

Quarterly Newsletter
CHAIR
iDANAE
INTELLIGENCE · DATA · ANALYSIS · STRATEGY

3Q25

Quantum Computing:
Strategic Insights for Decision-Makers



POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID

MSO Management
Solutions
Making things happen

Introduction to Quantum computing

Among emerging technologies, quantum computing (QC) stands out for the new possibilities it opens in tackling complex problems. Although still in its early stages of development, its potential to transform entire sectors is enormous, from supply chain optimization to the design of new drugs, as well as secure communications and artificial intelligence (AI).

While not yet mature for widespread business use, quantum computing is already shaping trends in technological innovation. Much like artificial intelligence a decade ago, its early progress is generating strong interest across industries. Understanding both its capabilities and limitations is therefore essential to anticipating its future role.

At its foundation, quantum computing relies on qubits¹, which differ fundamentally from classical bits. Qubits harness physical phenomena such as superposition² and entanglement³ and are manipulated through quantum gates⁴ to perform operations. These mechanisms allow information to be processed in ways that classical computers cannot, opening the door to solving calculations in optimization, system simulation and data analysis at unprecedented speed.

Combined with specialized architectures, these principles enable quantum computers to address problems involving exponential complexity, such as factoring large numbers or simulating molecular systems. Shor's algorithm⁵, for example, illustrates the potential impact on cryptography by threatening RSA-based encryption⁶, underscoring the urgency of quantum-resistant methods. [1]

From a business perspective, the implications are significant. In finance, quantum computing promises advances in portfolio

optimization and risk analysis. In pharmaceuticals, it accelerates drug discovery through molecular simulations. In energy, it supports dynamic optimization of grid systems and resource allocation. [2]

To prepare businesses and companies, leaders must assess sector's exposure to quantum disruption and their readiness for adoption. Strategic foresight is key: aligning exploration with business goals, investing in talent, and engaging with startups or research partners provides a pragmatic path to early experimentation. [3]

Quantum computing is no longer a distant possibility; it is an emerging capability that demands informed attention. Understanding both its mechanics and strategic potential is critical for organizations aiming to remain competitive in an increasingly complex digital economy. [4]

¹ Qubits (quantum bits) are the basic units of information in quantum computing. Unlike classical bits that can only be 0 or 1, qubits can exist in a combination of states due to superposition. They can also be linked through entanglement, enabling more complex and powerful computations.

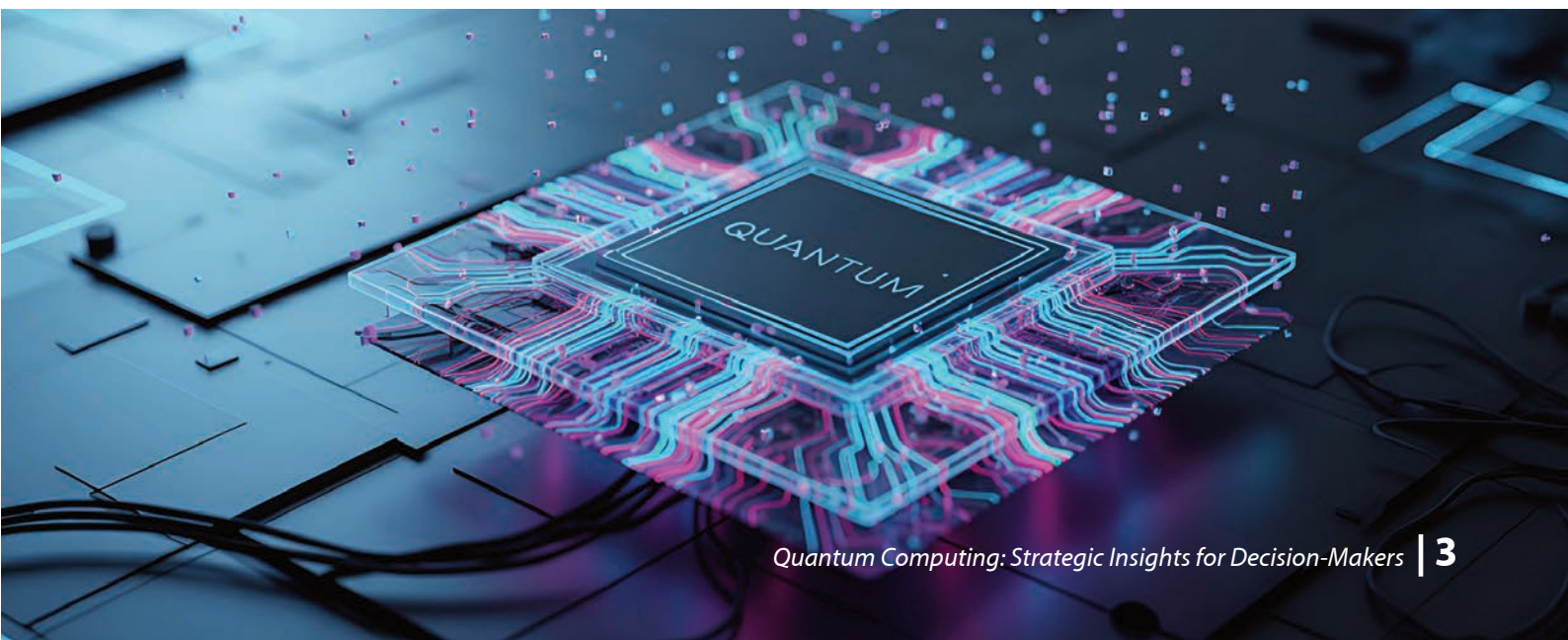
² Superposition: A qubit can exist in a combination of 0 and 1 states simultaneously, unlike a classical bit which is either 0 or 1. This allows quantum computers to process multiple possibilities at once.

³ Entanglement: A quantum phenomenon where two or more qubits become linked so that the state of one instantly affects the state of the other, no matter the distance between them. This enables strong correlations used in quantum computing and communication.

⁴ Quantum gates: Operations that change the state of qubits, similar to how classical logic gates manipulate bits. They perform reversible transformations on qubits, enabling quantum computation through superposition and entanglement.

⁵ Shor's algorithm: A quantum algorithm designed to efficiently factor large numbers into primes. Unlike classical factoring, which is slow for very large numbers, Shor's algorithm can solve it in polynomial time, threatening classical cryptography like RSA.

⁶ RSA-based encryption: A widely used public-key cryptography method that secures data by relying on the difficulty of factoring large numbers. Its security depends on the fact that, with classical computers, factoring the large product of two primes is computationally hard.



Problems quantum computing aims to solve

Quantum computing (QC) is emerging as a transformative tool across industries, opening new approaches to optimization, cryptography, and machine learning. [1]

Optimization is central to industries like logistics, finance, and energy, where the goal is to identify the best outcome among countless variables. Quantum algorithms, such as the Quantum Approximate Optimization Algorithm (QAOA)⁷, can evaluate many potential solutions more efficiently, reducing costs and time. Applications range from optimizing supply chains and traffic routing to renewable energy integration. [5]

Cryptography, the foundation of secure digital communication, is poised for disruption. Quantum computers threaten classical public-key systems but also introduce quantum-safe alternatives like lattice-based encryption⁸ and quantum key distribution⁹ (QKD), which leverage quantum uncertainty to provide theoretically secure communication. [1]

In machine learning, quantum-enhanced methods accelerate certain computational bottlenecks, such as high-dimensional data processing. Quantum-assisted models could enable more

efficient fraud detection, personalized healthcare insights, and financial risk modelling. [2]

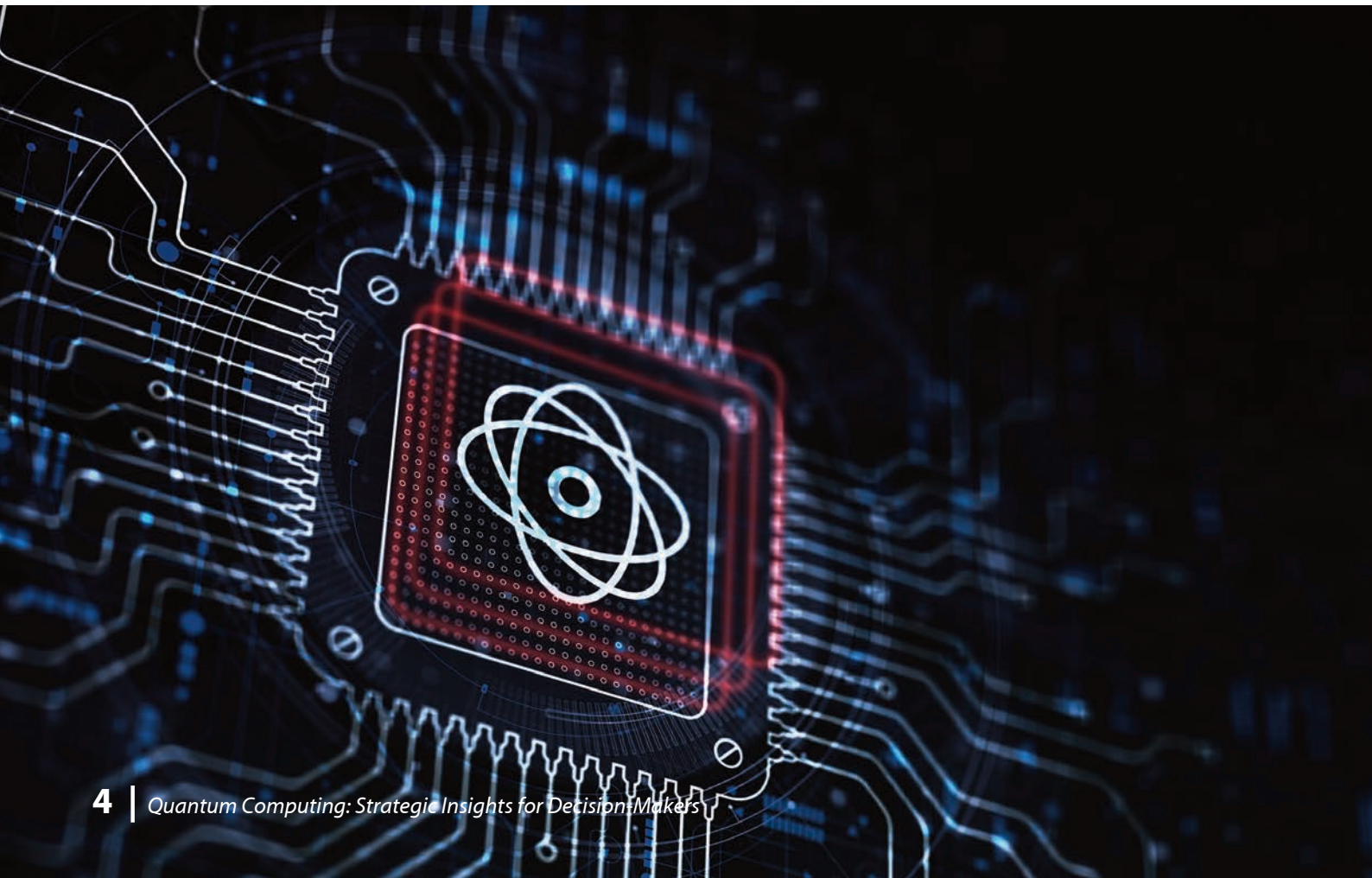
These breakthroughs are not merely theoretical. Pilot projects in banking are applying QC to portfolio rebalancing and risk simulations; pharma consortia are leveraging it to model protein folding; and energy providers are testing QC-based optimizations of grid management. [6]

Quantum computing doesn't just enhance existing processes; it reshapes decision-making itself by enabling probabilistic modelling and scalable scenario simulation. As the technology matures, its role in strategic planning and operational transformation will only deepen. [2]

⁷ QAOA: A quantum algorithm designed to find approximate solutions to combinatorial optimization problems.

⁸ Lattice-based encryption: A type of post-quantum cryptography that secures data using mathematical structures called lattices. It is considered resistant to attacks by quantum computers.

⁹ Quantum key distribution: A method for securely sharing encryption keys using quantum mechanics. It exploits principles like superposition and entanglement to detect any eavesdropping—if a third party tries to intercept the key, the quantum states are disturbed, revealing the intrusion.



Challenges quantum computing faces

Quantum computing faces a series of formidable obstacles. These challenges, spanning technical reliability, economic feasibility, and ecosystem readiness, must be addressed before the technology can achieve real-world impact. [7]

Technical fragility: tackling errors and scalability

Quantum systems rely on unique phenomena like superposition and entanglement, which allow them to process multiple possibilities simultaneously. However, these same properties also make quantum systems incredibly sensitive to their environments. [8]

One of the most significant hurdles is the high error rate in quantum operations. Qubits are prone to decoherence, meaning they can quickly lose their quantum state when exposed to external interference. This fragility makes it difficult to carry out long, reliable computations. [8]

Scalability is another core challenge. Most current quantum computers contain relatively few qubits, limiting their computational capacity. As systems grow, it becomes increasingly difficult to manage qubit interactions and control quantum gates with the precision required for accurate calculations. Scaling up will require innovations in materials, control systems, and error correction. [9]

High costs and uncertain ROI

Developing and operating quantum hardware is a capital-intensive endeavour. Building cryogenic infrastructure, isolating systems from environmental noise, and hiring specialized talent come with substantial costs. For many organizations, the economic case for investing in QC is still unclear. [10]

The return on investment remains difficult to quantify. While QC promises long-term gains in areas like optimization and simulation, the timeline for realizing these benefits is uncertain. Companies must weigh short-term costs against the potential for transformative outcomes, often with little clarity on when those outcomes will materialize.

There's also a growing concern around workforce readiness. The quantum talent pipeline is limited, and training new experts takes time. For businesses to benefit from QC, they need both the tools and the people capable of using them effectively. [10]

Ecosystem gaps: regulation, ethics, and standards

Beyond the lab, QC operates within a broader technological and social ecosystem. The regulatory landscape for quantum technologies remains underdeveloped. Policymakers are only beginning to grapple with how to govern a field that blends fundamental physics with digital infrastructure. [11]

Ethical concerns are also gaining attention. Quantum computing has the potential to break many of today's encryption systems, posing risks to data privacy and cybersecurity. Organizations must begin preparing for a future in which current cryptographic protections may no longer be sufficient. [8]

Standardization presents another hurdle. Without shared technical benchmarks and interoperability protocols, the industry risks fragmentation. Creating a common language and framework for quantum technologies will be essential for global collaboration and commercial viability. [11]

Quantum computing timelines

Quantum computing is evolving quickly, but the pace of real-world impact across industries remains uncertain. In medicine, quantum technologies are already shaping new horizons: quantum sensors enable ultra-precise detection of disease biomarkers, while quantum computers accelerate the analysis of vast health datasets and optimize molecular modelling for drug development and clinical trials. The integration of quantum tools in areas such as early diagnostics, personalized treatments, and secure data sharing is expected to revolutionize care models over the coming decade, yet successful adoption will depend on overcoming technical barriers and building clinical expertise. [12]

Pharmaceutical research is on the cusp of change as well. Quantum computers have already shown promise in simulating molecular interactions, enabling drug designers to identify and fine-tune promising candidates more rapidly than with traditional methods. Leading theoretical models and recent experimental papers suggest quantum technology could shorten drug development timelines by several years, especially for biological drugs and gene therapies, with large-scale impact projected as error-corrected quantum devices emerge during the 2030s. [13]

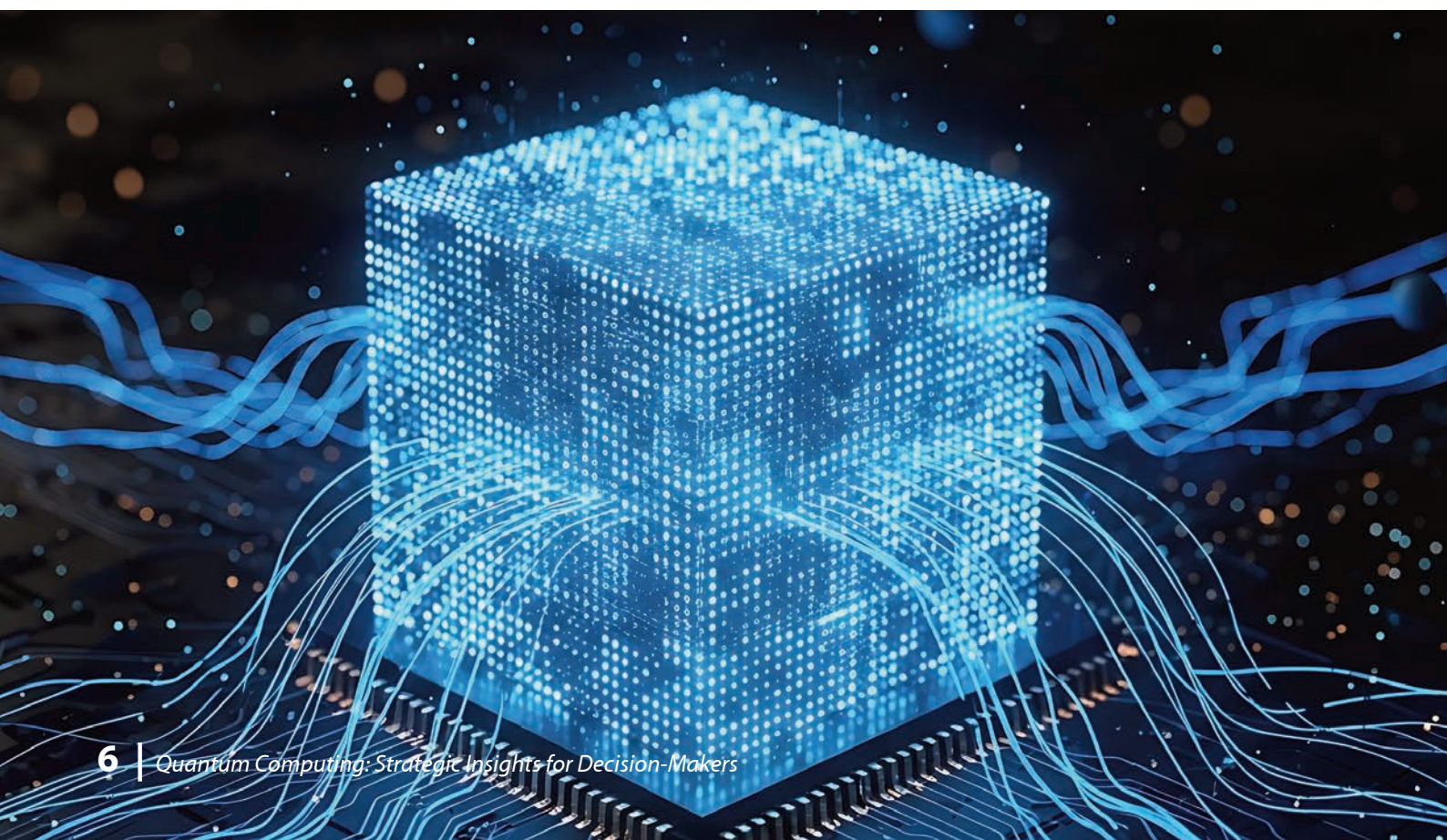
In finance, banks and insurers are already running pilots for quantum algorithms in risk analytics and fraud detection, but

most industry roadmaps (IBM and WEF) forecast meaningful, production-grade change closer to 2032–2035, contingent on scaling hardware and developing new regulatory standards. [14]

For logistics and global supply chains, the World Economic Forum reports that quantum computing is being piloted for route optimization and scenario forecasting, with sector-wide transformation expected as the ecosystem matures between 2030 and 2035. [15]

On cybersecurity, a quantum computer large enough to break RSA encryption is expected within the next 10–15 years. Research from Google Quantum AI and leading academic papers forecast a “Q-day” in the early-to-mid 2030s, driving the urgent migration to quantum-safe encryption for all critical infrastructures. [16]

Artificial intelligence and quantum computing are beginning to converge, as hybrid quantum-AI approaches show promise in health (diagnostics, genomics) and drug development. While quantum advantage is not yet routine outside research labs, peer-reviewed studies demonstrate quantum machine learning and molecular modelling have already outperformed classical approaches for specialized medical applications, with broader utility likely to follow as both fields mature. [12]



A Strategic Opportunity

Despite these challenges, QC remains one of the most promising frontiers in technology. Each hurdle presents an opportunity for innovation, investment, and leadership. Overcoming them will require collaboration across disciplines, sectors, and regions.

The path to quantum advantage is not linear, but it is navigable. As organizations build technical capacity, explore strategic use cases, and engage in shaping the broader ecosystem, they will help unlock the transformative power of quantum computing, not just as a tool, but as a catalyst for new ways of thinking and solving.

Strategic comparison with artificial intelligence: avoiding misconceptions and cycles in QC

Quantum computing is experiencing a wave of interest, marked by bold roadmaps and growing investments. To understand its trajectory, it is instructive to compare quantum computing's evolution with the history of artificial intelligence:

- ▶ Quantum computing stands on a foundation of mathematically proven theorems, notably the threshold theorem, which establishes that large-scale quantum error correction is feasible even when qubits and gates are imperfect, a result demonstrated in the development of topological color codes¹⁰ [17] [18]. This sets its evolution closer to artificial intelligence, whose theoretical advances from the 1960s and 1970s became impactful only once hardware caught up decades later.
- ▶ Like AI, quantum computing is now transitioning from theory to engineering: theoretical milestones are established, but practical value depends on robust hardware. For example, Google Quantum AI's Willow processor achieved operations below the quantum error threshold¹¹, a breakthrough confirmed in recent Nature publications [19]. This means scaling up quantum systems can exponentially suppress errors, enhancing computational reliability.
- ▶ Further, experimental validation of robust quantum logic using topological color codes has been achieved on neutral atom¹² platforms, as seen in recent work from Harvard, MIT, and QuEra [20], and was originally pioneered in a joint experiment between Martin-Delgado's group and Innsbruck laboratories [21].

Strategic Indicators: Lessons from AI's Evolution

Some strategic indicators may be used to measure the evolution of the implementation of QC:

- ▶ Functional utility must replace pure technical validation: quantum advantage, like AI, will be measured by successes in industrial problems and real application.
- ▶ Market absorption and business adoption: sustainable impact will come when quantum solutions power business models and widespread operational integration.
- ▶ Ecosystem and talent maturity: As with AI, quantum will require a skilled workforce, academic-industry collaboration, and robust software/hardware platforms.
- ▶ Patient investment and expectation management: Avoiding cycles of overpromise and disappointment means focusing on sustained, long-term progress, not hype.
- ▶ Media and policy realism: Carefully guided public discourse and policy can accelerate realistic expectations and constructive support.

Quantum computing's trajectory, like that of AI, will depend on persistent research, steady hardware progress, and practical cross-disciplinary collaboration. The path is not linear, but with the recent milestones in error correction and scalable logic, the field is positioned for a transition from foundational research to impactful technology.

¹⁰Topological color codes are a family of quantum error-correcting codes designed to protect quantum information from errors by encoding it in the global (topological) properties of a lattice of qubits, rather than local features. They work by arranging qubits on specifically colored, highly connected lattices—often in two or three dimensions—such that the encoded quantum state is robust against local noise and disturbances. Color codes are notable for enabling a broad range of fault-tolerant quantum gate operations, called transversal gates, which are performed in a way that errors do not spread uncontrollably. This structure makes color codes a leading candidate for scalable, fault-tolerant quantum computing and allows them to achieve computation below the error threshold needed for practical quantum advantage.

¹¹Quantum error threshold is a critical theoretical value in quantum computing that defines the maximum error rate—such as for qubit operations, storage, or measurements—that can be tolerated while still enabling reliable, large-scale quantum computation using error correction. If the physical error rates of a quantum processor stay below this threshold, quantum error-correcting codes can correct errors faster than they occur, allowing computations to be scaled indefinitely without information loss. Achieving and staying under the quantum error threshold is essential for building practical, fault-tolerant quantum computers and is the foundational goal of modern quantum hardware development.

¹²Neutral atom quantum computers are a type of quantum computing platform that use individual neutral atoms (rather than ions or superconducting circuits) as qubits. These atoms are trapped and arranged in precise patterns using lasers, often forming large, regular arrays. Quantum information is encoded in the internal states of the atoms, and operations between qubits are performed by shining laser pulses that induce interactions or entanglement. Neutral atom quantum computers are promising because they enable highly scalable architectures and flexible reconfiguration and have recently demonstrated fault-tolerant logic and error correction in large multi-qubit systems.

Learning from History, Leading into the Future

The current quantum community is working to avoid cycles of overpromise and delay by focusing on hybrid approaches, near-term applications, and hardware that meets error-correction thresholds. The optimism for quantum's future is justified by theoretical and experimental breakthroughs, but caution remains important: building a roadmap grounded in actual results, and not just aspirations, is essential.

Ultimately, the fate of quantum computing will mirror lessons from AI: persistence, hardware progress, and a focus on practical use cases will determine when and how the promise of quantum unfolds into everyday reality.

Strategic Frameworks for Evaluating Quantum Readiness

To navigate quantum adoption wisely, organizations must develop structured frameworks and decision criteria, assessing technological maturity, alignment with business goals, investment timeframes, synergy with existing workforce and infrastructure, and the regulatory environment. [7]

For example, industry benchmarks in finance (risk modelling, hybrid quantum-classical use), pharma (molecular simulations, tech partnerships), or energy (grid optimization, sustainability) can provide reality checks against hype.

Many organizations and researchers have developed structured frameworks for quantum readiness, such as the Quantum Readiness Toolkit from the World Economic Forum [22] and organizational readiness models highlighted in peer-reviewed literature. These tools help organizations assess their preparedness, set priorities for adoption, and avoid premature investments or vendor lock-in. As part of this strategic planning, technology leaders must recognize that any infrastructure or product relying on RSA or other current public-key cryptography will need to migrate to post-quantum safe algorithms in the years ahead, which is a priority underscored by NIST's official guidance and finalized standards for post-quantum cryptography, which recommend beginning this transition now to ensure future security and compliance [23].

Practical next steps: building quantum capacity

Some of practical steps may be considered to build quantum capacity in the organisations:

- ▶ Start with small, measurable pilot projects to test domain relevance and feasibility.
- ▶ Leverage partnerships with startups, cloud providers, and academic labs for access to expertise and rapid prototyping.
- ▶ Invest in executive and workforce education, drawing on accessible online programs and cross-sector conferences.
- ▶ Build cross-functional teams blending quantum and domain knowledge.
- ▶ Foster a culture of experimentation, iteration, and learning, not just with the technology, but with partnership and business models too. [7]

Closing Perspective: Strategic Foresight for QC

Quantum computing now appears closer than ever, but its timeline for mainstream adoption remains uncertain. As with artificial intelligence, transformative potential does not guarantee easy or immediate impact. Some industries will face challenges familiar from the AI journey: a shortage of highly trained specialists, unclear proof that the technology brings more value than mature classical solutions, and significant investment needs to establish the right infrastructure and integrate new workflows. In this landscape, it can be difficult for organizations to distinguish real opportunities from hype, or to pinpoint the use cases where quantum solutions will truly outperform existing tools.

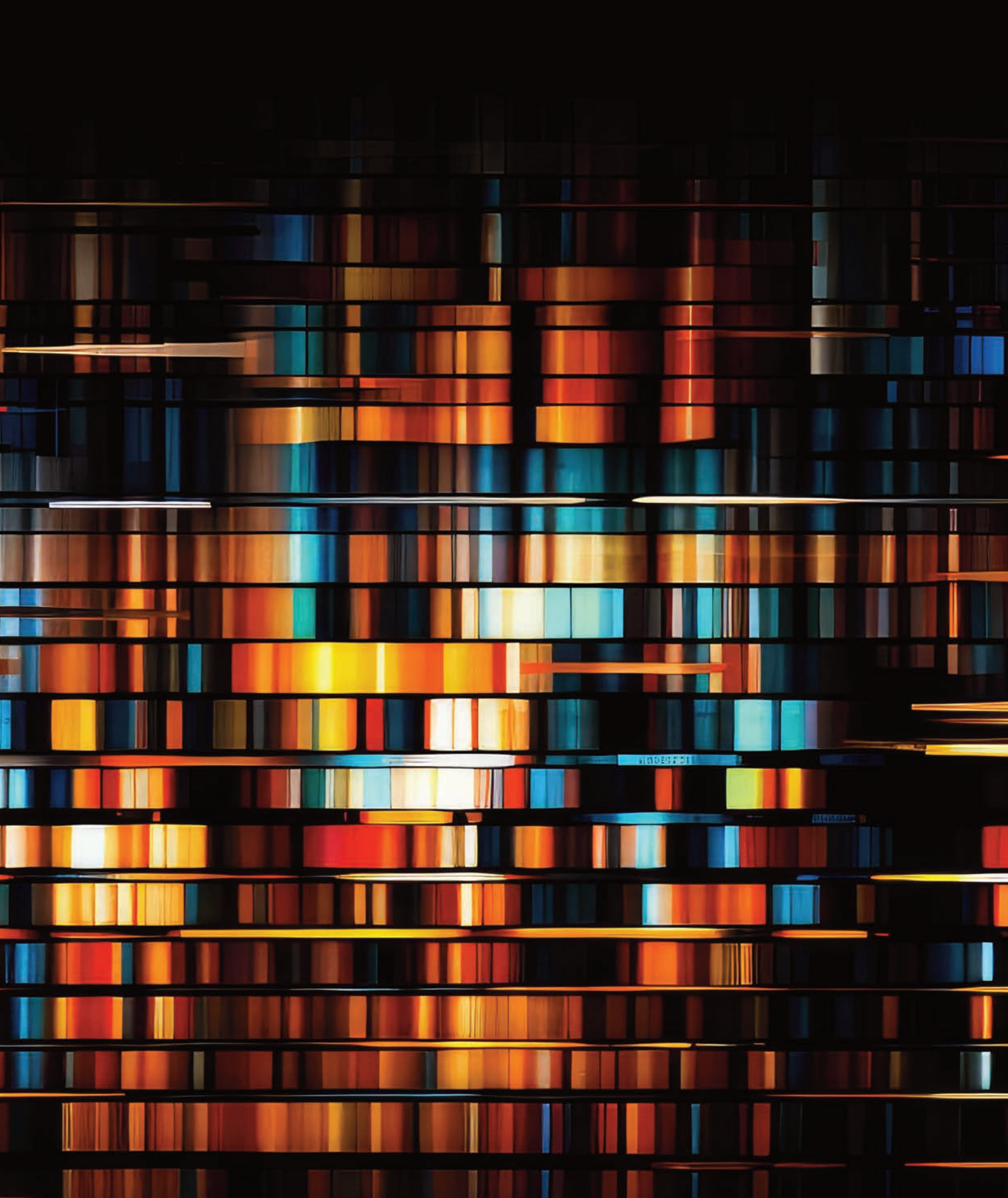
Much like the most successful AI projects, progress in quantum computing will depend on organizations that create environments where experts from diverse backgrounds (technical and business) can collaborate to identify and tackle the most pressing challenges. Building dedicated teams, crafting new ways of working, and embedding quantum strategies into daily operations will be essential. Just as crucial, any technology that relies on RSA cryptography will need to

begin a careful, planned migration to post-quantum safe algorithms. Decision-makers must actively evaluate quantum risks and update their technology strategy to ensure their systems are secure and future-ready. Only those organizations that combine realistic foresight with targeted ecosystem building will turn quantum's promise into tangible results.



Bibliography

- [1] Preskill, J.: Quantum Computing in the NISQ era and beyond (2018). <https://arxiv.org/pdf/1801.00862.pdf>.
- [2] IBM Research: The Future of Computing: IBM Quantum Roadmap (2022).
- [3] D-Wave Systems: Quantum Computing for Business: Practical Use Cases and Applications (2025).
- [4] ibm.com/roadmaps/quantum/
- [5] Quantum Computing Report: D-Wave Study Reports Over One-Quarter of Business Leaders Expect Quantum Optimization ROI of \$5 Million or Higher (2025).
- [6] <https://arxiv.org/abs/1910.11333>.
- [7] Quantum Computing in 2025: Hype vs Reality. [Supaboard.ai](https://supaboard.ai).
- [8] Quantum Computing Future - 6 Alternative Views Of The Next Decade. [Quantumzeitgeist.com](https://quantumzeitgeist.com).
- [9] Quantum Leaders Tell FT: Scaling Challenges Still Loom. [Thequantuminsider.com](https://thequantuminsider.com)
- [10] Quantum Computing in 2025: Milestones, Challenges, and What Lies Ahead. <https://www.linkedin.com/pulse/quantum-computing-2025-milestones-challenges-what-lies-ilja-bele%C5%84ki-jjnyf>
- [11] State of Quantum 2025 - Third Edition. [Meetiqm.com](https://meetiqm.com).
- [12] Martín-Delgado, M., et al.: Informes anticipando tecnologías cuánticas en la medicina del futuro. Observatorio de tendencias. Fundación Instituto Roche (2024).
- [13] Jeyaraman, N. et al.: Revolutionizing Healthcare: The Emerging Role of Quantum Computing in Enhancing Medical Technology and Treatment. National library of medicine (2024). doi: 10.7759/cureus.67486
- [14] Yndurain, E. et al.: Exploring quantum computing use cases for financial services. IBM Institute for business value (2019).
- [15] World Economic Forum: Quantum Economy Blueprint (2024).
- [16] Quantum computers may crack RSA encryption with fewer qubits than expected. [Phys.org](https://phys.org) (2025).
- [17] Bombin, H., & Martin-Delgado, M.A.: Topological quantum distillation. *Phys. Rev. Lett.* 97, 180501 (2006).
- [18] Bombin, H., & Martin-Delgado, M.A.: Topological computation without braiding. *Phys. Rev. Lett.* 98, 160502 (2007).
- [19] Google Quantum AI (2025): Willow processor breakthrough. *Nature*.
- [20] Sales Rodriguez, P., Robinson, J.M., Jepsen, P.N. et al. Experimental demonstration of logical magic state distillation. *Nature* 645, 620–625 (2025). <https://doi.org/10.1038/s41586-025-09367-3>.
- [21] Nigg, D., et al.: Quantum computations on a topologically encoded qubit. *Science* (2014).
- [22] World Economic Forum: Quantum Readiness Toolkit: Building a Quantum-Secure Economy (2023).
- [23] Alagic, G. et al.: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8545 (2025)



Authors

Ernestina Menasalvas (UPM)
Manuel Ángel Guzmán (Management Solutions)
Rodrigo Lojero (Management Solutions)



POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID

MS Management
Solutions
Making things happen

The Universidad Politécnica de Madrid is a multi-sector and multi-disciplinary Public Law Entity, which carries out teaching, research and scientific and technological development activities.

www.upm.es

Management Solutions is an international consulting firm, focused on business, finance, risk, organization, technology and process consulting, operating in more than 50 countries and with a team of 4,000 professionals working for more than 2,200 clients worldwide.

www.managementsolutions.com

For more information visit

blogs.upm.es/catedra-idanae/