

The next tech revolution: quantum computing

As part of its strategic partnership with Viva Technology, **McKinsey & Company** is publishing a series of articles looking at seven areas of technology that are potentially the most disruptive: Quantum computing, Cybersecurity, Connectivity & 5G, Cloud computing, AI, Digital ID, and Biotechnologies; as well as two major shifts for society: Future of work and Digital ecosystems



The next tech revolution: quantum computing

A powerful new form of computing could begin paying off for businesses within the next five years.
How best to prepare?

By Eric Hazan, Alexandre Ménard, Ivan Ostojic, and Mark Patel

Quantum computing is a fundamentally different type of computing from the laptops and smartphones we depend upon today. Instead of ever-smaller transistors, quantum machines operate along the principles of particle physics, and they are best at solving complex statistical problems with multiple variables.

An overview on quantum computing

Traditional computers use bits, representing zeros and ones, to solve all sorts of questions. But if you have multiple data streams, things quickly become more complicated, as current computers can handle only one set of inputs and make one calculation at a time. Qubits, which power quantum computers, are volatile and changeable in nature; more importantly, they can store values of one and zero at the same time, thanks to the principle of quantum superposition. This state allows quantum computers to solve multiple calculations, each with multiple inputs, simultaneously.

Quantum superposition is important, because it allows a group of qubits to explore different paths through a calculation. If programmed properly, the paths leading to incorrect answers are cancelled out, leaving the correct answer or answers highlighted.

For some very time-consuming problems, quantum computers can find a solution in far fewer operations than a conventional computer would need, which is why they appear to work so much faster.

Quantum computing has exactly the sort of computing power that would be needed to crack some of today's thorniest business questions and it has the potential to be both transformative and disruptive.

Puzzles like drug discovery or chemical synthesis could be rapidly accelerated by prototyping on a quantum computer. Quantum simulation would allow scientists to model complex molecules and simulate a drug's reaction inside the human body, or run advanced test on chemicals without risk of harm or waste. Quantum machines would narrow down the field of options, in crunching large sets of data, allowing technicians to test the substances identified as most likely by the quantum computer's analysis. This would revolutionize many types of R&D efforts.

Quantum computing's skills could tackle other business issues: Optimizing financial portfolios; designing efficient logistics networks that mix trucks, cars and scooters; training artificial intelligence (AI) to power autonomous vehicles—these are just a few examples of problems that traditional computers cannot crack with ease, but would potentially be short work for a powerful quantum computer.

Quantum computing will also transform cybersecurity. Even if it is unlikely to happen before 2030 or beyond, quantum computers will eventually be robust enough to factor the prime numbers underpinning current data security systems, meaning that businesses will need to completely rethink their cryptography systems.

Experts expect that pioneers in advanced industries, global energy and materials, finance, and travel and logistics might start generating significant value from quantum computers by 2025.¹ Other industries will follow, as quantum computing becomes accessible either through cloud vendors or on a standalone basis.

We must note, however, that this technology is in its infancy; The world saw quantum supremacy in late 2019, when a team at Google solved a longstanding mathematical problem that classical computers could not solve, with a basic quantum chip in just 200 seconds.

Some important technical challenges remain. In particular “noise or accuracy” is a big issue that has still to be solved: quantum computers make calculation errors up to 10-100 times higher than classical computers (due to noise and interference of qubits) and there is no error correction yet.

By the time technologists have wired up hundreds of thousands of qubits in sequence, then we will see the unleashing of quantum computing at scale.

+\$1 trillion

value potential by mid-2030s in 5 industries: finance, chemicals, pharmaceuticals, TMT, automotive

¹ The findings and insights presented in this article are substantially based on the work done by Alexandre Ménard, Ivan Ostojic, and Mark Patel, authors of the article *A game plan for quantum computing*, McKinsey Quarterly, February 2020, McKinsey.com. Sources for all figures in this article are included in that article.

How will quantum computers generate value for business?

Quantum computers have four fundamental capabilities that differentiate them from today's traditional computers:

1. **Quantum simulation**, where these computers will be able to model complex molecules
2. **Optimization** of multivariable problems at speed
3. **Quantum AI**, with better algorithms that could transform machine learning across industries
4. **Prime factorization**, which could revolutionize cryptography.

The best way to explore the business potential for quantum computing is to see how those capabilities would tackle a range of use cases. We analyzed more than 100 use cases,² and found they touch a wide range of problems and sectors.

Below, we illustrate four high-potential applications:

1. Slash development time for chemicals and pharmaceuticals with simulations

Molecule simulations are difficult to orchestrate with traditional computing, forcing scientists into the lab to experiment with chemical synthesis, adding to the cost and time invested in drug development. Quantum computers, on the other hand, are intrinsically well suited to tackle this sort of problem. After all, the interaction of atoms in a molecule is a quantum system. Experts believe that quantum machines will be able to model even the most complex molecules in our bodies. Each step along the way will yield new insights, driving product development, and potentially uncovering transformative new cures.

2. Solve optimization problems with unprecedented speed

So many business questions feature multiple variables. Where should I place robots on the factory floor? What is the shortest route for our delivery trucks? How can I optimize a financial portfolio's performance while minimizing risk? Answering these questions with traditional computing is arduous and produces hit-or-miss results. Quantum computers can work to narrow down options, and traditional computers can then

compare those results and select the best answer. Together, these technologies will solve thorny problems in much less time.

3. Accelerate autonomous vehicles with quantum AI

Self-driving cars could become a reality sooner with quantum computing in the mix. Currently, automakers are running hours of video, thousands of images, and terabytes of lidar data into complex neural networks to train AI to make crucial driving decisions, such as how to take a turn or where to speed up or slow down. Since quantum computers can perform multiple complex calculations in parallel, they could greatly accelerate the training of automotive AI systems. Now, this marriage of AI and quantum computing is unlikely to happen within the next five years, but it could prove promising over the longer term.

4. Quantum computing could transform cybersecurity

Today's data security systems power modern business, but quantum computing will revolutionize notions of security. Traditional encryption is based on manipulation of large prime numbers—the sort that today's computers have a hard time cracking—but with quantum computing's ability to parse such complex data quickly, a new generation of quantum encryption will be necessary to avoid catastrophic breaches of security across the business world. Luckily, today there is no quantum computer capable of managing the hundreds of thousands to millions of qubits needed to handle the sort of factoring that would crack current security. But between ten and twenty years from now, that might change, and scientists and forward-thinking policy makers are already working on this quantum cryptography to stay ahead of this tipping point.

² Ibid.

When will quantum arrive?

Quantum computing is a very complex, expensive technology, so do not expect to see it hit mass adoption quickly. Only a few companies with deep technology expertise are likely to lead the rollout. Google and IBM have hopes to double the number of qubits on their prototypes each year. Since the technology is nascent, progress might be slow. We estimate that there may be between 2,000 and 5,000 quantum computers in the world by 2030. Since there are many pieces of hardware and software required to tackle business issues, we expect it may be 2035 or beyond before those tools are in place.

Nevertheless, quantum computing is likely to start delivering value to businesses via the cloud service providers they rely on today. Amazon Web Services and Microsoft Azure are among the organizations that have already announced quantum offerings.

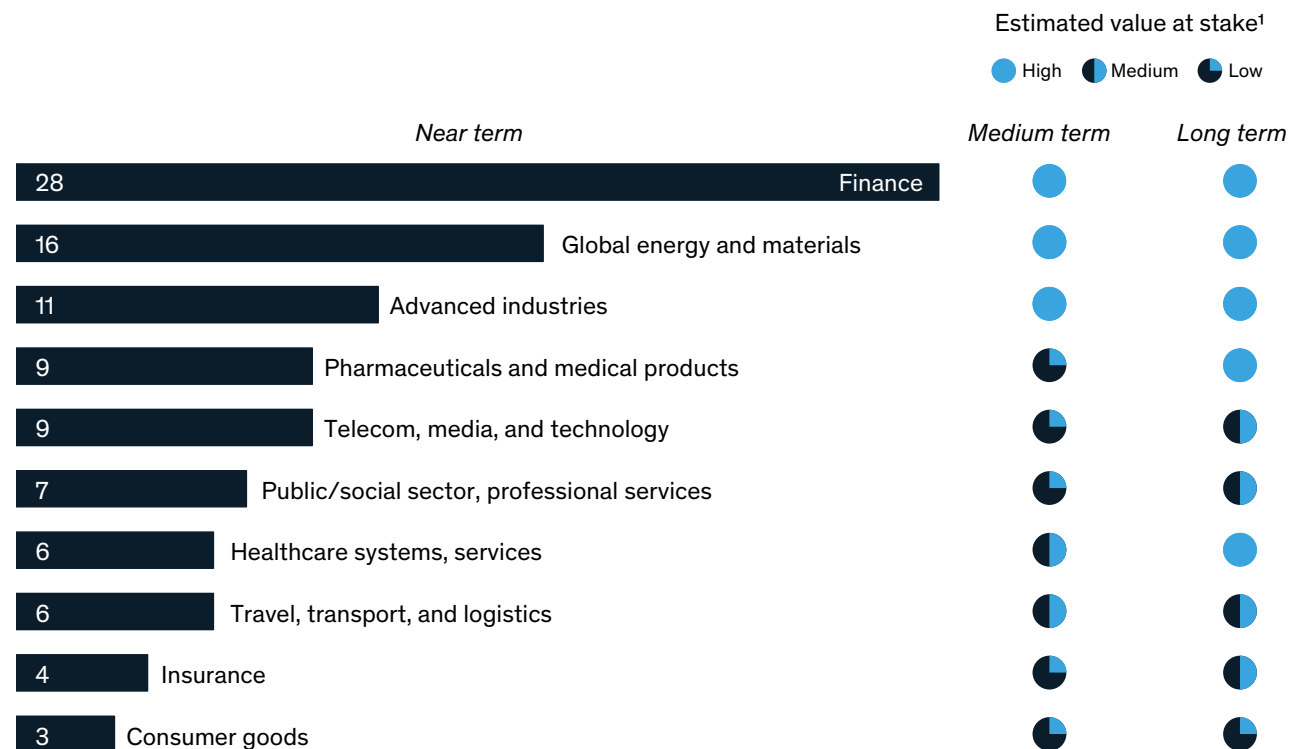
Between 2022 and 2026, we expect many businesses will begin using quantum and hybrid strategies to crack optimization issues. In this same span of time, we expect quantum machines powerful enough to generate meaningful simulations for chemical, materials, and pharmaceutical companies. Quantum AI is further off, and we believe that quantum machines won't be able to factor significant prime numbers (hundreds and thousands of digits long; the sorts used in today's encryption) until the very late 2020s, at the earliest.

As shown in the exhibit, by the mid-2030s, we expect a broad range of industries to have the potential to create significant value from quantum computing.

Exhibit

Who could create value with quantum computing?

Distribution of quantum-computing use case, 2019, %



1. Approximate timing for medium term is by the year 2025; for long term, by the year 2035. Experts consider these values at stake to be a snapshot in time. Fully developed quantum computing will lead to additional value within and shifts between industry verticals.

Source: Expert interviews; McKinsey analysis

How to best prepare your business for quantum computing?

Executives should be preparing for the arrival of quantum computing, even if it could be years away. Because quantum computers will be capable of making explicit all sorts of currently implicit knowledge, it is likely to prove disruptive for the unprepared.

Without question, quantum computers will alter industries in fundamental ways, revolutionizing processes but also altering workforces. For example, the sorts of research currently done by synthetic chemists in laboratories may be absorbed into quantum simulations. As a result, the pharmaceutical companies may need fewer synthetic chemists. The same can be said for career professionals across finance, insurance, transportation and more. Any sort of expertise or judgement that can be used to deal with thorny questions today, may be at risk from the precision of quantum computing in the future.

That is why we recommend that business leaders begin developing a strategy for quantum computing today. The first step in building such a strategy

involves studying the first-wave industries, such as finance, travel, logistics, global energy and materials, and advanced industries. These companies will provide examples of those using quantum technologies to reorganize, optimize and derive other value from the new technology. Some companies may want to begin hiring quantum developers to build an in-house team to create algorithms aimed at their own business issues.

Not every company will be able to find and hire quantum talent, so they may wish to partner with the technology companies currently developing quantum systems. This sort of partnership will give a company voice in how the technology and tools are developed.

Another element of quantum strategy would be the safeguarding of long-lived data assets. Any business or trade secrets could be put at risk by quantum computing, so the time to map out a migration plan for the shift from current cryptography to quantum cryptography is now.

Quantum computing is not an iterative technology. It has the potential to be both transformative and disruptive. Technologies of this sort can appear at unpredictable speed and cause unpredictable impact. The time to act is now, so you will be ready when quantum computers arrive.


This article is substantially based on the work done by **Alexandre Ménard**, **Ivan Ostojic**, and **Mark Patel** authors of the article *A game plan for quantum computing*, McKinsey Quarterly, February 2020, McKinsey.com.

Eric Hazan and **Alexandre Ménard** are two McKinsey senior partners in Paris, **Ivan Ostojic** is a McKinsey partner in Zurich, and **Mark Patel** is a McKinsey senior partner in San Francisco.

March 2020
Copyright © McKinsey & Company

www.mckinsey.com

 [@McKinseyFrance](https://twitter.com/McKinseyFrance)

 [McKinseyFrance](https://www.linkedin.com/company/mckinsey)

