantum Technology Monitor 2025. McKinsey Global Institute.
4. NIST (2024). Post-Quantum Cryptography Standards: FIPS 203, 204, 205. National Institute of Standards and Technology.
5. Preskill, J. (2018). Quantum Computing in the NISQ Era and Beyond. Quantum, 2, 79.
6. IBM Research (2025). IBM Quantum Development Roadmap 2025–2033. IBM Corporation.
7. Bova, F., Goldfarb, A., & Melko, R.G. (2021). Commercial applications of quantum computing. EPJ Quantum Technology, 8, 2.
8. Google Quantum AI (2024). Quantum error correction below the surface code threshold. Nature, 638, 920–926.