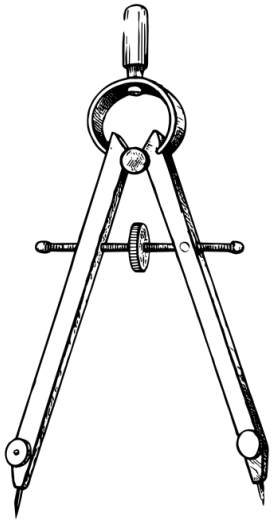

ARTELLICO

Quantum Computing

Foundations, Challenges, and Strategic Implications

Information Dossier

Alexander Pokorny
CEO, Entrepreneur, Lecturer

https://artellico.co

Version 1.0 • March 2026

This is not Policy — this is Mathematics.

Paradigm shift

Beyond Binary Certainties

Classical computer science has operated for over seven decades on an elegant foundation: the bit. Every computation, every decision, every encryption reduces to a sequence of zeros and ones. This architecture has transformed civilizations—and is now approaching fundamental limits. Quantum computing does not break with this tradition; it extends it into a dimension that challenges our intuition.

A classical computer processes information sequentially or in parallel, but always deterministically: each bit occupies a defined state at every moment. A quantum computer, by contrast, exploits the laws of quantum mechanics to encode information in states that collapse only upon measurement. This is not a technical detail—it is an ontological rupture.

\Qubit = superposition of two basis states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

The Qubit: Anatomy of Quantum Information

While a classical bit assumes exactly one of two states—0 or 1—a qubit exists in a superposition of both states simultaneously. Mathematically, this is described by a state vector in a two-dimensional Hilbert space: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex amplitudes whose squared magnitudes sum to unity.

Crucially, superposition is not an expression of ignorance. The qubit is not "either in 0 or 1, and we simply don't know which." It is demonstrably in both states simultaneously. Only measurement forces collapse into one of the basis states. This phenomenon, together with entanglement and interference, forms the physical foundation for the superiority of quantum algorithms.

Entanglement means that the state of one qubit is instantaneously correlated with the state of another—regardless of spatial distance. Einstein called this "spooky action at a distance," yet it has since been experimentally confirmed thousands of times and forms the backbone of quantum protocols.

Exponential vs. polynomial complexity

Classical and Quantum Computing Compared

The fundamental difference lies not in speed but in the complexity class of solvable problems. A classical computer with n bits can represent exactly one of 2^n states. A quantum computer with n qubits can simultaneously manipulate a

superposition of all 2^n states. This enables algorithmic shortcuts that are classically impossible.

Shor's algorithm factorizes large integers in polynomial time—a problem classically considered exponentially hard and the basis of RSA encryption. Grover's algorithm searches unsorted databases with quadratic speedup. These algorithms are not theoretical curiosities; they redefine the boundaries of what is computable.

Nevertheless, quantum computing is not a universal replacement. For the vast majority of everyday computing tasks—word processing, database queries, web applications—quantum computers offer no advantage. Their strength lies in specific problem classes: optimization, simulation of quantum-mechanical systems, cryptographic operations, and certain forms of machine learning.

Technological Challenges: Cooling, Coherence, Error Correction

10–15 millikelvin: colder than outer space

The greatest technical hurdle in quantum computing is decoherence: the tendency of qubits to lose their quantum properties through interaction with the environment. Superconducting qubits—the currently dominant technology, employed by IBM, Google, and Rigetti—must be cooled to temperatures near absolute zero: typically 10 to 15 millikelvin, achieved through multi-stage dilution refrigeration systems.

This cooling is energy-intensive and mechanically complex. A single quantum computer requires infrastructure resembling a large physics laboratory rather than a data center. Coherence times—the duration for which a qubit retains its quantum information—range from microseconds to milliseconds in superconducting systems. Every computation must be completed within this window.

Quantum error correction addresses this problem through redundancy: hundreds of physical qubits are combined into a single logical qubit that can tolerate errors. This means, however, that a practical quantum computer with a thousand logical qubits might physically require millions of qubits—a scale that currently remains out of reach.

Neutral-Atom Quantum Computers: An Alternative Architecture

Optical tweezers trap individual atoms

Alongside superconducting systems, neutral-atom quantum computers have emerged as a promising alternative. Companies like QuEra, Pasqal, and Atom Computing use individual neutral atoms—typically rubidium or cesium—trapped and manipulated by highly focused laser beams (optical tweezers) in two-dimensional or three-dimensional arrays.

The decisive advantage of this architecture lies in scalability. While superconducting qubits must be individually fabricated on chips, neutral-atom systems can simultaneously produce hundreds to thousands of identical qubits. The atoms are inherently identical—a rubidium atom is physically indistinguishable from any other—which eliminates manufacturing variability.

Moreover, Rydberg interactions—long-range couplings between highly excited atomic states—enable a flexible connectivity structure between qubits that is not restricted to physically adjacent qubits. This is a significant advantage over superconducting architectures, whose connectivity is limited by physical chip topology.

Topological Superconductors: The Dream of Error-Resistant Qubits

Majorana fermions as error-resistant qubits

The most elegant but also most ambitious strategy for overcoming decoherence comes from topological quantum mechanics. Topological superconductors—materials whose quantum states are protected by global geometric properties rather than local parameters—promise inherently error-resistant qubits.

The key concept is Majorana fermions: exotic quasiparticles that arise at the ends of topological superconductor wires, whose quantum information is not stored locally but delocalized across the entire structure. Perturbations acting only locally cannot destroy this information—a natural protection against decoherence.

Microsoft pursues this approach with its Majorana 1 program, which demonstrated a functional topological qubit in February 2025. However, the technology remains in an early stage. The experimental fabrication of reliable Majorana states is extraordinarily demanding, and the path from individual topological qubits to scalable systems is still long. Nevertheless, should this approach succeed, it would drastically reduce error correction overhead and fundamentally transform quantum computing.

Application Domains: Where Quantum Computing Creates Impact

From pharma to financial markets

The most promising application areas lie where classical computers fail due to combinatorial explosion. In pharmaceutical research, quantum simulation of molecular interactions accelerates drug development: protein structures, binding energies, and reaction pathways can be modeled directly at the quantum level rather than classically approximated.

In materials science, quantum simulators open the possibility of predicting novel materials—high-temperature superconductors, more efficient catalysts, higher-performance battery chemistries—before they are synthesized. In finance, quantum algorithms promise advantages in portfolio optimization, risk modeling, and pricing of complex derivatives.

Optimization problems in logistics and supply chain management, traffic flow control, and network design are likewise candidates for quantum advantage. Caution is warranted, however: proof of genuine quantum advantage—superiority over the best classical algorithms on real, economically relevant problem instances—remains outstanding for most of these application domains.

Energy Implications: A Double-Edged Sword

Energy paradox: fewer operations, more cooling

The energy balance of quantum computers is paradoxical. On one hand, quantum algorithms promise to perform certain computations with exponentially fewer operations than classical methods—theoretically implying a dramatic efficiency gain. On the other hand, operating current quantum computers is extremely energy-intensive.

A dilution refrigeration system for superconducting qubits typically consumes 15 to 25 kilowatts continuously—for cooling alone. Add control electronics, signal processing, and the classical co-processors that manage the quantum chip, and the total energy consumption of a quantum computing system exceeds that of a comparable classical HPC node by a significant multiple.

In the long term, however, quantum computers could make an indirect but profound contribution to energy efficiency: through simulation and optimization of materials for more efficient solar cells, batteries, and catalysts; through optimization of energy grids and logistics chains; and through accelerating research on fusion reactors. The question is not whether quantum

computers themselves consume little energy, but whether the insights they enable can transform the energy consumption of entire industries.

Quantum Computing and Cryptography: The Erosion of Classical Security

Harvest now, decrypt later

The cryptographic implications of quantum computing are perhaps the most immediate. Shor's algorithm threatens the security of asymmetric encryption schemes such as RSA, DSA, and ECC—schemes that carry the entire digital trust system of the internet: TLS certificates, digital signatures, secure communications.

The threat is not abstract. Intelligence organizations are presumably already conducting so-called "harvest now, decrypt later" strategies: intercepting and storing encrypted communications in the expectation of decrypting them with future quantum computers. For data with long secrecy horizons—diplomatic communications, medical records, trade secrets—this is a real, present-day threat.

The cryptographic response is twofold. First, post-quantum cryptography (PQC): algorithms that run on classical computers but resist quantum attacks. NIST finalized the first PQC standards in 2024 (FIPS 203–205). Second, Quantum Key Distribution (QKD), which uses quantum-mechanical principles to enable physically secure key distribution. Both approaches are complementary, not alternative.

Quantum Computing and Artificial Intelligence

Quantum Machine Learning: potential and skepticism

The intersection of quantum computing and artificial intelligence is the subject of intense research—and equally intense exaggeration. Theoretically, quantum computers could accelerate certain sub-problems of machine learning: solving linear systems of equations (HHL algorithm), optimizing loss functions, searching high-dimensional parameter spaces.

Quantum Machine Learning (QML) explores variational circuits as parameterized models—so-called Quantum Neural Networks—trained by classical optimizers. Initial results show advantages on small-scale problems, but scalability to industrially relevant datasets remains unclear. The fundamental bottleneck is data input and output: classical data must be encoded into quantum states and results read out classically—a bottleneck that can negate potential quantum advantages.

More realistic is the deployment of quantum computers for specific optimization problems within AI pipelines: optimizing molecular candidates in drug discovery, solving combinatorial allocation problems, or efficiently searching graph-based structures. The revolution lies not in quantum computers training LLMs—they foreseeably will not—but in solving problems that classical AI needs as input or context.

Outlook: Between Hype and Physics

NISQ → FT-QC: a decade?

Quantum computing is in the so-called NISQ era (Noisy Intermediate-Scale Quantum): devices with dozens to a few thousand noisy qubits that may be useful for specific tasks but do not yet operate with error correction. The transition to fault-tolerant quantum computation (FT-QC) will likely take another decade or longer.

The strategic implication for organizations and institutions is clear: quantum computing does not require immediate investment in hardware, but it demands immediate attention in three areas. First, cryptographic preparedness: migration to quantum-resistant algorithms should begin now, not when quantum computers arrive. Second, algorithmic literacy: organizations should understand which of their problems are quantum-suitable. Third, sovereign infrastructure: in a future where quantum computers can break classical encryption, control over one's own data architecture becomes not optional but existential.

Quantum computing is neither a panacea nor an imminent disruptor. It is a fundamental expansion of the computable—and thus an invitation to extend the boundaries of our thinking as much as the boundaries of our machines.

References

Arute, F. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505–510.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings 28th ACM Symposium on Theory of Computing, 212–219.

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79.

National Institute of Standards and Technology (2024). FIPS 203–205: Post-Quantum Cryptography Standards. NIST.

Bluvstein, D. et al. (2024). Logical quantum processor based on reconfigurable atom arrays. Nature, 626(7997), 58–65.

Nayak, C. et al. (2008). Non-Abelian anyons and topological quantum computation. Reviews of Modern Physics, 80(3), 1083–1159.

Kitaev, A. Y. (2003). Fault-tolerant quantum computation by anyons. Annals of Physics, 303(1), 2–30.

Microsoft Research (2025). Majorana 1: A topological qubit chip. Microsoft Technical Report.

Cerezo, M. et al. (2021). Variational quantum algorithms. Nature Reviews Physics, 3(9), 625–644.

Bauer, B. et al. (2020). Quantum algorithms for quantum chemistry and quantum materials science. Chemical Reviews, 120(22), 12685–12717.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41.

Bernstein, D. J. & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.

Fellous-Asiani, M. et al. (2022). Limitations in quantum computing from resource constraints. PRX Quantum, 3, 020319.

Alexeev, Y. et al. (2021). Quantum computer systems for scientific discovery. PRX Quantum, 2, 017001.