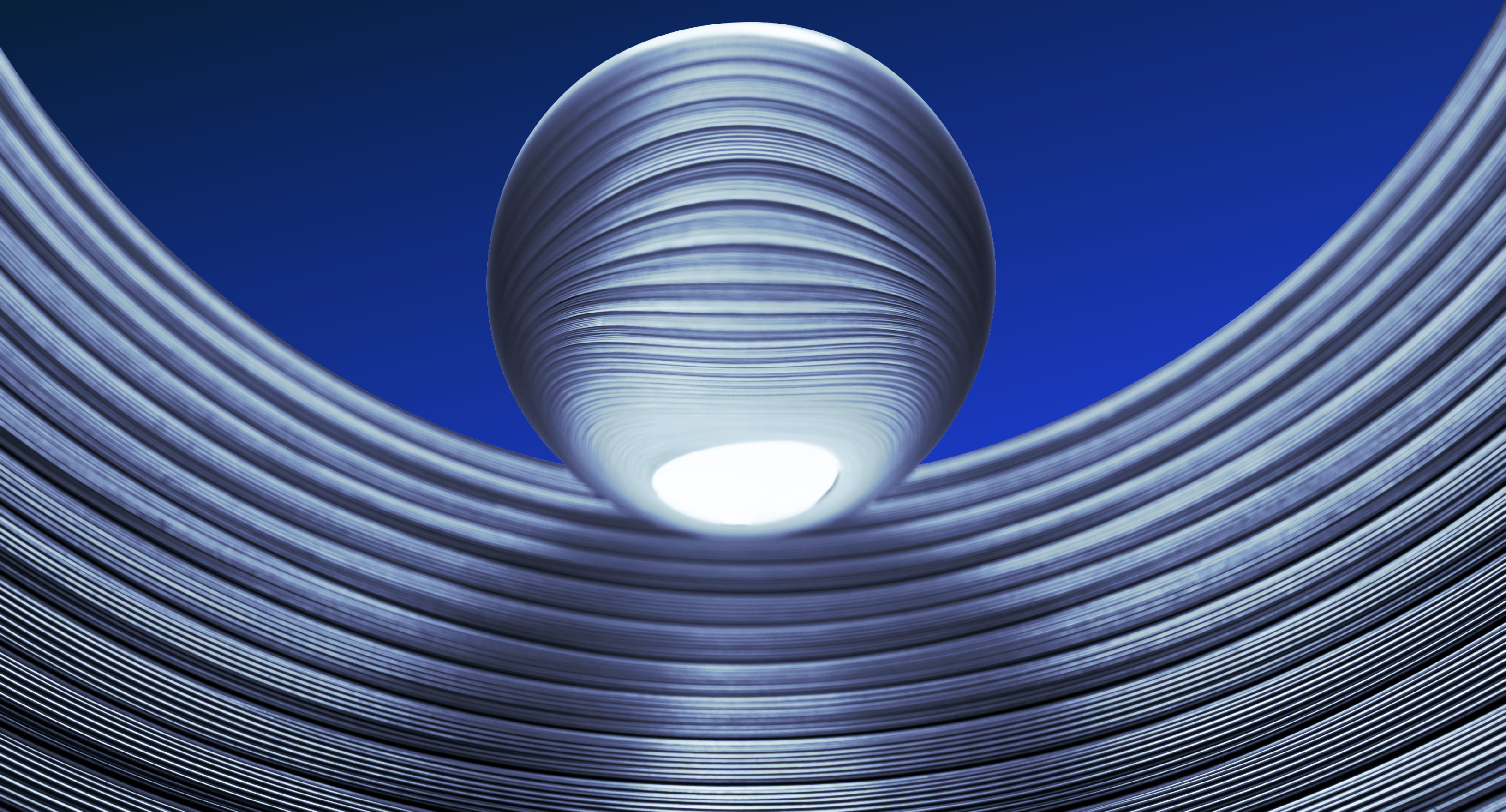
McKinsey & Company

Quantum computing: An emerging ecosystem and industry use cases

December 2021



McKinsey & Company

McKinsey & Company is a global management consulting firm, deeply committed to helping institutions in the private, public, and social sectors achieve lasting success. For more than 90 years, our primary objective has been to serve as our clients' most trusted external adviser. With consultants in more than 100 cities in over 60 markets, across industries and functions, we bring unparalleled expertise to clients all over the world. We work closely with teams at all levels of an organization to shape winning strategies, mobilize for change, build capabilities, and drive successful execution.

Cover image: © Paolo Carnassale/Getty Images

Contents

Preface

Accelerating advances in quantum computing are powerful reminders that the technology is rapidly advancing toward commercial viability. In just the last few months, for example, a research center in Japan announced a breakthrough in entangling qubits (the basic unit of information in quantum, akin to bits in conventional computers) that could improve error correction in quantum systems and potentially make large-scale quantum computers possible. And one company in Australia has developed software that has shown in experiments to improve the performance of any quantum-computing hardware.

As breakthroughs accelerate, investment dollars are pouring in, and quantum-computing start-ups are proliferating. Major technology companies continue to develop their quantum capabilities, as well: companies such as Alibaba, Amazon, IBM, Google, and Microsoft have already launched commercial quantum-computing cloud services.

Of course, all of this activity does not necessarily translate into commercial results. While quantum computing promises to help businesses solve problems that are beyond the reach and speed of conventional high-performance computers, use cases are largely experimental and hypothetical at this early stage. Indeed, experts are still debating the most foundational topics for the field.

Still, the activity suggests that CIOs and other leaders who have been keeping an eye out for quantum-computing news can no longer be mere bystanders. Leaders should start to formulate their quantum-computing strategies, especially in industries such as pharmaceuticals that may reap the early benefits of commercial quantum computing. Change may come as early as 2030, as several companies predict they will launch usable quantum systems by that time.

To help leaders start planning, we conducted extensive research and interviewed 47 experts around the globe about quantum hardware, software, and applications; the emerging quantum-computing ecosystem; possible business use cases; and the most important drivers of the quantum-computing market. In this report, we discuss the evolution of the quantum-computing ecosystem and dive into quantum computing's

Accelerating advances in quantum computing are powerful reminders that the technology is rapidly advancing toward commercial viability.

possible commercial uses in pharmaceuticals, chemicals, automotive, and finance—fields that may derive significant value from quantum computing in the near term. We then outline a path forward and how industry decision makers can start their efforts in quantum computing.

This article was a collaborative effort by Matteo Biondi, Anna Heid, Nicolaus Henke, Niko Mohr, Ivan Ostojic, Lorenzo Pautasso, Linde Wester, and Rodney Zemmel.

The authors wish to thank the following individuals for their contributions to this report: Ahmed Abdulla, Mohammad Ardati, Florian Budde, Ruben Contesti, Sameer Kohli, Thomas Lehmann, Anika Pflanzer, Henning Soller, Alexander Thobe, Daniel Volz, and Matija Zesko, as well as several members of the McKinsey Technology Council, a group of global experts convened to track and assess emerging trends in business and technology, including: Alán Aspuru-Guzik, chief scientific officer at Zapata; Charles Beigbeder, founding partner at Quantonation; Serguei Beloussov, founder and chairman at SIT, founder and chief risk officer at Acronis, and co-chairman at Runa Capital; Michael Brett, global business development lead, quantum computing at Amazon Web Services; Jerry Chow, director of quantum hardware system development at IBM; Tommaso Demarie, chief executive officer at Entropica Labs; Chad Edwards, head of strategy and product at Cambridge Quantum; Andrew Horsley, chief executive officer at Quantum Brilliance; John Martinis, professor of physics at UCSB; Mark Mattingley-Scott, general manager EMEA at Quantum Brilliance; Celia Merzbacher, executive director at QED-C; Sam Mugel, chief technology officer at Multiverse Computing; Jeremy O'Brien, co-founder and chief executive officer at PsiQuantum; Christopher Savoie, chief executive officer at Zapata; Arun Karthi Subramaniyan; and Matt Trevithick, chief operating officer at Google Quantum AI.

Executive summary

A fast-developing ecosystem, increasing investment, and accelerating research breakthroughs in quantum computing signal it's time for executives to consider the technology's business implications.

In anticipation of possible developments in the field, we discuss the emerging quantum-computing ecosystem, dive into relevant use cases in four key industries, and preview the path forward, including how to get started. To evaluate commercial use cases for quantum computing, we focus on pharmaceuticals, chemicals, automotive, and finance because our research and analysis suggest that these industries will derive significant value from quantum computing in the near term. Given the nascency of quantum computing, our overview of several use cases is intended to guide researchers and users toward high-potential areas in which to further develop their insights rather than provide a comprehensive list.

An ecosystem that can sustain a quantum-computing industry is unfolding

Funding. Because quantum computing is still a young field, the majority of funding for basic research in the area still comes from public sources.

However, private funding is increasing rapidly. In 2021 alone, announced investments in quantum computing start-ups have surpassed $1.7 billion, more than double the amount raised in 2020. We expect private funding to continue increasing significantly as quantum-computing commercialization gains traction.

Hardware. Hardware is a significant bottleneck in the ecosystem. The challenge is both technical and structural. First, there is the matter of scaling the number of qubits in a quantum computer while achieving a sufficient level of qubit quality. Hardware also has a high barrier to entry because it requires a rare combination of capital, experience in experimental and theoretical quantum physics, and deep knowledge—especially domain knowledge of the relevant options for implementation.

Multiple quantum-computing hardware platforms are under development. The most important milestone will be the achievement of fully error-corrected, fault-tolerant quantum computing, without which a quantum computer cannot provide exact, mathematically accurate results.

Experts disagree on whether quantum computers can create significant business value before they are fully fault tolerant. However, many say that imperfect fault tolerance does not necessarily make quantum-computing systems unusable.

When might we reach the fault tolerance? Most hardware players are hesitant to reveal their development road maps, but a few have publicly shared their plans. Five manufacturers have announced plans to have fault-tolerant quantum-computing hardware by 2030. If this timeline holds, the industry will likely establish a clear quantum advantage for many use cases by then.

Software. The number of software-focused start-ups is increasing faster than any other segment of the quantum-computing value chain. In software, industry participants currently offer customized services and aim to develop turnkey services when the industry is more mature. As quantum-computing software continues to develop, organizations will be able to upgrade their software tools and eventually use fully quantum tools. In the meantime, quantum computing requires a new programming paradigm—and software stack. To build communities of developers around their offerings, the larger industry participants often provide their software development kits free of charge.

Cloud-based services. In the end, cloud-based quantum computing services may become the most valuable part of the ecosystem and can create outsize rewards for those who control them. Most providers of cloud-computing services now offer access to quantum computers on their platforms, which allows potential users to experiment with the technology. Since personal or mobile quantum computing is unlikely this decade, the cloud may be the main way for early users to experience the technology until the larger ecosystem matures.

Four industries—pharmaceuticals, chemicals, automotive, and finance—could realize earliest use cases

Most known use cases fit into four archetypes: quantum simulation, quantum linear algebra for AI and machine learning, quantum optimization and search, and quantum factorization. We describe these fully in the report, as well as outline questions leaders should consider as they evaluate potential use cases.

We focus on potential use cases in a few industries that research suggests could reap the greatest short-term benefits from the technology: pharmaceuticals, chemicals, automotive, and finance. Collectively (and conservatively), the value at stake for these industries could be between roughly $300 billion and $700 billion.

Pharmaceuticals. Quantum computing has the potential to revolutionize the research and development of molecular structures in the biopharmaceuticals industry as well as provide value in production and further down the value chain. In R&D, for example, new drugs take an average of $2 billion and more than ten years to reach the market after discovery. Quantum computing could make R&D dramatically faster and more targeted and precise by making target identification, drug design, and toxicity testing less dependent on trial and error and therefore more efficient. A faster R&D timeline could get products to the right patients more quickly and more efficiently—in short, it would improve more patients' quality of life. Production, logistics, and supply chain could also benefit from quantum computing.

While it is difficult to estimate how much revenue or patient impact such advances could create, in a $1.5 trillion industry with average margins in earnings before interest and taxes (EBIT) of 16 percent (by our calculations), even a 1 to 5 percent revenue increase would result in $15 billion to $75 billion of additional revenues and $2 billion to $12 billion in EBIT.

A faster R&D timeline could get products to the right patients more quickly and more efficiently—in short, it would improve more patients' quality of life.

Chemicals. Quantum computing can improve R&D, production, and supply-chain optimization in chemicals. Consider that quantum computing can be used in production to improve catalyst designs. New and improved catalysts, for example, could enable energy savings on existing production processes—a single catalyst can produce up to 15 percent in efficiency gains—and innovative catalysts may enable the replacement of petrochemicals by more sustainable feedstock or the breakdown of carbon for CO_2 usage. In the context of the chemicals industry, which spends $800 billion on production every year (half of which relies on catalysis), a realistic 5 to 10 percent efficiency gain would mean a gain of $20 billion to $40 billion in value.

Automotive. The automotive industry can benefit from quantum computing in its R&D, product design, supply-chain management, production, and mobility and traffic management. The technology could, for example, be applied to decrease manufacturing process–related costs and shorten cycle times by optimizing elements such as path planning in complex multirobot processes (the path a robot follows to complete a task) including welding, gluing, and painting. Even an industry-standard 2 percent productivity gain—in the context of an industry that spends $500 billion per year on manufacturing costs—would create $10 billion to $25 billion of value per year.

Finance. Finally, quantum-computing use cases in finance are a bit further in the future, and the advantages of possible short-term uses are speculative. However, we believe that the most promising use cases of quantum computing in finance are in portfolio and risk management. For example, efficiently quantum-optimized loan portfolios that focus on collateral could allow lenders to improve their offerings, possibly lowering interest rates and freeing up capital. It is early—and complicated—to estimate the value potential of quantum computing–enhanced collateral management, but as of 2021, the global lending market stands at $6.9 trillion, which suggests significant potential impact from quantum optimization.

Preparing for a quantum future

Until about 2030, we believe that quantum-computing use cases will have a hybrid operating model that is a cross between quantum and conventional high-performance computing. For example, conventional high-performance computers may benefit from quantum-inspired algorithms.

Beyond 2030, intense ongoing research by private companies and public institutions will remain vital to improve quantum hardware and enable more—and more complex—use cases. Six key factors—funding, accessibility, standardization, industry consortia, talent, and digital infrastructure—will determine the technology's path to commercialization.

Leaders outside the quantum-computing industry can take five concrete steps to prepare for the maturation of quantum computing.

1. Follow industry developments and actively screen quantum-computing use cases with an in-house team of quantum-computing experts or by collaborating with industry entities and by joining a quantum-computing consortium.

2. Understand the most significant risks and disruptions and opportunities in their industries.

3. Consider whether to partner with or invest in quantum-computing players—mostly software—to facilitate access to knowledge and talent.

4. Consider recruiting in-house quantum-computing talent. Even a small team of up to three experts may be enough to help an organization explore possible use cases and screen potential strategic investments in quantum computing.

5. Prepare by building digital infrastructure that can meet the basic operating demands of quantum computing; make relevant data available in digital databases and set up conventional computing workflows to be quantum ready once more powerful quantum hardware becomes available.

Introduction

A fast-developing ecosystem, increasing investment, and accelerating research breakthroughs in quantum computing signal it's time for executives to consider the technology's business implications.

Quantum computing—the application of quantum mechanics to computational problems and the focus of this report—is a novel technology that can help businesses solve problems that are beyond the reach of conventional high-performance computers (HPCs) and solve existing problems significantly faster (for a basic primer on quantum computing, see sidebar "Quantum computing: An overview"; for a list of key terms, see Glossary).[1]

As the potential of quantum computing becomes more apparent, investments have ballooned; our research finds that 2020 alone saw about $700 million in private funding for quantum technology start-ups. Announced private investments for 2021 are already double this amount, bringing the total private investment in quantum computing from 2001 to 2021 to more than $3.3 billion.[2] Announced public investments in quantum computing are even higher: nearly $30 billion to date.

Buoyed by this investment, the ecosystem of players in quantum computing is expanding across the value chain. The number of quantum-computing start-ups has jumped from a handful in 2013 to more than 200 in 2021, with increasingly more start-ups focused on software.[3] Major technology companies continue to develop their quantum capabilities as well: companies such as Alibaba, Amazon, IBM, Google, and Microsoft have already launched commercial quantum-computing cloud services.

Of course, the business potential from all this activity could benefit from analysis, particularly because commercial quantum computing is still in its early days. The number and quality of qubits, basic units of

[1] For more information on the differences between quantum and conventional computers, see Alexandre Ménard, Ivan Ostojic, Mark Patel, and Daniel Volz, "A game plan for quantum computing," February 2020, McKinsey.com.
[2] The cumulative value increases to about $4.2 billion when including investments in quantum communication and quantum sensing.
[3] "The Quantum Technology Monitor," September 2021, McKinsey.com.

Quantum computing: An overview

Quantum computing is based on entirely different physical processes than conventional computing. Quantum computers use quantum bits (qubits) as their most basic unit of information. Unlike conventional binary bits that are either 0 or 1, quantum bits can assume values that are a combination—superposition—of both 0 and 1. This characteristic of quantum physics enables new computing algorithms that can massively compress computation time.

Quantum computing was first proposed in 1980.[1] And in the past few years, quantum computers demonstrated that they could outperform the most powerful supercomputers at specific tasks. For instance, Google claimed quantum supremacy in 2019 when it solved in seconds a problem that would have taken the world's most powerful supercomputer at the time thousands of years.[2] While such achievements are extraordinary scientific breakthroughs, commercial uses of quantum computing are in their early days.

[1] Paul Benioff, "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *Journal of Statistical Physics*, May 1980, Volume 22, pp. 563–91, link.springer.com; R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, 1982, Volume 21, pp. 467–88, link.springer.com.
[2] Frank Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, 2019, Volume 574, Number 7779, pp. 505–10, nature.com.

About the research

Because quantum computing is fundamentally different from conventional computing—and involves different physical processes—identifying technically viable, commercially relevant use cases requires deep expertise in both quantum computing and specific industries. We examined four archetypical use cases:

1. Quantum simulation of molecular processes

2. Quantum linear algebra for artificial intelligence (AI) and machine learning

3. Quantum optimization and quantum search algorithms for Monte Carlo simulations

4. Quantum factorization for cybersecurity

With those use cases in mind, we interviewed 47 experts around the globe, including members of the McKinsey Technology Council, a group of global experts convened to track and assess emerging trends in business and technology, about quantum hardware and software, applications, the emerging quantum-computing ecosystem, and the most important drivers of the quantum-computing market. Of these experts, nearly half specialize in quantum computing and work in universities, quantum-computing hardware and software start-ups, and major tech companies. The remaining interviewees have other ties to quantum computing, such as expertise in data science applied to industry and active investments in quantum computing.

From September 2020 to April 2021, we convened groups of experts—both quantum enthusiasts and skeptics—to discuss and record their views on the key computational challenges in their industries. Questions we posed include:

1. What are the relevant—and proven—quantum use cases for your industry's challenges?

2. What would be the business impact from resolving these challenges?

3. Would eliminating these challenges disrupt the industry—and force every industry participant to adopt quantum-computing solutions to remain relevant?

The experts gave their opinions and helped us estimate the business value of selected quantum-computing use cases. These interviews—focused on industry-specific challenges—helped us uncover areas where quantum computing might be uniquely valuable.

Of course, the early stage of quantum computing technology and the immaturity of the quantum-computing industry make identifying relevant use cases largely a theoretical exercise. And while many use cases have the potential to be highly disruptive, their total economic value depends on many unknown factors. Because of the level of uncertainty involved, we err on the side of offering conservative estimates for the value at stake.

In our research, we systematically identified quantum-computing use cases by matching use-case archetypes with known, relevant industry problems, such as predicting products' toxicity in the pharmaceuticals and chemicals industries. More broadly, research in quantum use cases has gained momentum over the past few years and is likely to lead to many new discoveries. The use cases we identify should therefore be regarded as high-value areas for exploration, not as an exhaustive list of quantum-computing use cases.

information in quantum computing, are currently low, which makes quantum computers error-prone and often unreliable. Most industry use cases require hardware that is highly fault tolerant, where errors are corrected and do not invalidate computations. A number of companies believe they will be able to offer fault-tolerant quantum-computing hardware sometime between 2026 and 2030, though some industry experts are more pessimistic.

However, there might already be some relevant use cases, though open questions and debates remain (for more detail, see sidebar "Open questions in quantum computing"). Use cases with significant business value may also emerge before high fault tolerance is achieved if developers discover algorithms that can overcome significant hardware errors. We expect the development of quantum-computing hardware to gradually evolve through a pre-fault-tolerant phase marked by increasing numbers and quality of qubits as well as gradual improvements in error mitigation, making it worthwhile to track the evolution of each phase. Technology leaders should stay alert to developments in the field to avoid falling behind while competitors reap quantum computing's early benefits.

In anticipation of possible developments in the field, we will discuss the emerging quantum-computing ecosystem, dive into relevant use cases in four key industries, and preview the path forward, including how to get started. To evaluate commercial use cases for quantum computing, we focus on pharmaceuticals, chemicals, automotive, and finance because our research and analysis suggest that these industries will derive significant value from quantum computing in the near term. Given the nascency of quantum computing, our overview of use cases is not comprehensive; instead, it is intended to guide researchers and users toward high-potential areas in which to further develop their insights.

Open questions in quantum computing

Experts continue to explore many open questions and debates on topics such as the state of development of the technology, standards and metrics for performance, and the value of different use cases.

Some debates in these areas relate to semantics—for example, using the term "circuit model for quantum computing" or "gate-based quantum computing" for the same concept. Others revolve around basic concepts. For instance, experts differ on whether they believe quantum supremacy has ever been demonstrated, and some believe that it receives undue emphasis. Additionally, while experts agree that the number of qubits alone is not a good measure of quantum hardware's performance (many we interviewed say that the race for higher qubit counts is fueled by media attention), there is no agreed-upon alternative to qubit counts as a measure of quantum-computing systems' performance. Some experts name quantum volume, which accounts for the number, quality, and connectivity of qubits in a single standardized metric.[1] However, they also warn that as qubit count and quality improve, the metric may need to be reconsidered. Still other experts point out that the emphasis on qubit quantity and quality shortchanges other major areas of development, such as improvements in components and systems software.

In discussions of quantum-computing hardware, experts disagree on the interpretations of different groups' findings because of a lack of transparency. This deficiency makes it difficult to infer the efficacy of alleged advances in business use cases. Indeed, estimates of quantum computing's potential value in different industries vary. For instance, some experts consider our conservative estimates of the potential value of portfolio optimization and quantum AI in finance very low, while others find the use cases unlikely in the near future.

Experts also disagree on the importance of fault tolerance for making quantum-computing use cases viable. Some believe that fault tolerance is required to solve business problems. Others believe that fault tolerance is a continuum rather than a binary—either/or—condition.

These open debates mean that some experts disagree with some of the ideas we discuss in this report. Experts we interviewed do, however, agree that the emphasis at this early stage should be on the possible fit between quantum-computing technology and challenges in the market rather than on the technology itself. While the experts we consulted confirmed that this report covers the most important use cases, some believe that quantum computing could have a significant role in combatting climate change in areas such as material design to facilitate the storage of new types of fuels. Others believe that the first use case of value will be simulation of complex quantum systems in theoretical physics, rather than any use case that will create business value. Others point out that quantum-inspired conventional-computing algorithms are already in use and creating value—and merit attention on their own.

Significantly, some experts indicate that not enough time and resources have been invested in developing use cases to reliably indicate which use cases are more or less viable. Our discussion of use cases should therefore be used as a guide to areas to explore further, not a definitive road map.

[1] Jerry Chow and Jay Gambetta, "Quantum takes flight: Moving from laboratory demonstrations to building systems," IBM, January 2020, ibm.com; "Quantum volume," IBM, ibm.com; Andrew W. Cross et al., "Validating quantum computers using randomized model circuits," *Physical Review A*, September 2019, Volume 100, Issue 3, pp. 323–28, journals.aps.org.

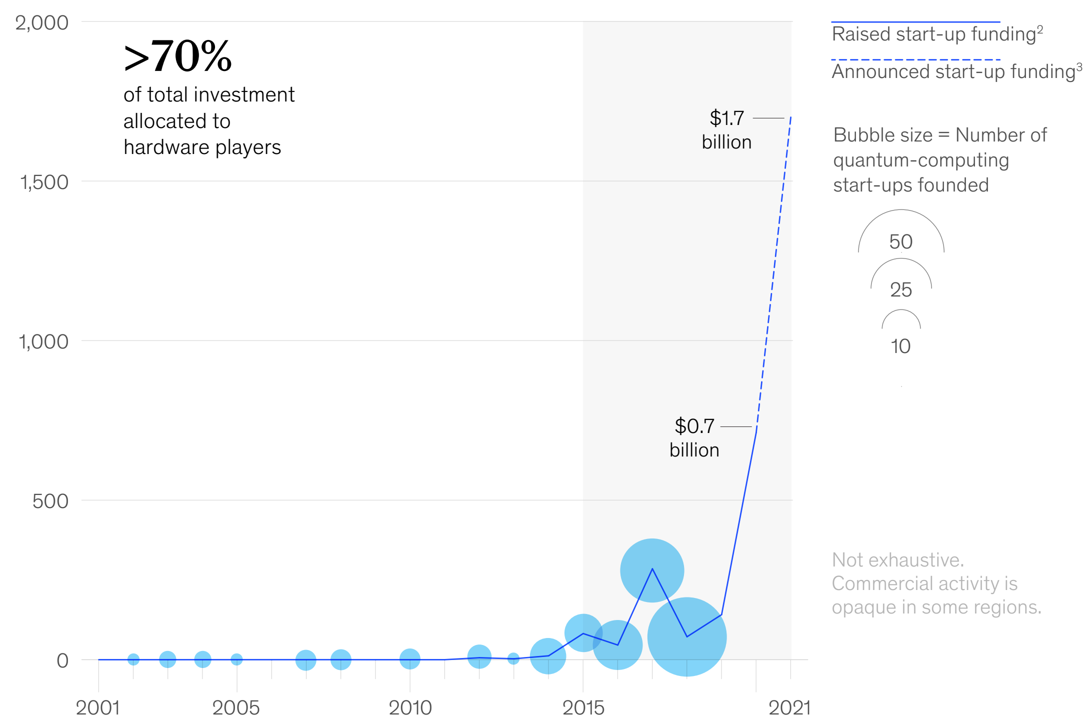
1 Increasing funding fuels an emerging quantum ecosystem

Our research indicates that the value at stake for quantum-computing players is nearly $80 billion (not to be confused with the value that quantum-computing use cases could generate). Over the past decade, an ecosystem of quantum-computing players—from components makers to service providers—has developed across the quantum-computing value chain to capture portions of this value. As quantum computing progresses toward commercial viability, these businesses are attracting increasing amounts of private funding. In 2021 alone, announced investments in quantum-computing start-ups have surpassed $1.7 billion, more than double the amount raised in 2020 (Exhibit 1). We expect private funding to continue increasing significantly as commercialization of quantum computing gains traction.

Exhibit 1

Start-up activity and investments in quantum computing have skyrocketed since 2015.

Volume[1] of raised funding, $ millions



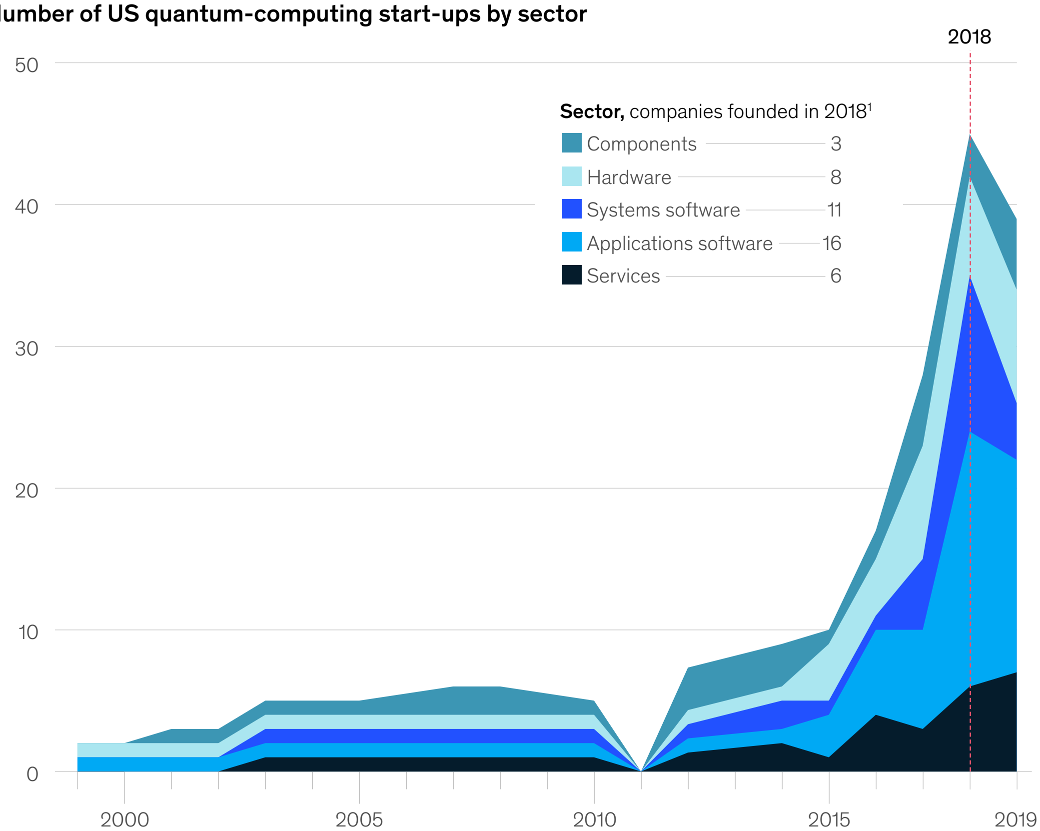
[1]Based on public investment data recorded in PitchBook; actual investment is likely higher.
[2]Public announcements of major deals; actual investment is likely higher.
[3]Start-ups from 2019 and later are likely still in stealth mode or are not yet recognized as quantum-computing companies by relevant platforms and experts.
Source: PitchBook; McKinsey analysis

Our research shows that the Canada, the United Kingdom, and the United States are home to the most quantum-computing starts-ups, which collectively took in 90 percent of the $3.3 billion in private funding raised during the past two decades. Within the value chain, start-up hardware companies (which manufacture quantum computers) saw more than 70 percent of private investments. However, the application software sector now appears to be growing the fastest—of the 45 companies founded in 2018, 65 percent were in software (Exhibits 2 and 3).

Exhibit 2

The United States is home to the highest number of quantum-computing start-ups, with software seeing the highest level of global start-up growth.

Number of US quantum-computing start-ups by sector



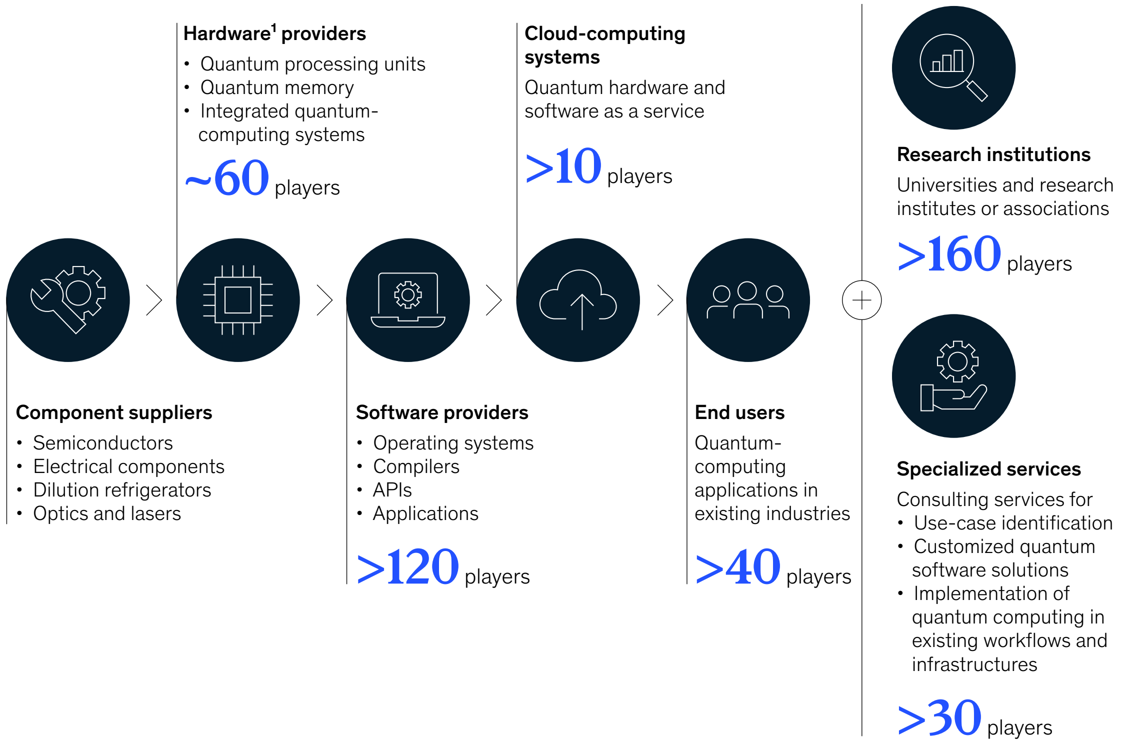
Number of quantum-computing start-ups by region 2015 2018

Note: Not exhaustive; commercial activity is opaque in some regions.
[1]Number only quoted until 2018, since start-ups with a later founding date may still be in stealth mode (ie, they have not disclosed their activity publicly.
Source: Capital IQ; Crunchbase; PitchBook; Quantum Computing Report; McKinsey analysis

Exhibit 3

In the quantum-computing value chain, software has the largest number of players.

Overview of players in the quantum-computing value chain



[1]Complete computing systems.

Governments are also committing significant funding to develop quantum technologies domestically; nine governments have each announced funding of $500 million or more. China has announced $15 billion in funding, more than all other governments combined have dedicated to the endeavor (Exhibit 4).[4]

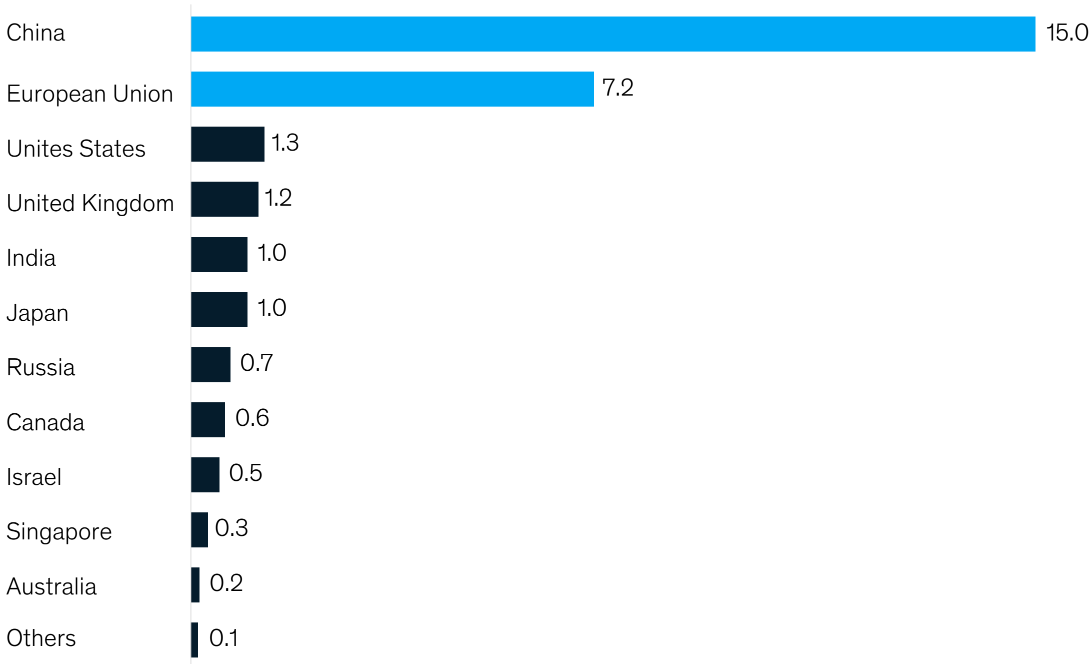
Hardware is the limiting factor for the growth of the ecosystem and for quantum computing in general. Scaling the number of qubits in a quantum computer while achieving a sufficient level of qubit quality is a significant technical challenge. Hardware also has the highest barriers to entry because it requires a rare combination of capital, deep knowledge, experience in experimental and theoretical quantum physics, and domain knowledge of the relevant implementation options (such as superconducting electronics, photonics, and ion traps); there is a relatively small number of hardware providers in existence today. However, investors are in hot pursuit of opportunities—seven of the ten largest quantum-technology deals in the past ten years went to quantum-computing hardware manufacturers for amounts as high as $650 million (for definitions of the hardware platforms, see Glossary).[5]

[4]"The Quantum Technology Monitor," September 2021, McKinsey.com.
[5]Analysis of PitchBook data on quantum-computing deals from 2011 to 2021 combined with announced deals from 2021 that are not yet in the database.

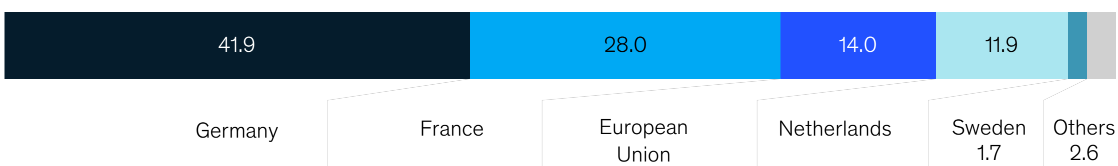
Exhibit 4

China and the European Union lead significantly on public funding for quantum computing.

Announced planned governmental funding,[1] $ billions



EU public funding sources, %



Note: Figures may not sum to 100%, because of rounding.
[1]Total historic announced funding; timelines for investment of funding vary per country.

Diverse software players look to build communities

Because quantum computing requires a fundamentally new programming paradigm, it requires an entirely new software stack, including programming languages at different levels of abstraction (which corresponds to the amount of complexity necessary to view or program a system). Most of the larger industry participants offer their own software development kit, often free of charge, to build a community of developers.

In developing quantum-computing software solutions, industry participants currently offer customized services, targeting problems for which quantum solutions can be combined with HPCs. Specifically, providers help clients identify use cases that are suitable for their businesses and develop custom algorithms. Providers aim to offer turnkey services when the industry is more mature. As quantum hardware develops further, organizations can upgrade their quantum software and eventually use fully quantum tools.

Cloud providers have made quantum hardware accessible to the public

Cloud-based quantum-computing services may be the most valuable part of the quantum-computing ecosystem, delivering disproportionate rewards to the parties that control it. Some of the largest providers of cloud-computing services currently offer access to quantum computers on their platforms, and some hardware developers have made their hardware devices accessible through proprietary cloud services. This availability allows prospective quantum-computing users to experiment with the technology. Because personal or mobile quantum computing is unlikely this decade, cloud access may become the main way for early users to experience quantum computing.

2 A closer look at quantum-computing use cases

Quantum computing could unleash significant business value across industries. Further exploration is needed, and it requires deep expertise in both quantum algorithms and their industries—a combination that is still rare today.

In this section, we will discuss how to evaluate potential use cases and provide five main use-case archetypes. Because hardware will be the determining factor that can unlock quantum computing across these industries, we discuss the current state of hardware and key milestones in its expected course of development. We then explore quantum-computing use cases in pharmaceuticals, chemicals, automotive, and finance.

Evaluating use cases

Until quantum-computing hardware is more accessible and less expensive, commercially viable applications of quantum computing will likely focus on high-value use cases.

When evaluating quantum-computing use cases, business leaders need to answer five key questions:

1. Does the economic value achieved by the quantum speedup—or the resolution of a previously unsolvable problem—justify the investment?

2. Is there a known quantum algorithm for the mathematical problem behind the use case?

3. How large a quantum speedup is required to create a practical advantage over conventional HPCs?

4. What kind of quantum hardware will be required to achieve this speedup? When might it be available?

5. Can being an early mover create a long-term strategic advantage?

Because of open technical questions, creating quantum algorithms that solve business problems faster is not straightforward. For starters, quantum computing is not the next iteration of supercomputing, which speeds up any type of computational task. Rather, it is a different mode of computing that enables fundamentally new algorithmic techniques (ways in which algorithms function) that can speed up the computation of specific mathematical problems.

For leaders seeking viable quantum-computing use cases, the main concern is whether the mathematical problem behind the business challenge can be solved with a known quantum algorithm. Fewer than 100 algorithms with a proven quantum speedup (a measure of how much better a quantum computing solution is compared to the best conventional-computing alternative) are currently known,[6] and the speedup can differ significantly between algorithms.

[6] For a comprehensive list of quantum-computing algorithms, see Steven Jordan, "Quantum Algorithm Zoo," February 2021, quantumalgorithmzoo.org; the best way to measure quantum speedup is under discussion. For more, see Troels F. Rønnow et al., "Defining and detecting quantum speedup," *Science*, July 2014, Volume 345, Issue 6195, pp. 420–24, science.org.

Another consideration is how much speedup is required to create a practical advantage over conventional HPCs and what kind of quantum hardware is necessary to make that speedup possible. Some algorithms produce exponential speedups, while others may offer less powerful quadratic speedups. For algorithms with exponential speedups, even small quantum computers of about 100 qubits (the basic building blocks of a quantum computer) could theoretically outperform current HPCs; for context, the machine that first achieved a beyond-conventional result had a 54-qubit quantum processor. For algorithms with only quadratic quantum speedups, significantly more advanced and powerful quantum processors will be required to demonstrate practical advantages over the most powerful conventional computers.[7]

The four types of use cases

Most known use cases fit into four archetypes: quantum simulation, quantum linear algebra for AI and machine learning, quantum optimization and search, and quantum factorization.

Quantum simulation is the simulation of quantum-mechanical systems or processes such as molecules, chemical reactions, or electrons in solids. Conventional computers are unable to accurately simulate quantum systems that have more than a few dozen particles, so such problems are currently solved approximately—or not at all. Quantum computers, however, are inherently suited for such intractable quantum simulations because they are quantum systems themselves, which provides an exponential speedup over conventional computers. Quantum-simulation use cases—such as quantum mechanics (QM), molecular mechanics (MM), and molecular dynamics (MD) simulations—are mostly found in the pharmaceuticals and chemicals industries for tasks such as lead identification or catalyst optimization.[8]

Quantum linear algebra is a broad field with a diverse set of quantum techniques and approaches, mostly applied in AI and machine learning. In some applications, critical steps in conventional machine-learning pipelines (which automate the machine-learning workflow) are replaced by quantum algorithms with a proven quantum speedup to shorten training time. In other applications, the entire learning approach is transferred into the quantum world, as in quantum neural networks. Quantum linear algebra applications can provide an exponential speedup over conventional algorithms but require stringent requirements on hardware (quantum memory, fault tolerance) and mathematically well-defined problems. Quantum computing may be especially valuable in natural language processing, as it can accurately extract meaning from complex sentences and form outputs. When deployed at scale, this processing will be useful for automation of complex tasks such as providing financial advice. Quantum AI and machine learning are applicable across a broad range of industries, including pharmaceuticals, automotive, and finance, for tasks such as autonomous driving, automated trading, and predictive maintenance. Quantum linear algebra can also be used to simulate classical physics, such as mechanical stability; thermodynamic behavior; and noise, vibration, and harshness (NVH) characteristics.

Quantum optimization is expected to solve much more complex problems than conventional computers can. The technique could find better solutions in the same amount of time and solve previously intractable problems; for example, quantum algorithms for discrete optimization typically provide a quadratic speedup over conventional computing. Experts hope that it could facilitate real-time optimization by compressing computation times from hours to seconds. Use cases for quantum optimization are found in almost every industry for tasks such as generative design, traffic management, and portfolio optimization. Quantum search enables a quadratic speedup to find specific entries in an unstructured database. Similar techniques are used to improve conventional Monte Carlo simulations, which are ubiquitous in quantitative finance for

[7] For more on qubits, see Alexandre Ménard, Ivan Ostojic, Mark Patel, and Daniel Volz, "A game plan for quantum computing," February 2020, McKinsey.com.
[8] Lead generation is the process by which pharma companies identify promising compounds and molecules that can become the basis for new drugs.

activities such as pricing derivatives. Quantum search could reduce the calculation time from days to hours and enable faster trading decisions.

Quantum factorization is the most widely known application of quantum computing. Shor's algorithm for the calculation of the prime factors of large numbers was among the first algorithms for which a quantum speedup was mathematically proven, providing an exponential speedup over the best conventional algorithm to date. Efficient quantum factorization is most readily applicable to breaking RSA encryption, the basis of most of today's secure data-transfer protocols. Because "post-quantum" alternatives to RSA encryption already exist, we do not expect an acute cybersecurity crisis. However, organizations should update their encryption standards in the coming years.

How advances in quantum-computing hardware affect use-case realization

Multiple quantum-computing hardware platforms are currently in development. The most advanced are superconducting circuits and trapped ions, on which all currently commercially available quantum computers are based. Other promising platforms are photonic networks, spin qubits, and neutral atoms.

Current and potential quantum-computing use cases run alongside a development continuum from early-stage, pre-fault-tolerant algorithms to late-stage, fault-tolerant quantum computers. Reaching fault tolerance depends on the pace and scale of hardware improvements. The key milestone to watch for is the achievement of fully error-corrected, fault-tolerant quantum computing. Without full error correction, gate-based quantum computers cannot provide exact, mathematically accurate results. In other words, a quantum computer without full error correction does *not* necessarily work most of the time and gives an error some of the time. Even if each individual gate has a low error rate, given the sheer number of gates needed for a computation, the full computation will more often be wrong than right. Experts hope to find quantum-computing use cases that can outperform high-performance computing despite the error rate. We therefore divide the future development of quantum-computing hardware into two phases: the pre-fault-tolerant phase and the fault-tolerant phase. Each of these phases contains substages characterized by increasing numbers of qubits in a single quantum computer, better gate operations, and higher-quality qubit readouts (Exhibit 5).

The pre-fault-tolerant phase. We are currently in the early part of the pre-fault-tolerant phase, in which there are two types of quantum computers: gate-based and annealer-based (see Glossary).

Some experts argue that gate-based quantum computers have achieved quantum supremacy and can therefore be used in areas such as cryptography, which draws on quantum computers' ability to generate truly random outputs. This verifiable randomness can be used to improve the security of encryption protocols. However, other viable use cases that offer significant benefit to business cannot be realized on today's gate-based quantum computers. According to experts, the performance of quantum-computing hardware will improve by about tenfold in the pre-fault-tolerant phase, which will allow the first demonstrations of quantum simulation and optimization use cases on gate-based quantum devices.

Among experts, quantum computing's ability to provide significant business value before it is fully fault tolerant is a topic of much discussion. While some experts do not believe use cases exist at all for pre-fault-tolerant computers, others are more optimistic. Many experts we interviewed agree that fault tolerance is not a binary event and that error correction is a continuum; imperfect fault tolerance does not necessarily make quantum-computing systems unusable. One expert noted that the conventional computers that put people on the moon were not fault tolerant.

Exhibit 5

Maturing quantum-computing hardware will make more use cases viable.

Lighthouse use cases along the quantum-computing hardware development timeline

Development timeline: Not fully error corrected → Fully error corrected

Current state of development: Early stage

	Early stage	Late stage	Fault-tolerant early stage	Fault-tolerant late stages	Universal quantum supercomputer[2]
Proxy for hardware needs,[1] qubits ● Annealing ● Gate-based QC	Logical: N/A ● ~10,000 ● ~100	Logical: N/A ● ~100,000 ● ~1,000	Logical: ~100 ● ~100,000 ● ~100,000	Logical: ~1,000 ● ~1,000,000 ● ~1,000,000	Logical: ~10,000+ ● ~10,000,000+ ● ~10,000,000+
Challenges for gate-based quantum computing		Scalability and error correction			Quantum data storage (quantum RAM) and efficient data input and readout
Challenges for annealing		Better qubit connectivity			
Lighthouse use cases Algorithm archetypes: Linear algebra (AI/ML) Optimization Simulation Factoring Other Industries: Pharmaceuticals Chemicals Automotive Finance Logistics	Certified randomness (Job) scheduling optimization Route and fleet optimization Clinical-trial site-selection optimization	Synthetic-data generation Approximate QM simulation[3] Small-scale quantum reinforcement learning Collateral and portfolio optimization Robot path optimization Production-process optimization	Light risk simulation (Approximate) MD,[3] MM[3] simulation (eg, protein folding) Trading-strategy optimization Protein folding	Breaking RSA cryptography Financial and cyberrisk simulation Large-molecule simulation ADME[4] and toxicity prediction Complex-mixture simulation Solid-material simulation Catalysis or synthesis optimization Finite element method Supply-chain optimization	Supply-chain-disruption modeling Self-driving robots Credit-risk management Financial-crime detection Personalized medicine Automated drug recommendations Multiscale production optimization

Outlook Fault-tolerant quantum computing is expected between 2025 and 2030, based on announced hardware road maps for gate-based quantum-computing players.

[1]Physical qubits needed to achieve 1 logical qubit varies per qubit technology. Estimates included are based on current error rates for superconducting qubits.
[2]Use cases will combine algorithm archetypes or the archetype is not yet confirmed.
[3]QM: quantum mechanics; MD: molecular dynamics; MM: molecular mechanics.
[4]Absorption, distribution, metabolism, and excretion.
Source: McKinsey analysis

Quantum annealers that contain over 5,000 physical qubits can already solve certain types of optimization problems. There is evidence, for example, that quantum annealers can outperform HPCs on the simulation of specific material properties.[9] A select few organizations in finance, automobiles, and logistics are already experimenting with quantum computing for optimization purposes. Other relevant use cases in these and other industries could follow when fault tolerance or more powerful annealers are achieved. The number of qubits for quantum annealing has doubled every two years, while its error rate has stayed consistent. While the value of increasing the number of qubits versus qubit quality remains under debate, as the capacity of quantum annealers to handle large-scale optimization problems increases, some experts believe quantum annealers could surpass HPCs for a large class of optimization use cases.

The fault-tolerant phase. This phase has three stages. The first stage will be marked by the first fully error-corrected quantum computer, which will be able to operate as intended even when some of its components fail. This advancement will unlock a broad range of use cases, in areas such as drug and catalysis design. In the second stage, quantum computers will contain more than 1,000 error-corrected logical qubits, which corresponds to roughly a million physical superconducting qubits at current error rates. This stage marks the beginning of significantly expanded computational power and data-handling capability, which can help solve more data-heavy problems (such as optimizations involving large-scale traffic or supply chains) and achieve valuable speedups, even for algorithms with only quadratic speedups.

In the final stage of the fault-tolerant phase, there will be a universal quantum supercomputer that contains quantum random access memory (QRAM), the quantum equivalent of RAM. QRAM will dramatically increase the amount of data that can be coherently processed (using only quantum tools). QRAM may be indispensable for some use cases that involve processing large volumes of data, such as quantum machine learning. At this point, experts hope to have found ways to efficiently encode conventional data into quantum computers, which is the final step to unlock the full potential of quantum AI.

When might we reach the fault-tolerant phase? Most hardware players are hesitant to reveal their development road maps, but a few have publicly shared their plans. Five manufacturers have announced plans to have fault-tolerant quantum-computing hardware by 2030. If this timeline holds, the industry will likely establish a clear quantum advantage for many use cases by then.

IBM, for example, announced plans to release its 1,000 physical-qubit machine by the end of 2023, which actually marks the beginning of the late pre-fault-tolerant stage and potentially viable quantum-computing use cases.[10] If private-sector use of such gate-based systems is successful, it could trigger increased investments from the industry and accelerate the development and implementation of quantum computing. However, again, many experts warn against using qubits as the measure of progress.

Google, which, like IBM, manufactures quantum computers using superconducting circuits, aims to build a useful, error-corrected quantum computer within the decade.[11] Hardware manufacturer PsiQuantum, which uses its silicon photonics-based architecture to manufacture key quantum components in a conventional silicon-chip foundry (through a partnership with chip manufacturer GlobalFoundries), expects to stand up the manufacturing processes necessary to assemble its large-scale quantum computer by the middle of this decade. Well within this decade, PsiQuantum anticipates seeing applications enabled by its quantum computer.

---

[9] Andrew D. King et al., "Scaling advantage over path-central Monte Carlo in quantum simulation of geometrically frustrated magnets," *Nature Communications*, February 2021, Volume 12, nature.com.
[10] Jay Gambetta, "IBM's roadmap for scaling quantum technology," IBM, September 2020, ibm.com. The balance between—and value of—quality and quantity of qubits is under debate. In a system with 100 qubits, each qubit can perform roughly a single operation before the entire quantum-computing system loses coherence. Some error-mitigation strategies may help, but systems with 1,000 qubits will not achieve their anticipated performance without sufficiently high-quality qubits.
[11] Erik Lucero, "Unveiling our new Quantum AI campus," Google, May 2021, blog.google.

Besides qubit count and error rates, many elements need to be in place to make quantum computing effective. Constraints include the lengths of time a quantum computer can run without interruption, the speed at which it can process inputs, and the level of connectivity between different qubits.

Value at stake for four industries expected to realize earliest use cases

While the viability and value of use cases is uncertain given the immaturity of the quantum-computing technology and industry, our research and modeling indicate that four industries could be among the first to reap the value of quantum computing. Collectively (and conservatively), the value at stake for these industries—pharmaceuticals, chemicals, automotive, and finance—could be in the range of $300 billion to $700 billion, with use cases in chemicals expected to potentially generate half that value (Exhibit 6). These estimates and the exploration of potential use cases to follow are intended to guide research toward areas that could generate significant value rather than serve as definitive projections.

Quantum computing in pharmaceuticals

Quantum computing has the potential to revolutionize the research and development of molecular structures in the biopharmaceuticals industry. New drugs take an average of $2 billion and more than ten years to reach the market after discovery.[12] Quantum computing could make R&D dramatically faster and more targeted and precise by making target identification, drug design, and toxicity testing less dependent on trial and error and more efficient (Exhibit 7). A faster R&D timeline could get products to the right patients more quickly and more efficiently—in short, it could improve more patients' quality of life.

Quantum computing is expected to be useful during target identification and validation, which aims to understand the role of a particular gene or protein in a disease. Here, it could be used to predict protein structures reliably and efficiently, which is essential to predicting key proteins' interactions with drugs. This capability would be a significant advancement because the mathematical complexity of predicting the structure of a protein, also known as protein folding, exceeds the capabilities of today's most powerful computers. Instead, protein structures are determined by expensive and error-prone X-ray and nuclear magnetic resonance (NMR) experiments. As a result, pharmaceuticals companies sometimes develop drugs without ascertaining the structure of a protein, accepting the risk of a trial-and-error approach in subsequent steps of drug development. Artificial intelligence has helped fuel some recent progress in this area.[13] However, challenges associated with simulations based on conventional computing remain in areas such as protein-to-protein interactions.

Quantum computing can be especially beneficial for hit generation and validation, which is the discovery of small molecules that can form the basis of new treatments.[14] While researchers already use computer-aided drug design (CADD), the techniques are based on heuristic approximations of quantum-mechanical effects, limiting their accuracy. Accurate quantum simulations would massively increase the accuracy and applicability of CADD, allowing CADD outputs to replace costly experiments. And because current CADD techniques are limited to small- to medium-sized drug candidates, sufficiently powerful quantum computers could one day allow pharma companies to solve problems in some biologics (which are larger and more complex drugs made from living organisms and their outputs) and perform in silico (computer-generated) search and validation of experiments more efficiently than they can with present-day techniques.

At the lead optimization stage, when the most promising leads are refined for improved effectiveness, quantum computing may enhance a drug's absorption, distribution of the drug within the organism, metabolism, and excretion. For instance, quantum computing could use simulations to estimate drug

---

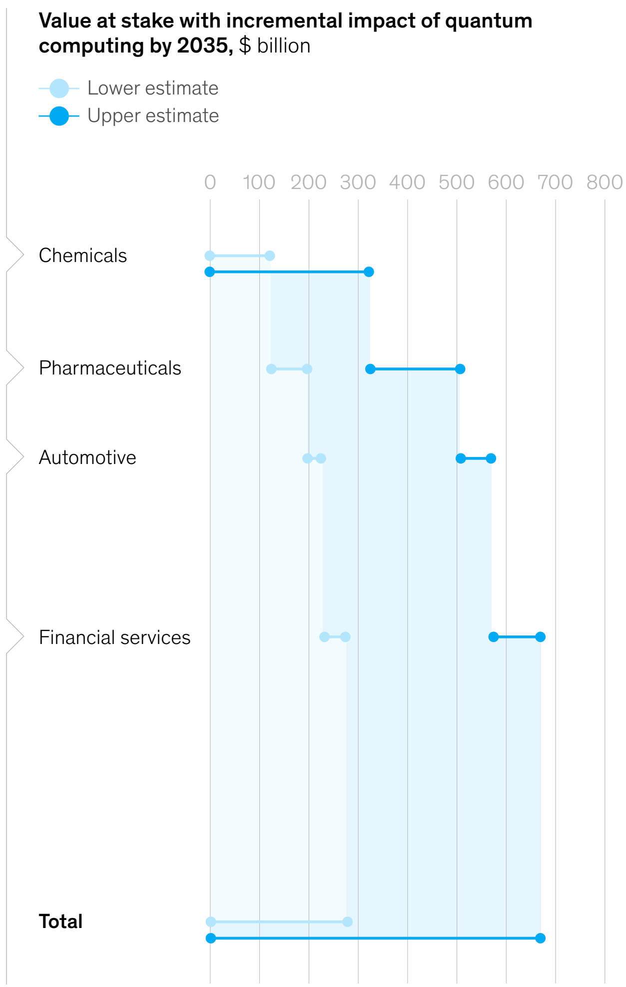
[12] Anna Heid and Ivan Ostojic, "Recalculating the future of drug development with quantum computing," October 2020, McKinsey.com.
[13] Alphafold Protein Structure Database, EMBL-EBI, November 23, 2021, alphafold.ebi.ac.uk.
[14] For more on technology in pharmaceuticals R&D, see Matthias Evers, Anna Heid, and Ivan Ostojic, "Pharma's digital Rx: Quantum computing in drug research and development," June 2021, McKinsey.com.

Exhibit 6

Conservatively, we estimate that the value at stake in pharmaceuticals, chemicals, automotive, and finance use cases could be up to nearly $700 billion.

Economic value: Low, Medium, High

Industry, key segment for quantum computing	Economic value ~2025–30	Economic value ~2030–35
Global energy and materials		
Oil and gas	Low	Medium
Sustainable energy	Medium	High
Chemicals	Medium	High
Pharmaceuticals and medical products		
Pharmaceuticals	Medium	High
Advanced industries		
Automotive	Low	Medium
Aerospace and defense	Low	Medium
Advanced electronics	Low	Medium
Semiconductors	Low	Medium
Financial industry		
Financial services	Low	Medium
Telecom, media, and technology		
Telecom	Low	Medium
Media	Low	Low
Travel, transport, and logistics		
Logistics	Low	Medium
Insurance	Low	Low



Note: Viability and value of use cases is uncertain due to the immaturity of quantum-computing technology and the industry; given that business-value estimates are speculative and on the conservative side, they are intended to guide research toward areas of quantum applications with a high value potential, rather than to serve as definitive projections for business value.
Source: McKinsey analysis

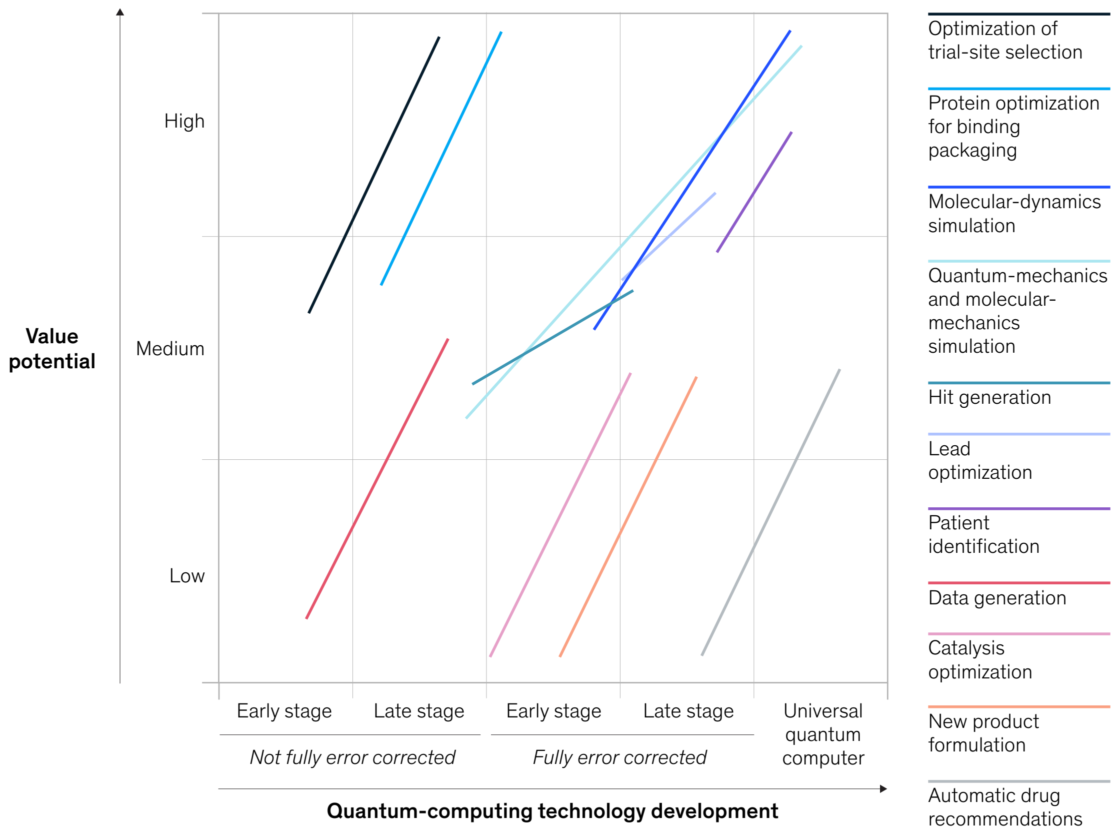
candidates' solvency through the blood-brain barrier, which currently blocks most therapeutic agents from entering the brain. The technology is also expected to yield more accurate predictions for activity and safety considerations such as toxicity for organ systems, dosing, and solubility optimization.[15]

Overall, quantum CADD may lead to significant cost savings and speedier product optimization, shortening the time between patent application and new drugs reaching patients. Even a 10 to 20 percent improvement from lab-based R&D to CADD would lead to savings of $33 billion to $66 billion, which could allow for the

[15] For a more detailed overview of use cases in drug discovery, see Maximillian Zinner et al., "Quantum computing's potential for drug discovery: Early stage industry dynamics," *Drug Discovery Today*, July 2021, Volume 26, Number 7, pp. 1680–88, sciencedirect.com.

Exhibit 7

Quantum computing may be applicable in its early stages in pharmaceuticals.



Note: Potential value ranges are estimates.

development of other products in the pipeline. While it is difficult to estimate how much revenue or patient impact such advances could create, in a $1.5 trillion industry with average EBIT margins of 16 percent (by our calculations), even a 1 to 5 percent revenue increase would result in $15 billion to $75 billion of additional revenues and $2 billion to $12 billion in EBIT.

The most expensive stage of the development process is clinical trials, which account for about two-thirds of drugs' R&D costs.[16] According to experts we interviewed, conventional AI and machine learning can already enhance clinical trials. Quantum computing could further optimize tasks such as patient identification and stratification (division into subgroups) and population pharmacokinetic modeling (which is used to describe and investigate the time course of drug exposure in patients) to optimize clinical trials. Quantum computing may be used to simulate outcomes based on the characteristics of selected patients and improve drugs' efficacy and safety. In trial planning and execution, quantum computing could optimize the selection of the trial sites.

Quantum computing could also use machine-learning algorithms to fill in missing data points at every stage of R&D. This application is particularly valuable when data are scarce, as with rare diseases. Of course,

[16] "Modernizing clinical trials: Digital technologies and the cloud," FiercePharma, pages.awscloud.com/rs/112-TZM-766/images/AWS_ClinicalTrials_Whitepaper_Final.pdf.

this application comes with the risk of creating bias, which is built in whenever synthetic data are created using any method. Efficiency improvements through quantum computing–enabled AI in the order of 5 to 10 percent would result in annual cost savings of $11 billion to $22 billion. This assumes only an incremental enhancement to savings generated by HPC, which is estimated to be more than 20 percent, based on basic optimization techniques such as elimination of underperforming testing sites.[17]

Production
In the production of active ingredients, quantum computing may aid in the calculation of reaction rates, optimize catalytic processes, and create significant efficiencies in the development of new product formulations—such as making product formulations more cost-efficient by using a mix of less expensive ingredients, or increasing the use of inexpensive ingredients while using fewer expensive ones. Production costs in pharma are about $150 billion to $200 billion per year, and even a 10 percent improvement in process efficiency would save the industry between $15 billion and $20 billion per year. Digitalization such as process automation can already save 10 to 25 percent of costs.[18]

Other use cases
Further down the value chain, quantum computing in pharma could optimize logistics and improve the supply chain. Toward market access and commercial, it may even automate drug recommendations to help healthcare providers and health systems optimize and personalize treatment for patients.

Of course, the potential benefits of quantum computing outlined above are relative to the technology available to the pharmaceuticals industry today. Alternative technologies may ultimately capture part of this value, particularly in areas such as optimization and AI. In addition, risks and challenges remain, including the pace and sophistication of regulation, the ability to ensure patient safety, and public trust in the technology and the decisions it facilitates.

Quantum computing in chemicals
In chemicals, quantum computing can create significant value in R&D, production, and supply-chain optimization (Exhibit 8).[19]

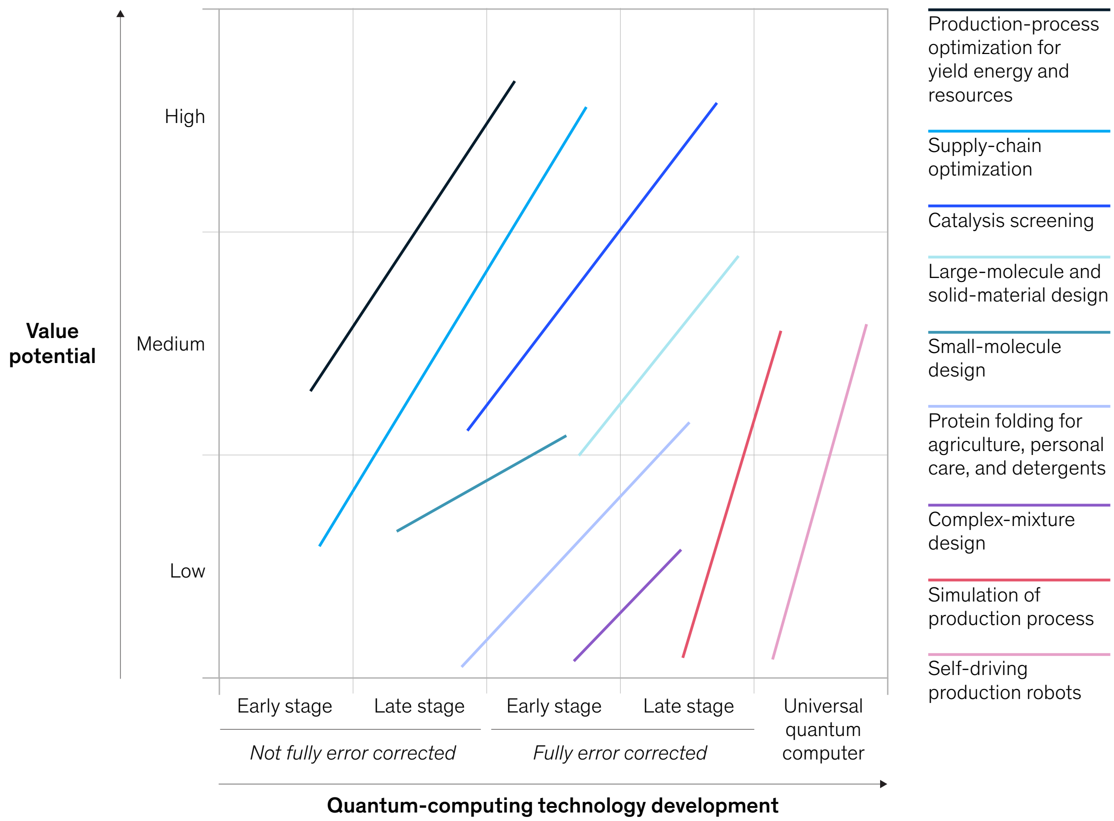
R&D
The design of new small molecules or polymers relies on accurate predictions of molecular properties. While chemical researchers have already made a lot of headway with conventional computational-chemistry tools to streamline R&D, today's tools rely on approximations and typically provide only partial information on molecules' properties. Quantum computers will enable exact quantum-mechanical simulations in situations where no reliable computational methods exist today, creating savings and revenue opportunities.

Virtualizing large parts of current trial-and-error, lab-based experiments has the potential to massively reduce the R&D cost of a new product. If quantum computing lives up to its promise of accurately predicting molecular processes, this could nearly eliminate lab-based experiments for new-product development, which can amount to $24 billion to $64 billion, about 30 to 80 percent of R&D spend. Instead, the optimization of newly identified products would become an iterative exchange between quantum simulation and lab-based validation. Significant cost reductions in quality control and toxicity testing could also become possible, though some testing will rightly continue to be required by law. While some lab-based

[17] Ibid.
[18] Philipp Espel, Michael Herbener, Frederic Rupprecht, Christian Schröpfer, and Andreas Venus, "How industrial companies can cut their indirect costs—fast," April 2020, McKinsey.com.
[19] For more information on the impact of quantum computing on chemicals, see Florian Budde and Daniel Volz, "The next big thing? Quantum computing's potential impact on chemicals," July 2019, McKinsey.com.

Exhibit 8

Quantum computing could have diverse applications in chemicals.



Note: Potential value ranges are estimates.

experiments will remain legally necessary, quantum computers could predict many instances of toxicity at the early stages of development.

Quantum computing's impact on product development could be dramatic. The significant computing power could spark breakthroughs that disrupt markets or solve long-standing problems, such as how to create more environmentally safe chemicals to protect crops. For instance, early progress in the design of protein-based crop protection promises a more environmentally friendly alternative to traditional pesticides and herbicides, as it only targets the DNA of a specific species without posing risks to the environment and human health. Quantum simulations could significantly speed up development of this innovation by helping researchers understand how molecules target specific DNA strands.

Quantum computing is also expected to improve the development of new product formulations by modeling the complex molecular-level processes involved. For example, a new cleaning-product formulation is currently based on trial-and-error experiments and simple theoretical models based on conventional computing. Quantum computing could calculate exactly how, for example, detergent molecules interact with a wine stain on a fiber and identify the best active ingredients and formulations to remove it. A team using a quantum computer and the appropriate algorithm could reduce the required calculation time from days to seconds.

We expect the main revenue opportunities to come from segments of the chemicals industry that have medium to high innovation pressure, such as personal care, agriculture, detergents, pigments and paints, and petrochemicals. These subsegments collectively amount to total revenues of more than $2.1 trillion.[20] An incremental revenue uplift of 1 to 5 percent in these subsegments corresponds to $21 billion to $105 billion. The lower estimate is comparable to the cumulative revenue lift for plastics that resulted from the development of biodegradable plastics.[21] Of course, additional revenue from new and improved products could be significantly higher because no one knows the new products that might be discovered and created. Some experts we interviewed said that revenue gains of up to 50 percent are possible in specific segments. However, skeptics point out it may be difficult to make a business case for most products because the chemicals industry is fragmented and the cost of approval and scaling up production of new products is high. While a few pioneers are already experimenting with quantum computing, full adoption in the chemicals industry may not happen until quantum computing is widely accessible at low cost.

Production

Simulations based on quantum computing could be used to better understand reaction mechanisms, design improved catalysts, optimize process conditions, and avoid production issues.

The experts we interviewed highlighted the high value potential of catalyst development. In addition to possible energy savings on existing production processes—a single catalyst can produce up to 15 percent in efficiency gains—innovative catalysts may enable the replacement of petrochemicals by more sustainable feedstock or the breakdown of carbon for CO_2 usage. This is likely to become more important given that the cost of energy and CO_2 emission is expected to rise. Experts also pointed out that while catalysis is a promising use case, improvements in algorithms and software will influence the rate of adoption.[22]

The spend on production in the chemicals industry is about $800 billion; roughly 50 percent of production processes rely on catalysis. This amount includes the production of all major polymers, which is a subsegment with high value at stake. A 5 to 10 percent efficiency gain, which experts we interviewed consider realistic, would amount to $20 billion to $40 billion.

Quantum optimization could also improve production processes by fine-tuning conditions to generate fewer byproducts, optimize yields, or reduce resource requirements. Quantum-powered simulations of the overall production process—from the microscopic quantum-mechanical processes to the larger mechanical details—could help to avoid occasional production issues that stem from faulty designs. These use cases would require large-scale quantum computing but could save another 5 to 10 percent, or $40 billion to $80 billion.

Supply-chain optimization

Based on our research, we estimate that the average supply-chain spend on chemicals is about 9 percent of revenue, which corresponds to about $350 billion. This number is expected to increase as companies source more sustainable materials. Because suppliers of such raw materials are often more scattered, chemical companies' supply chains will become more complex, with costlier logistics.

Although many elements, such as end-to-end processes, can make supply chains more efficient, quantum computing may be able to increase efficiency of supply and distribution chains by optimizing the supply-

[20] Based on added revenues of relevant segments combining Capital IQ, MarketsandMarkets, and Statista databases.
[21] MarketsandMarkets database, November 23, 2021, marketsandmarkets.com; Statista database, November 23, 2021, statista.com.
[22] For a technical reference on algorithmic improvements for catalysis, see Vera von Burg et al., "Quantum computing enhanced computational catalysis," *Physical Review Research*, July 2021, Volume 3, Issue 3, journals.aps.org.

chain network, logistics, and inventory. Experts indicated in interviews that the most significant value of these capabilities could come from the ability to quickly reoptimize supply chains and logistics in reaction to disruptions. If this greater efficiency results in even a 5 to 10 percent overall savings in supply-chain costs—which appears realistic based on our research and expert input—the savings would amount to $18 billion to $35 billion. This target is viable, since conventional optimization methods can already achieve efficiency improvements near 40 percent, and quantum optimization would speed up and improve this process.

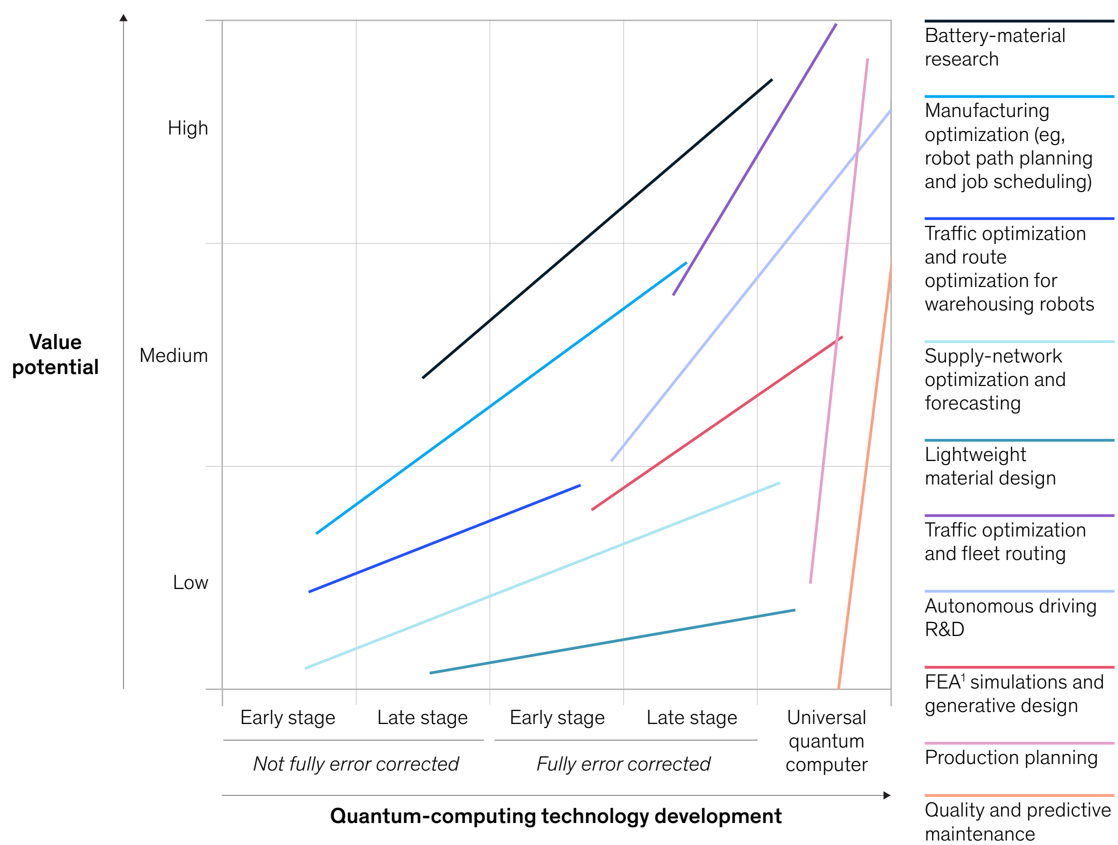
Our discussion of quantum computing's potential value for the chemicals industry is relative to the benefits of currently available technology. Alternatives to quantum computing may capture some of this value, particularly in areas such as optimization and AI.

Quantum computing in automotive

Quantum-computing use cases in the automotive sector are found in R&D and product design, supply-chain management, production, and mobility and traffic management (Exhibit 9).[23]

Exhibit 9

Several quantum-computing use cases in the automotive sector are expected to become viable with some error correction.



Note: Potential value ranges are estimates.
[1]Finite element analysis.

[23] For more information on the impact of quantum computing on automotive, see also Ondrej Burkacky, Niko Mohr, and Lorenzo Pautasso, "Will quantum computing drive the automotive future?" September 2020, McKinsey.com.

R&D and product management

One of the most interesting use-cases is the speedup of finite element simulations that OEMs and suppliers use to simulate vehicles' mechanical stability, aerodynamic properties, thermodynamic behavior, and NVH characteristics. Increasing the speed and precision of these simulations may create value by reducing the cost of prototyping and testing and by creating better, higher-performance designs at a lower cost. We estimate that a 5 to 10 percent reduction in prototyping costs could lead to $2 billion to $4 billion in savings.

Quantum computing will also likely advance autonomous driving. Faster machine-learning models can shorten R&D cycles, and quantum computing–generated synthetic data can reduce the cost of collecting and labeling data and enhance vehicles' performance in uncommon situations—which, therefore, come with limited real-world training data.

In addition, automotive OEMs are increasingly interested in the development of advanced future fuels, where quantum computing could play an important role. It could, for instance, aid in the design of better materials for hydrogen storage. And battery development will also benefit from quantum-chemistry simulations used to identify new or improved materials and better cell designs, resulting in a lower cost per kilowatt-hour. We know of at least one battery manufacturer that has performed research suggesting that quantum computing can help in battery design. For an electric-vehicle market that we project to be worth about $240 billion in 2030, small improvements in the 5 to 10 percent range from quantum computing–based quantum-chemistry simulations can create $12 billion to $24 billion in value.

Another promising area for quantum computing is in prototyping and testing, which, according to our research, currently accounts for 20 to 30 percent of the total $100 billion R&D cost of a new vehicle, including hardware components and the assembly and testing of vehicles. In the future, quantum computing's speed and ability to perform complex tasks that conventional computing can't handle will allow for more virtual testing—and will reduce the number of test vehicles required. High-performance computing has already reduced the cost of prototyping and testing by 50 percent.[24] Quantum computing is likely to enable further savings by speeding up calculation time, making room for more tests, and improving accuracy. An additional improvement of 5 to 10 percent would create cost savings of $1.5 billion to $3 billion across all automotive OEMs, but it would require a fully fault-tolerant quantum computer.

Quantum computing could also help OEMs by facilitating better designs and performance at a lower cost. OEMs already continuously work to reduce production cost and improve vehicle performance during the lifetime of a vehicle model. They usually achieve savings of 0.3 to 0.5 percent per year on production costs, or about $3 billion to $5 billion. The savings usually come from identifying and eliminating overspecified parts or optimizing the manufacturing process. The vastly increased simulation speed from quantum computing should allow for many more iterations of design options that help optimize specifications across the entire vehicle, to the point of having close-to-optimal designs at the start of production. Our analysis suggests that, in theory, starting production with the elements of optimal cost and performance in place would create an additional $3 billion to $5 billion of value per year. Industry experts we interviewed stated that even a tenfold speedup would be highly valuable.

An extension of these simulation techniques is generative design, which could also take advantage of the quantum speedup of finite element simulations and quantum-optimization techniques. Computer-generated designs have already been shown to be superior to human-made designs in some scenarios, such as in optimizing heat-exchanger performance. However, quantum generative design has been limited

[24] "HPC accelerates dream car design," Huawei, 2017, huawei.com.

by computation time and modeling complexity. Quantum computing may be the key to enabling generative design's wider use.

Supply-chain management

Major automotive companies experience a month-long supply-chain disruption on average every 3.7 years, which results in about $15 billion per year in economic damage for car manufacturers.[25] Conventional high-performance computing cannot handle global supply-chain networks' ever-increasing complexity. However, end-to-end quantum-computational simulations of automotive supply networks could help manage acute disruptions by simulating the effects of possible countermeasures and identifying the most cost-effective solution. These simulations could also stress-test existing supply networks and identify the best combination of cost, lead time, and resilience. Even a 5 to 10 percent decrease in loss from disruption management, which experts consider realistic, would lead to $0.75 billion to $1.5 billion in savings. Of course, in addition to the availability of sufficiently powerful quantum hardware, digitization and centralization of all relevant supply-chain data will be key; the master pool of data will need to serve many production sites, warehouses, and supplier facilities.

Manufacturing

With OEMs incurring about $500 billion in annual manufacturing costs (excluding direct materials) per year, even a 2 to 5 percent productivity gain—consistent with typical annual improvement rates in the industry—through quantum computing–enabled optimization would create $10 billion to $25 billion of value per year. As the number of vehicle configurations has exploded in recent years, neighboring vehicles on the assembly line are rarely the same. Because different configurations require slightly different processing times at each station, optimal job scheduling and line balancing has become increasingly difficult, especially since the high level of complexity and the relatively short planning cycles make computerizing the planning process difficult. Quantum computing can help create optimized job schedules, eliminate avoidable inefficiencies, and increase productivity.

Quantum computing could also improve process costs, by, for example, optimizing path planning in complex multirobot processes (the path a robot follows to execute a task) such as welding, gluing, and painting. Current HPCs cannot manage the complexity of typical multirobot path planning, but quantum computer–optimized paths can shorten cycle times and reduce production costs.

Many experts believe that AI-based use cases, such as automatic optical inspection and predictive maintenance, can also benefit from quantum-enhanced AI workflows. However, there are currently few, if any, quantum AI algorithms that are proven to work. Many challenges also remain, such as the slow input of data—relative to the speed of quantum computing—that can erase any potential speed advantage.

Mobility and traffic management

Quantum computing promises to make today's difficult tasks faster and easier. Specifically, quantum computing could simulate highly complex traffic systems for large metropolitan areas—or even entire countries—to inform decisions about infrastructure investment and reduce average travel times. Traffic simulation and optimization may be especially useful for finding the optimal balance between road and rail maintenance and maximum network capacity. Similarly, real-time traffic prediction and coordinated route optimization for vehicle fleets steered by a central computer can reduce system-level traffic congestion.

[25] For more information, see "Risk, resilience, and rebalancing in global value chains," McKinsey Global Institute, August 2020, on McKinsey.com.

The potential value created by quantum computing as outlined in all of these use cases is relative to the value generated in the automotive industry with technology available today. However, future technology alternatives may compete with quantum technologies and may capture part of this value.

Quantum computing in finance

The financial industry operates based on principles of trust and safety; most financial products rely on secure data and communication channels and on reliable ways to verify user identity. Most widely used cybersecurity tools and techniques, particularly RSA cryptography, will not be secure against mature quantum technology. While this development is years into the future, financial institutions will need to shift their data-security strategies and consider adopting RSA alternatives, such as quantum encryption (quantum key distribution)—or enhancing conventional encryption (post-quantum cryptography) to drastically reduce the likelihood that it will be broken by a quantum computer.[26]

Compared to the disruptive effect of quantum decryption, quantum use cases may offer a more incremental benefit to financial institutions' operations. Advanced computational techniques that work with increasingly complex products and operations are already ubiquitous in the financial sector; areas such as risk management and algorithmic trading already use the most advanced version of conventional computing resources, and the key challenges involve data quality and availability. However, better computational techniques can further optimize operations or reduce costs by lowering the energy consumption of calculations across clusters of CPUs and GPUs.

The most promising use cases for quantum computing are in portfolio and risk management. Quantum machine-learning methods in areas such as fraud-prediction modeling and credit scoring may also become viable (Exhibit 10).

Use cases of quantum computing in the finance sector may be farther in the future than they are for the chemicals and pharmaceuticals industries. Short-term use cases may arise from quantum optimization, but their advantage is more speculative. However, the exploration is worthwhile because of the value at stake, which we estimate could be in the range of $100 billion. We lay out some possible use cases here.

Portfolio management

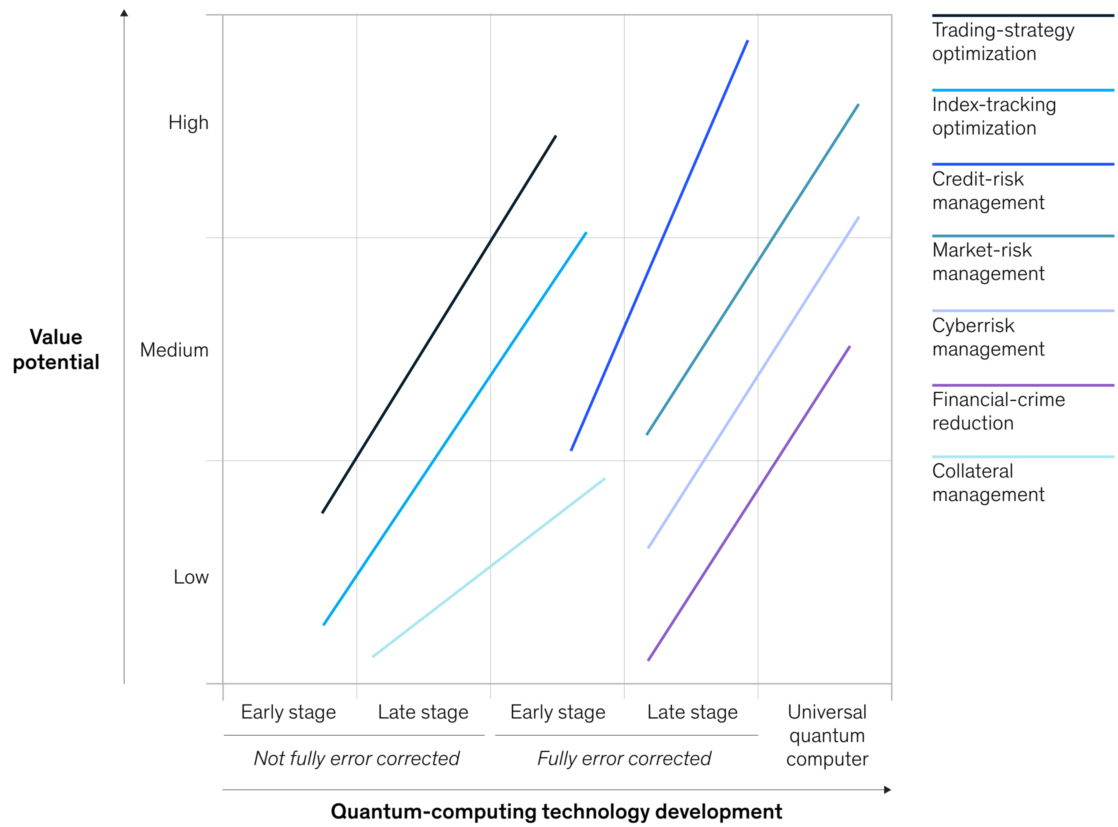
No matter the type of portfolio, its complexity increases with the number of assets it contains. Choosing a portfolio of ten assets from a potential list of 50 means 10 billion different possible combinations. Accounting for additional factors such as different sequences of buying and selling is intractable in conventional computing. While quantum computing cannot entirely resolve this challenge, it may be able to identify more optimal portfolios than existing conventional optimizers; it will also be able to do so more quickly, allowing more frequent portfolio updates.

Quantum computing for portfolio management could create business impact quickly in use cases such as trading-strategy optimization, index tracking for stock portfolios, and optimization of managed collateral. For instance, quantum computing could help develop trading strategies to determine when to buy or sell specific assets to achieve a specific rate of return at a set level of risk. Conventional optimization methods typically analyze millions of trading strategies over multiple hours. When hardware is sufficiently mature, quantum-optimization algorithms with quadratic speedups may be able to significantly increase the total number of scenarios to assess—and likely find better strategies.

[26] For more information on the impact of quantum computing on financial services, see Jens Backes, Miklos Dietz, Nico Henke, Jared Moon, Lorenzo Pautasso, and Zaheen Sadeque, "How quantum computing could change financial services," December 2020, McKinsey.com.

Exhibit 10

Finance has many computationally intense tasks that could benefit from quantum computing.



Note: Potential value ranges are estimates.

While expert opinions disagree on the long-term advantage of algorithmic trading and the impact of quadratic speedups, others argue that optimization through conventional machine learning or quantum-inspired algorithms can also significantly improve the performance of portfolios. Still, if quantum computing–powered portfolio strategies can improve an average return on investment by 1 to 2 percent per year, these strategies would generate an additional $36 billion to $71 billion.[27] Some experts argue that this number could be much higher, as use cases may extend to other areas of portfolio management such as index tracking (funds crafted to track an underlying group of assets). What's more, quantum computing through cloud services could make sophisticated techniques for portfolio management available to smaller players in the industry. This shift could produce significant value, as the total global value of assets under management is roughly $100 trillion.[28]

A similar approach could be used to optimize collateral management for loan portfolios. The overall risk and value of such portfolios depend not only on the risk and value of individual collateral assets, but also on their spread. For instance, if all the collateral in a loan portfolio depends on the same guarantor or is based on

[27] This estimate is based on $100 trillion in assets under management globally, according to Statista. Within this pool, 60 to 73 percent of US equity trading is algorithmic.
[28] Statista database.

securities in the same industry, the portfolio's overall risk would be higher than if the collateral were more diverse. Efficiently quantum-optimized loan portfolios that focus on collateral could allow lenders to improve their offerings, possibly lowering interest rates and freeing up capital. It is early—and complicated—to estimate the value potential of quantum computing–enhanced collateral management, but as of 2021, the global lending market stands at $6.9 trillion, which suggests significant potential impact from quantum optimization.[29]

Risk

Accurately managing diverse types of risk is another important possible application. Minimizing a bank's overall risk is one of the most computationally intense tasks in banking because the risk depends on many factors. An accurate estimate of overall risk therefore comes from processing a vast pool of data. Quantum-computing techniques could decrease the computation time for a typical risk assessment that uses a classic Monte Carlo simulation from days to hours. By processing more samples faster, this approach can also help improve the accuracy of a bank's overall risk assessment. Our analysis reveals that the 20 largest global financial institutions collectively hold $800 billion as a capital buffer, with an annual cost of capital worth $80 billion. More accurate risk assessments that reduce this buffer by 1 to 2 percent would free up $0.8 billion to $1.6 billion per year. According to experts, this target is realistic, considering that savings of up to 10 percent have already been realized with traditional risk-management techniques, leaving the remaining room for improvement limited by legislation.

Risk management is also built into the pricing of complex derivatives, financial instruments whose price is derived from one or more underlying assets. Pricing a typical derivative contract can take several hours; faster pricing can therefore be a significant competitive advantage.

Quantum AI could be used to improve the selection of data features, which reduces the number of variables in a predictive model to the most relevant ones. This development allows for the timely analysis of larger data sets, more accurate models, and faster retraining for machine-learning models. These tools—particularly efficient training for machine-learning models—can be applied to specific tools in risk management. For instance, more accurate credit scoring can reduce credit risk. An improvement of 1 to 2 percent in the global default rate corresponds to a savings of $17 billion to $33 billion. This amount is comparable to the potential revenue increase through conventional risk analytics, which is $10 billion to $20 billion.[30]

While it is difficult to estimate the impact of quantum machine learning and AI to other areas of risk management, we expect them to affect the value lost to payment-card fraud, which is about $27.85 billion per year as of 2018.[31] Other potential areas of impact are cyberrisk mitigation and money-laundering detection, areas where industry experts say the 20 largest financial institutions currently spend about $11 billion a year; a decrease of 1 to 2 percent would lead to savings between $100 million and $200 million.[32] The impact of quantum machine learning remains a contested topic; while some experts are skeptical due to a limited number of viable use cases, others believe that in the future, quantum machine learning will have many high-value use cases beyond the ones we investigated.

Because of its computational intensity, experts we interviewed expect quantum risk management to be viable around 2030. But as with all possible quantum-computing use cases, the value generated is relative to the value of currently available technology, not compared to alternatives that may capture some of this value.

---

[29] The total global lending market is $6.9 trillion as of 2021, according to Research and Markets. Global data on default rates is unclear, but we conservatively estimate it to be 5 percent and assume a loss given default (the value of an asset that is lost in the event of a default) of 50 percent of the initial value of the loan.

[30] This estimate is based on a global lending market of $6.9 trillion as of 2021, according to Research and Markets, with an average of 3 percent return on loans and a conservative assumption on the default rates. Prior research suggests that revenue increases of 5 to 10 percent are attainable. For more information, see Rajdeep Dash, Andreas Kremer, Luis Nario, and Derek Waldron, "Risk analytics enters its prime," June 2017, McKinsey.com.

[31] "Card fraud losses reach $27.85 billion," Nilson Report, November 18, 2019, nilsonreport.com.

[32] Industry experts estimate that top financial institutions spend an average of $8 billion per year on management of cyberrisk and $3 billion a year on detection of financial crimes.

3 The path forward

In the mid term—until about 2030—quantum-computing use cases will have a hybrid quantum-HPC operating model. In the longer term, six key factors—funding, hardware access, standardization, industry consortia, talent, and digital infrastructure—will determine quantum computing's path to commercialization. Despite many unknowns, industry leaders should take concrete steps to prepare for the maturation of quantum computing.

A mid-term hybrid operating model

Before 2030, industry will likely see a hybrid computing-operating model that combines conventional computing with emerging quantum computing. For example, conventional HPCs may benefit from quantum-inspired algorithms for tasks such as products recommendations for customers and OLED (organic light-emitting diode) simulations.[33]

The scarcity of talent and expertise in quantum algorithms suggests that quantum software firms will work with leading corporations to identify and solve problems amenable to quantum computing. At the same time, quantum software firms will create hybrid quantum-conventional analytics workflows that integrate quantum algorithms into conventional computing use cases wherever they are beneficial; for annealing, the first instance of a hybrid solver is already available. Leading cloud and HPC providers will also integrate the best available quantum hardware into their services and facilitate the execution of hybrid quantum-conventional workflows: quantum technology will effectively be a coprocessor to conventional computing infrastructure.

Beyond 2030, intense ongoing research by private companies and public institutions will remain vital to improve quantum hardware and enable more—and more complex—use cases.

Six key factors affecting advances in quantum computing

Funding, accessibility, standardization, industry consortia, talent, and digital infrastructure will determine the rate at which quantum computing develops.

Funding

Public funding for quantum-computing research will continue to be crucial to the academic and start-up ecosystems. But with the commercialization of quantum computing underway and business use cases on the horizon, a further shift in balance from public to private funding will be required to efficiently fuel growth in the most business-relevant areas. Experts we interviewed have observed a marked increase in private funding in response to enthusiasm for quantum computing—to the point that there are not enough quantum-computing start-ups that can absorb the capital. However, the long-term development of the industry depends on a steady source of funding.

[33] Juan Miguel Arrazola et al., "Quantum-inspired algorithms in practice," *Quantum*, August 2020, Volume 4, pp. 307–31, quantum-journal.org.

The COVID-19 crisis has not dampened private investors' enthusiasm for the industry; several large investment rounds have been announced in 2021 so far, including $650 million, $450 million, and $100 million rounds for three North American start-ups.[34] To better support the global quantum-computing industry, small to midsize enterprises outside the United States will need better access to private investments. At the same time, investors should spread their funding across a wide swath of quantum-computing enterprises.

Accessibility

Democratized access to quantum hardware may significantly accelerate the identification and implementation of commercially valuable use cases. Making quantum hardware accessible as a cloud service—at affordable prices—will be key. While quantum-computing cloud services already exist, providers need to increase hardware capacity to meet growing demand. In addition, hardware and software providers should develop and promote a standardized, open-source, hardware-agnostic programming language to lower the barrier for software developers to engage in hands-on quantum programming.

Standardization

Industry standards for elements such as interfaces and programming languages will be important to simplify collaboration within the quantum-computing ecosystem. Similarly, performance metrics for quantum hardware are needed to create transparency and confidence for end users. Initial standardization efforts have focused on defining common terminology, performance metrics, and benchmarking.[35] However, benchmarking is intensely debated within the industry, especially since the performance of each quantum-hardware platform is still highly dependent on the specific metrics. While benchmarks will be important to help steer investments to promising solutions, it may still be too early to commit to industry-wide performance benchmarks.

Collaboration and industry consortia

To maximize the industry's pace of innovation and value creation, players need to find the right balance between collaboration and competition. Consortia of participants from across the quantum ecosystem, including academia, can serve as forums to drive standardization, identify viable use cases, and leverage quantum computing to address global challenges, such as climate change, while simultaneously advancing the technology and broadening the industry's reach. Industry and academic consortia have already formed in Europe and the United States, but they require continued commitment from all industry participants to effectively move the whole industry forward.

Talent

Talent scarcity is a major concern in quantum computing. Quantum-computing companies currently recruit candidates with research backgrounds such as quantum physics, engineering, and statistics—profiles that are already in high demand. Our research shows that short-term talent shortages can represent a serious risk, particularly when more enterprises enter the quantum-computing arena and must to compete with quantum communication and sensing companies, which will be looking for similar candidates. We predict that talent shortages will only be resolved after 2030 without active mitigation measures.

Industry leaders should respond to the implications of this shortfall and collaborate with universities through partnerships and funding to fill some of the gap. Universities may also introduce more interdisciplinary quantum-computing degree programs—and update their STEM programs—to meet the need for quantum-computing talent.

[34] For more details, see "The Quantum Technology Monitor," September 2021, McKinsey.com.

[35] "Information technology – Quantum computing – Terminology and vocabulary," ISO, November 23, 2021, iso.org; "P7130 – Standard for quantum technologies definitions," The Institute of Electrical and Electronics Engineers (IEEE), November 23, 2021, standards.ieee.org; "P7131 – Standard for quantum computing performance metrics & performance benchmarking," IEEE, November 23, 2021, standards.ieee.org.

Digital infrastructure

All quantum-computing use cases require machine-readable input data that are readily available from central repositories and digital and analytical workflows into which a quantum computer can be integrated. However, many fields that may benefit from quantum computing still lack basic digital infrastructure. Enterprises will need to evolve their data platforms, data governance, and data pipelines to make the right data sources available for quantum computation—and integrate the outputs into business processes and workflows.

Leaders of industries with promising quantum-computing use cases should ensure that the necessary digital infrastructure is in place when quantum hardware progresses enough to enable industry-specific use cases. In the meantime, quantum-software providers should embed their quantum-computing offerings into conventional digitization services and help users set up integrated business solutions that tap into the power of quantum computing.

Getting started

Leaders outside the quantum-computing industry can take five concrete steps to prepare for the maturation of quantum computing.

1. Follow industry developments and actively screen quantum-computing use cases with an in-house team of quantum-computing experts or by collaborating with industry entities and by joining a quantum-computing consortium.

2. Understand the most significant risks and disruptions and opportunities in their industries.

3. Consider whether to partner with or invest in quantum-computing players—mostly software—to facilitate access to knowledge and talent.

4. Consider recruiting in-house quantum-computing talent. Even a small team of up to three experts may be enough to help an organization explore possible use cases and screen potential strategic investments in quantum computing.

5. Prepare by building digital infrastructure that can meet the basic operating demands of quantum computing; make relevant data available in digital databases and set up conventional computing workflows to be quantum-ready once more powerful quantum hardware becomes available.

Quantum computing could fuel explosive value generation for diverse industries. While the technology is still under development, it is evolving quickly. Because of its potential—and because early movers can shape the way quantum computing is eventually used—leaders in every industry should stay updated on developments in quantum computing and be alert to the opportunities and threats the technology brings. The learning starts now.

Matteo Biondi and **Anna Heid** are consultants in McKinsey's Zurich office, where **Ivan Ostojic** is a partner; **Nicolaus Henke** is a senior adviser and senior partner emeritus in the London office, where **Lorenzo Pautasso** is a consultant; **Niko Mohr** is a partner in the Düsseldorf office; **Linde Wester** is a consultant in the Amsterdam office; and **Rodney Zemmel** is a senior partner in the New York office.

Glossary

fault tolerance: Technical noise in electronics, lasers, and other components of quantum computers lead to small imperfections in every single computing operation. These small errors ultimately lead to erroneous computation results. Such errors can be countered by encoding one logical qubit redundantly into multiple physical qubits. The required number of redundant physical qubits depends on the amount of technical noise in the system. For superconducting qubits, experts expect that about 1,000 physical qubits are required to encode one logical qubit. For trapped ions, due to their lower noise levels, only a few dozens of physical qubits are required. Systems in which these errors are corrected are fault tolerant.

gate-based quantum computer: A quantum computer that can be programmed through a sequence of gate operations to execute computations, similar to a conventional computer. Also known as the circuit model for quantum computing.

photonic network: A quantum-computing hardware platform that various start-ups are developing. Each qubit occupies a photonic waveguide (a structure for guiding light). Photonic quantum computers have far less stringent cooling requirements than superconducting circuits.

quantum advantage: The practical advantage of a quantum-computing application over the best conventional alternative: the quantum application needs to bring a sizable business uplift. For instance, because quantum hardware is still immature compared to conventional high-performance computers, a quantum algorithm that provides a significant quantum speedup may not yet have a practical quantum advantage.

quantum annealer: A specific type of quantum processor tailored to solve certain optimization problems. For example, one type of quantum annealer is constructed using arrays of superconducting circuits.

quantum gate: A basic operation on quantum bits and the quantum analogue to a conventional logic gate. Unlike conventional logic gates, quantum gates are reversible. Quantum algorithms are constructed from sequences of quantum gates.

quantum speedup: The improvement in speed for a problem solved by a quantum algorithm compared to running the same problem through a conventional algorithm on conventional hardware.

quantum supremacy: An event defined by the resolution of a quantum computation that cannot be done by the most powerful existing conventional computers in a practical amount of time.

qubit: Also known as a quantum bit, a qubit is the basic building block of a quantum computer. In addition to the conventional—binary—states of 0 or 1, it can also assume a superposition of the two values.

spin qubits in semiconductors: A quantum-computing hardware platform that is under development at multiple start-ups and companies. In theory, it harnesses the spin of an electron in a semiconductor or insulator such as silicon or a diamond. Similar to photonic quantum computers, spin qubits have far less stringent cooling requirements than superconducting circuits.

superconducting circuits: Quantum-computing hardware that leverages superconductivity to minimize electrical resistance and enhance quantum effects at the macroscopic scale. The main challenges with this hardware involve error correction and scaling beyond a few thousand qubits while maintaining high qubit quality and addressing problems with wiring and cooling.

trapped ions: A quantum-computing hardware platform that contends with superconducting circuits for the status of "most developed." It functions by tapping into the energy of ions trapped by electromagnetic fields. As each ion is given by nature, every qubit is essentially the same, and errors are less likely. The number of qubits per computing system is projected to double every year, but scaling challenges remain.

ultra cold atoms: A quantum-computing hardware platform in proof-of-concept phase. Majority of ultra-cold atom hardware is developed for specific research applications in quantum simulation of complex materials and optimization; some versions are suitable for universal quantum computing.