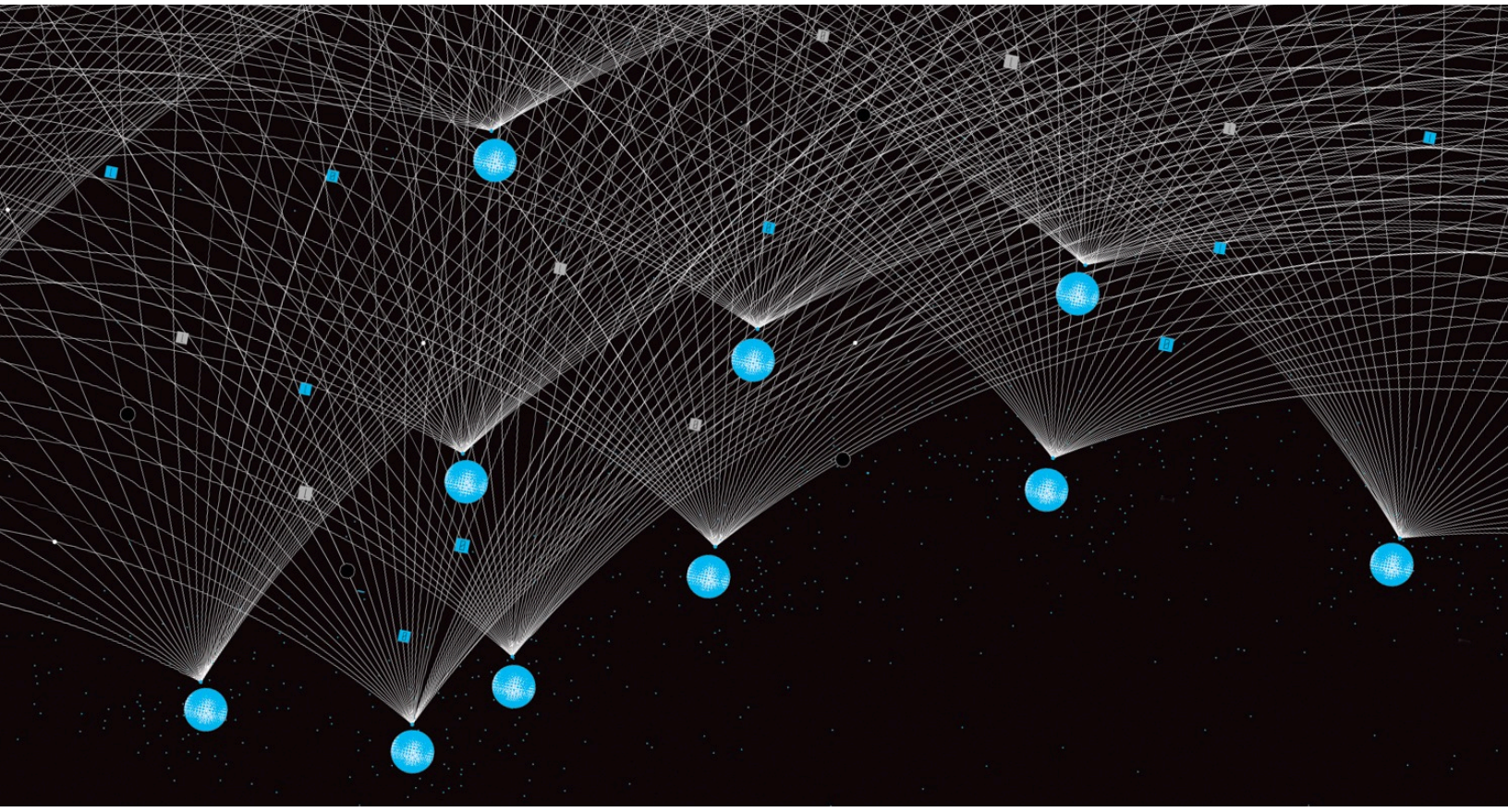
McKinsey Quarterly

Quantum's bold promise: What business leaders need to know

Quantum computing could optimize portfolios, simulate molecules, and model supply chains. That's just a start. In the next decade, as the technology matures, early movers could unlock real value.

by Henning Soller and Sven Smit
with Anna Heid



May 2026

For years, business leaders and corporate boards have viewed quantum computing (QC) as a threat—and for good reason: It has the potential to break today's strongest encryptions. That moment, commonly known as Q-Day, will occur when quantum computers succeed in factoring exceptionally large numbers, undermining the math that public-key cryptography depends on.

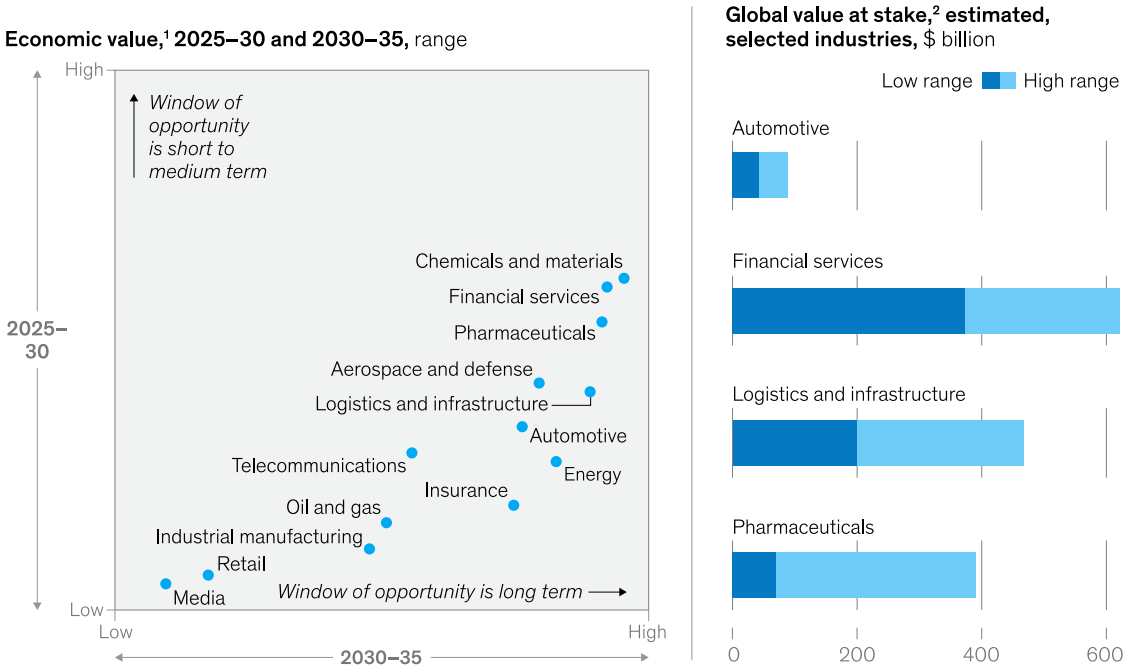
Though business leaders are keeping Q-Day top of mind, they are viewing QC through a new lens—less a threat and more an opportunity. Many are spurring their companies to experiment with QC now so that they will be ready to deploy it at scale once quantum computers become mainstream, which could happen within the next five years.

The potential benefits for early adopters are considerable. McKinsey research suggests that QC could create multibillions of dollars in enterprise value in the coming decade—and that's just for the industries we analyzed that are most likely to benefit (Exhibit 1). Providers of quantum computing have accelerated their engineering road maps and made algorithmic breakthroughs that suggest that scalable applications could arrive in a matter of years.

Exhibit 1

Quantum computing is poised to deliver immense economic value to companies worldwide by 2035.

Potential economic value from quantum computing by 2035



[1]Economic value is defined as the additional revenue and saved costs that the application of quantum computing (QC) could unlock at organizations.
[2]Our estimates are based on the additional economic value that QC-enabled use cases could deliver in each respective industry. We examined four industries in depth that are likely to realize value from QC in the next 10 years. Ranges illustrate conservative and optimistic scenarios and should be interpreted as approximate rather than definitive projections for business value.

McKinsey & Company

Unlike classical computers, which process information in a linear way, quantum computers leverage the principles of quantum mechanics to explore many potential solutions in parallel (see sidebar "Three principles of quantum mechanics"). While quantum computers themselves are extremely complex, they differ from classical computers in one fundamental way. Classical computers are built on units of information called bits, which can be represented by either a zero or a one. Quantum computers, on the other hand, are built on quantum bits, or qubits, which can represent any combination of zero, one, or both simultaneously. This form of nonlinear processing allows quantum computers to solve complex tasks far faster than even today's most powerful supercomputers.

Three principles of quantum mechanics

Quantum mechanics is the branch of physics that explains how the smallest particles in the universe, such as atoms and electrons, behave in unpredictable and counterintuitive ways. It provides a mathematical framework describing how energy and matter exist as both waves and particles, governed by probabilities rather than certainties. Quantum computing (QC) leverages three principles of quantum mechanics in particular.

Superposition

A classical computer using transistor-based classical bits can exist in only one of two states: zero or one. In a quantum computer, systems can instead be held in a special physical state called superposition, in which quantum bits (qubits) exist in a probabilistic combination of both zero and one simultaneously. Thus, a quantum computer requires fewer bits to describe the equivalent information compared with a classical computer. The implication in QC is that fewer bits are needed to describe equivalent information, which unlocks the possibility of performing extremely complex computations very quickly. Google recently announced that its quantum computer had successfully run a new algorithm 13,000 times faster than a top supercomputer could, for example.[1]

Entanglement

Entanglement is a unique quantum phenomenon in which qubits become deeply correlated so that manipulating the state of any one qubit instantaneously and predictably affects the state of another, regardless of physical distance. This "spooky action at a distance," as famously described by Albert Einstein, defies classical intuition. When entangled, qubits act as a unified system where measuring or manipulating one will directly affect the others no matter how far apart they are. The implication for QC is exponential parallelism. By entangling multiple qubits, quantum computers can represent and process an exponential number of possible states simultaneously. This capability underpins quantum computing's advantage in solving complex problems such as simulating molecular interactions in drug discovery or factoring large numbers for cryptographic analysis, tasks that are prohibitively difficult for classical machines.

Wave interference

Wave interference in quantum computing occurs when the probability amplitudes of different qubit states, stemming from their wave-like nature, interact—sometimes amplifying and sometimes canceling each other out. By carefully designing quantum algorithms, computer scientists can harness this wave interference to boost the probability of desired outcomes, while reducing the likelihood of errors. When a quantum computation is run multiple times, wave interference can increase the chances of obtaining a correct high-fidelity answer. However, because quantum results are based on probabilities, repeat measurements are needed to ensure that outcomes are accurate.

[1] "Google's quantum computer makes a big technical leap," Cade Metz, New York Times, updated October 27, 2025.

QC's greatest strength lies in its ability to solve problems that overwhelm classical computers, such as advanced simulation and probabilistic modeling. These capabilities make QC attractive for applications such as drug discovery, material simulation, supply chain optimization, and financial modeling—all areas where early QC applications are gaining traction. Already today, some organizations claim that QC outperforms classical computing by a wide margin (what's known as "quantum supremacy") and that the technology has matured to the point where companies are deriving incremental value from it.

QC has yet to hit the mainstream, however, because of two key challenges: Qubits are fragile and prone to errors, and QC hardware is expensive to build and operate. These constraints mean that for most companies today, QC is best suited to a small number of high-value use cases, rather than as a replacement for classical computing. However, advances in software are quickly helping to address these limitations. Algorithms that mitigate and correct errors could soon enable even imperfect quantum computers to deliver high-impact results. This algorithmic leap means that raw quantum hardware could become less important, making large-scale QC use happen sooner than hardware road maps alone suggest.

CEOs don't need to understand the intricacies of quantum computing to derive value from it. But they do need to know enough about the technology to understand where QC is headed and how it could affect their P&L. They also need to develop a clear view of the use cases that are relevant for their companies and partner with technology teams to map QC rollouts to measurable business results, such as cost savings or productivity gains.

Over the next ten years, we expect QC to evolve in two stages. In the first stage, limited use cases will develop in a hybrid approach with classical computing. During the second stage, so-called fault-tolerant quantum computers could unleash new scalable use cases that deliver significant value. In this article, we map out the potential evolution of QC over the next decade, then outline key actions business leaders can take to capture value from the technology.

First movers recognize that quantum utility will precede quantum perfection. Motivated pioneers in financial services, telecommunications, automotive, pharmaceuticals, chemicals, and other industries are accelerating pilots today. Business leaders who wait for a "perfect" fault-tolerant quantum computer before they act may find themselves behind the curve once such a machine does emerge. Their faster-moving competitors will have built intellectual property (IP) on top of today's QC machines—often in a hybrid environment with classical computers—giving them a strong head start on solving some of tomorrow's thorniest computing challenges (see sidebar "Four problems quantum computing can solve").

Four problems quantum computing can solve

For business leaders looking to grasp the fundamentals of quantum computing (QC), we have identified four evolving QC capabilities that will emerge over the next three to ten years. All will be critical for solving complex computational problems.

Quantum simulation

Quantum simulation can model complex systems, such as molecules and advanced materials, that are extremely challenging or impossible to simulate accurately on classical hardware because of the immense computational resources required. For example, simulating the quantum behavior of just 50 quantum bits (qubits) requires tracking more than one quadrillion states simultaneously. Quantum computers, by directly exploiting quantum principles such as superposition and entanglement, naturally represent these states, enabling the efficient and accurate simulation of quantum phenomena beyond the reach of classical computers. Quantum-simulation applications for chemistry, materials science, and drug discovery are already being deployed in small numbers and should reach scale within three years. Large-scale deployments are expected by the late 2020s to the early 2030s. This is contingent on developing error-corrected systems containing tens of thousands to hundreds of thousands of qubits.

Quantum optimization

Quantum optimization addresses complex combinatorial and numerical problems by leveraging quantum algorithms that explore vast solution spaces more efficiently than classical methods. While concrete field-specific examples are still emerging, early use cases in logistics and finance are demonstrating promising quantum optimization. For example, financial-services companies could use QC for portfolio optimization, helping identify optimal asset allocations faster and more efficiently than classical computational techniques. This can allow a financial institution to determine the ideal investment mix within a portfolio and quickly alter its approach to respond to risks. In one example, Citi Innovation Labs has partnered with QC software company Classiq to explore opportunities for portfolio optimization.[1]

Exploratory quantum hardware has also begun showing promise in accelerating heuristic algorithms to solve complex problems such as energy grid design or traffic flow management.

Broader commercial applications of heuristic optimization could emerge within five years, with large-scale deployments in the early 2030s. These applications will first leverage hybrid quantum–classical workflows before fully fault-tolerant machines become widely available.

Quantum AI

Quantum AI promises to harness quantum processors to either speed up existing AI training or enable fundamentally new learning paradigms, such as quantum neural networks that could analyze data far more efficiently than today's AI systems. Full-scale deployments are still at least a decade away, but quantum-machine-learning (QML) algorithms have been demonstrated in small-scale experiments. For example, researchers have developed a new liquid biopsy technique using QML that distinguishes between exosomes (microscopic particles released by cells) from cancer patients and those from healthy individuals by analyzing their electrical "fingerprints."[2] This approach could offer a faster, less invasive, and more cost-effective way to detect cancer.

---

[1] Louis Thompsett, "Citi explores quantum computing for portfolio optimisation," Classiq press release, February 9, 2024.
[2] Abhimanyu Thakur et al., "Quantum machine learning-based electrokinetic mining for the identification of nanoparticles and exosomes with minimal training data," Bioactive Materials, September 2025 Volume 51.

Quantum AI could also offer a synergistic feedback loop, as classical AI methods could improve quantum algorithms and hardware control, potentially accelerating the maturation of quantum systems.

Prime factorization

Prime factorization could dramatically accelerate the factoring of large integers compared with classical algorithms. This process uses a sequence of steps known as Shor's algorithm, which combines quantum interference with classical math routines to efficiently factor large integers and could break the math underpinning existing public-key cryptography.

Although demonstrated for small numbers on quantum devices containing only a few qubits, prime factorization at scale will require fault-tolerant quantum computing, as well as advances in error correction and qubit scaling. That may take at least ten years. From the mid-2030s onward, prime factorization could become commonplace, necessitating urgent attention from companies today to ensure they secure their systems for a postquantum cryptography world.

The next decade of quantum

The next ten years will bring significant technological gains that will advance the potential of quantum computing. Business leaders who understand the QC landscape will be better equipped than their peers to map corporate objectives against the industry's evolution.

The two-to-five-year horizon: Early value from hybrid systems

In the short term, executives can seek to capture value by deploying hybrid systems that combine QC applications with classical high-performance computing and AI. Practical use cases include simulating complex molecules and materials, which has gained traction in pharmaceuticals and chemicals; optimizing financial portfolios; and modeling complex supply chains or energy grid loads, where even small improvements can deliver significant value. Such QC pilots are most often deployed alongside classical computers. In these cases, classical computers process high-volume calculations, while QC machines solve the knottiest computations. Even a hybrid approach promises to dramatically boost computing speed, which our analysis shows could translate into billions of dollars in value for large organizations.[1] QC companies claim that quantum computers can outperform classical computers; now they must prove that this performance can translate into measurable business value.

The five-to-ten-year horizon: Full-scale impact from fault-tolerant QC

Recent product road maps suggest that a new set of technological advances is likely to enable fault-tolerant quantum computing (FTQC by 2030. This breakthrough will feature automatic error correction and stable qubits. Coupled with more advanced algorithms, FTQC machines will

[1] *Emergent Mind*, "Hybrid quantum-classical algorithms," updated October 18, 2025.

enable applications such as large-scale simulation for complex biology, climate, and materials modeling; deep integration of QC into mission-critical optimization and risk engines; and advanced AI that can spot patterns in high-dimensional data for yet-undiscovered applications. Pairing QC with AI will be critical. For example, quantum machine learning (QML) is already speeding up some of the heavy math and optimization steps that make AI model training so resource intensive today, while quantum circuits could allow smaller, lower-cost AI models to perform much more efficiently. These technological gains signal an upcoming convergence between AI and QC and could be the breakthrough that propels the long-term value creation from QC that executives seek.

Quantum's key stakeholders

Our analysis identifies three main stakeholder groups—users, investors, and technology providers—that will be at the forefront of transforming QC from a theoretical promise to a foundational element of the next computational era.

Users

Our research shows that hundreds of organizations worldwide are already engaging with QC. Activity among sectors, however, remains uneven. We see an "urgency paradox" in quantum adoption. While sectors such as pharmaceuticals and chemicals have the most promising problem sets that could be solved by QC, other sectors are moving faster, such as defense, finance, and telecommunications (Exhibit 2). These industries are still operating from a risk perspective, where the cost of being second outweighs the technology's uncertainty. Nonetheless, today's early efforts can guide leaders just starting to explore how QC could affect their businesses, informing them on what's possible in the near to medium term.

For some sectors, such as manufacturing, public services, and insurance, QC may seem like a distant technology with few immediate applications relevant to their core operations. But neglecting to engage with QC at all today could be a mistake. That's because even if a company does not deploy QC directly, it will likely still be affected by it—especially when it comes to cybersecurity. (The looming Q-Day, when QC breaks today's encryption, will require companies to rapidly shift to new forms of security.)

Investors

QC is a capital-intensive sector that will need billions of dollars in investment to scale. QC requires clean rooms, advanced manufacturing, and complex software. Investors span venture capital and private equity firms, corporations, and governments, each essential to the sector's development. Both public and private investors will need to accelerate their activity to move QC into the mainstream.

Global quantum investment is highly uneven. Europe and parts of Asia stand out for public funding, while the United States, and increasingly China and the United Kingdom, are attracting a disproportionate share of the private capital needed for late-stage scaling. Our analysis shows

that as of 2024, QC companies in the United States have captured 57 percent of worldwide private quantum investment, while those in the European Union have attracted only 10 percent. This disparity belies the strong public support and large talent pool of quantum scientists in Europe.

Business leaders need to remain attuned to investment trends to strategically plan their organizations' future QC deployments and partnerships. Creating a robust quantum strategy means looking globally. For instance, leaders could look to the US ecosystem for commercial partnerships and to European innovation hubs to recruit scarce talent.

Technology providers

Technology providers produce QC components, hardware, and software. They run the gamut from start-ups spun out from academic research institutes to unicorn private companies such as PsiQuantum to large tech providers such as Google and IBM.

Two key sectors are on-premises QC machine sales—primarily to government and research organizations—and quantum-as-a-service (QaaS) platforms, which allow customers to access QC applications via cloud subscriptions and pay-per-use pricing. Providers of on-premises machines, which can cost millions to tens of millions of dollars apiece, include IBM, IonQ, IQM Quantum Computers, and Quantinuum. Some of the main QaaS providers today include Amazon Braket, IBM Quantum, and Microsoft Azure Quantum. These companies resell capacity from technology providers such as IonQ, Quantinuum, and Rigetti, which also sell their QC capacity directly to users.

In addition to these QaaS platforms, software providers are developing vertical applications that combine domain expertise with quantum algorithms in areas such as molecular modeling for drug discovery or risk analysis for financial services. We expect some of these vertical QaaS applications to evolve into outcome-based business models where customers pay for tangible results delivered by QC. This customer-centric commercialization model could be especially prevalent in the pharmaceutical sector, where companies already pay for each viable drug candidate discovered using AI. Complementing QaaS offerings will be full-stack solutions that combine hardware sales, software licensing, and consulting services, in which QC technology providers cocreate tailored solutions for each customer.

Rather than betting that a single leading QC technology provider will emerge, executives can adopt a multivendor approach, selecting specific providers to solve specific business use cases.

Three steps for QC success

Many companies will want to ready themselves for the maturation of quantum computing, given its potential to create value. For forward-thinking companies, that preparation can begin now. Our research shows that a strategic QC playbook balances prudence with risk-taking over three crucial steps.

Step one: Map exposure and opportunity

Getting QC right requires both defense and offense. Business leaders can map a defensive strategy by examining how their companies' sensitive data and critical infrastructure could pose quantum-related security risks, especially when Q-Day arrives. This requires inventorying which data and products must remain secure and then migrating those assets to quantum-resistant cryptography and hybrid encryption schemes. In parallel, leaders should embed quantum risk into vendor strategies by updating procurement standards and ensuring that their vendors can rapidly adopt postquantum cryptography standards as they become available.

Simultaneously, business leaders can outline an offensive strategy by mapping their companies' specific business problems to potential quantum solutions. They can start by identifying a few high-value use cases where the performance limits of classical computing are holding back innovation. These are the use cases where even an incremental quantum advantage could create material differentiation, such as developing R&D pipelines or conducting combinatorial optimization for scheduling, routing, or asset allocation. Once these use cases are identified, companies can invest in partnerships with QC companies, pilot programs, and talent development. In particular, they can explore whether software solutions from companies such as Classiq, Horizon Quantum Computing, Kipu Quantum, Q-CTRL, and Strangeworks could address their use cases, or whether they want to engage in the deep hands-on work of building QC software themselves.

Beyond these defensive and offensive plays, leaders can benchmark their QC readiness against industry peers, many of which are already cementing early partnerships with technology providers. Mapping exposure in this way can help organizations quantify both the risk of disruption and the potential for value creation from QC.

Step two: Secure options on technology and talent

The companies that will win with QC tomorrow are building the necessary technology infrastructure today. To get that right, CEOs and their technology teams can establish strategic relationships with quantum hardware or cloud providers, ideally spanning different technological approaches, including on premises, cloud, and hybrid. They can also begin adapting their own technology architectures incrementally. This could include modernizing data pipelines, modularizing compute workflows, and ensuring their high-performance computing and AI environments can interoperate with emerging quantum run times. Of course, companies should be mindful not to alter their existing tech stacks too quickly or dramatically. They can instead build a flexible foundation that enables the integration of QC capabilities as they mature, given that the market is still early and the trajectory uncertain.

Forward-thinking CEOs are already securing the talent they will need to adopt QC in the next three to five years. The demand is high, and the talent pool is small, so moving fast will be essential. Hiring QC experts from research labs and universities is one proven avenue. CEOs can also build a small internal "translation" team of two to five people who will oversee the company's gradual shift from classical computing to QC. This team should be closely tied to AI units and tasked with evaluating QC use cases, coordinating pilots, and connecting business, data, and quantum experts.

Step three: Run targeted experiments during the readiness window

Getting good at anything requires practice, and QC is no exception. This means that business and technology leaders can design a few high-value QC pilots now in areas such as molecular simulation, portfolio optimization, or logistics using the latest QC offerings or hybrid quantum–classical computing platforms. Developing early QC algorithms on small-scale machines can help ensure that a company owns the IP for this software when more powerful machines come online.

Companies can also get their data ready today for a quantum future. Quantum algorithms require data to be structured differently than classical AI models, so cleaning and re-architecting enterprise data now is a prerequisite for future speed. In addition, technical teams can integrate QC considerations into their broader AI and cloud road maps.

Whichever pilots their companies deploy, CEOs should measure not just ROI but also the IP created, the talent developed, and the ecosystem relationships built. This approach can deliver maximum learning and secure long-term value.

Quantum computing is moving from scientific theory to strategic reality. Many technical hurdles remain, but the combination of advancing hardware, faster progress on software algorithms, and accelerating investment shows that QC will soon become mainstream. Clearly, most business leaders can no longer treat QC as a distant curiosity.

Leaders who act now to understand where quantum intersects with their core challenges, secure options on talent and technology, and run targeted pilots will have a crucial head start. They will be able to defend against the upcoming security transition and seize QC's opportunities offensively. Over the next decade, their companies could be poised to capture a large share of economic value that QC may deliver.

Henning Soller is a partner in McKinsey's Frankfurt office, **Sven Smit** is a senior partner emeritus and senior adviser in the Amsterdam office, and **Anna Heid** is an associate partner in the Zurich office.

This article was edited by Kristi Essick, an executive editor in the Bay Area office.