February 2020
McKinsey Quarterly

A game plan for quantum computing

Thanks to technology advances, some companies may reap real gains from quantum computing within five years. What should you do to prepare for this next big wave in computers?

by Alexandre Ménard, Ivan Ostojic, Mark Patel, and Daniel Volz

Pharmaceutical companies have an abiding interest in enzymes. These proteins catalyze all kinds of biochemical interactions, often by targeting a single type of molecule with great precision. Harnessing the power of enzymes may help alleviate the major diseases of our time.

Unfortunately, we don't know the exact molecular structure of most enzymes. In principle, chemists could use computers to model these molecules in order to identify how the molecules work, but enzymes are such complex structures that most are impossible for classical computers to model.

A sufficiently powerful quantum computer, however, could accurately predict in a matter of hours the properties, structure, and reactivity of such substances—an advance that could revolutionize drug development and usher in a new era in healthcare. Quantum computers have the potential to resolve problems of this complexity and magnitude across many different industries and applications, including finance, transportation, chemicals, and cybersecurity.

Solving the impossible in a few hours of computing time, finding answers to problems that have bedeviled science and society for years, unlocking unprecedented capabilities for businesses of all kinds—those are the promises of quantum computing, a fundamentally different approach to computation.

None of this will happen overnight. In fact, many companies and businesses won't be able to reap significant value from quantum computing for a decade or more, although a few will see gains in the next five years. But the potential is so great, and the technological advances are coming so rapidly, that every business leader should have a basic understanding of how the technology works, the kinds of problems it can help solve, and how she or he should prepare to harness its potential.

How does a quantum computer work?

Quantum computing is a fundamentally different approach to computation compared with the kinds of calculations that we do on today's laptops, workstations, and mainframes. It won't replace these devices, but by leveraging the principles of quantum physics it will solve specific, typically very complex problems of a statistical nature that are difficult for current computers.

Qubits versus bits

Classical computers are programmed with bits as data units (zeros and ones). Quantum computers use so-called qubits, which can represent a combination of both zero and one at the same time, based on a principle called superposition.

It's this difference that gives quantum computers the potential to be exponentially faster than today's mainframes and servers. Quantum computers can do multiple calculations with multiple inputs simultaneously. Today's computers can handle only one set of inputs and one calculation at a time. Working with a certain number of qubits—let's say n for our example—a quantum computer can conduct calculations on up to 2^n inputs at once.

That sounds crystal clear. But when you dig into the details of how a quantum computer actually works, you start to understand that many existing challenges must be solved before quantum computers deliver on that potential. (See sidebar, "Quantum computing versus classical computing.")

Technical obstacles

Some of these obstacles are technical. Qubits, for example, are volatile. Every bit in today's computers must be in a state of one or zero. A great deal of work goes into ensuring that one bit on a computer chip does not interfere with any other bit on that chip. Qubits, on the other hand, can represent any combination of zero and one. What's more, they interact with other qubits. In fact, these interactions are what make it possible to conduct multiple calculations at once.

Controlling these interactions, however, is very complicated. The volatility of qubits can cause inputs to be lost or altered, which can throw off the accuracy of results. And creating a computer of meaningful scale would require hundreds of thousands or millions of qubits to be connected coherently. The few quantum computers that exist today can handle nowhere near that number.

Software and hardware companies—ranging from start-ups you've never heard of to research institutes to the likes of Google, IBM, and Microsoft—are trying to overcome these obstacles. They're working on algorithms that bear little resemblance to the ones we use today, hardware that may well wind up looking very different from today's gray boxes, and software to help translate existing data into a qubit-ready format. But they have a long way to go. Although quantum computing as a concept has been around since the early 1980s, the first real proof that quantum computers can handle problems too complicated for classical computers occurred only in late 2019, when

Sidebar

Quantum computing versus classical computing

Their essence is different: Bits versus qubits

A **bit** is the essential information unit for today's classical computers. Each bit can store either a zero or a one.

A **qubit** is the essential information unit for quantum computers. Qubits can store any combination of zero and one at the same time.

Their product is different: A single result versus a narrowed range of possibilities

The limitation of bits comes into play when classical computers face a problem with multiple variables. In these scenarios, computers must conduct a new calculation every time a variable is changed. Each calculation is a single path to a single result.

Quantum computers, on the other hand, have an exponentially larger working space, thanks to the nature of qubits. They can explore a gigantic number of paths simultaneously, which is what gives quantum computers the potential to be so much faster. They deliver multiple results in a tight range, getting you closer to the answer far faster than classical computers can.

But they can—and will—work together: The hybrid approach

In the 2020s, we expect many multivariable problems to be solved through a combination of quantum and classical computing. For instance, by using nascent quantum computers to narrow the range of possible solutions to a finance or logistics problem, a company might reach the optimal solution 10 percent faster. This kind of incremental progress will be the norm until quantum computing matures enough to deliver massive breakthroughs in areas such as drug development and cryptography.

Google announced that its quantum computer had solved such a calculation in just 200 seconds. But this was more of a mathematical exercise than anything that could be applied to business—the problem had no real-world use at all.

Ranges, rather than answers

The nature of quantum mechanics also presents obstacles to exponential speed gains. Today's computers operate in a very straightforward fashion: they manipulate a limited set of data with an algorithm and give you an answer. Quantum computers are more complicated. After multiple units of data are input into qubits, the qubits are manipulated to interact with other qubits, allowing for a number of calculations to be done simultaneously. That's where quantum computers are a lot faster than today's machines. But those gains are mitigated by the fact that quantum computers don't deliver one clear answer. Instead, users get a narrowed range of possible answers. In fact, they may find themselves conducting multiple runs of calculations to narrow the range even more, a process that can significantly lessen the speed gains of doing multiple calculations at once.

Getting a range rather than a single answer makes quantum computers sound less precise than today's computers. That's true for calculations that are limited in scope, which is one reason quantum computers won't replace today's systems. Instead, quantum computers will be used for different kinds of problems, incredibly complex ones in which eliminating an enormous range of possibilities will save an enormous amount of time.

How will businesses use quantum computers?

Quantum computers have four fundamental capabilities that differentiate them from today's classical computers: quantum simulation, in which quantum computers model complex molecules; optimization (that is, solving multivariable problems with unprecedented speed); quantum artificial intelligence (AI), with better algorithms that could transform machine learning across industries as diverse as pharma and automotive; and prime factorization, which could revolutionize encryption.

The best way to understand the business potential of quantum computing is to see how those capabilities could tackle a variety of use cases. Certain industries have specific problems that are particularly well suited to quantum computing. In total, we've reviewed more than 100 nascent use cases and found that they cover a wide range of problems and sectors, including pharmaceuticals, cybersecurity, finance, materials science, and telecommunications. Our research also suggests significant diversity in the development life cycle of these applications, and in the nature of business benefit they could confer. To paint a richer picture of these dynamics at work, let's consider four high-potential applications:

1. Cut development time for chemicals and pharmaceuticals with simulations

Scientists looking to develop new drugs and substances often need to examine the exact structure of a molecule to determine its properties and understand how it might interact with other molecules. Unfortunately, even relatively small molecules are extremely difficult to model accurately using classical computers, since each atom interacts in complex ways with other atoms. Currently, it's almost impossible for

computers to simulate molecules with just several dozen atoms—and proteins, to cite just one example, have thousands of them. That's why today's scientists are forced to actually create the molecules in question (using synthetic chemistry) to physically measure their properties. Often the molecule doesn't work as expected, entailing more synthesis and testing. Each optimization cycle is expensive and time-consuming. This is one reason why developing new drugs and chemicals is such a lengthy process.

Quantum computers are intrinsically well suited to tackle this problem, since the interaction of atoms within a molecule is itself a quantum system. In fact, experts believe that quantum computers will be able to model even the most complex molecules in our bodies. Every bit of progress in this direction will drive faster development of new drugs and other products, and potentially lead to transformative new cures.

2. Solve optimization problems with unprecedented speed

Across every industry, many complex business problems involve a host of variables. Where should I place robots on the factory floor? What's the shortest route for my delivery truck? What's the most efficient way to deploy cars, motorcycles, and scooters to create a transportation network that meets user demand? How can I optimize the performance and risk of a financial portfolio? These are just three of the many examples that business leaders confront.

Solving these problems with classical computing is an arduous, hit-and-miss process. To isolate the inputs that drive performance gains or losses, the number of variables that can be shifted in any calculation must be seriously limited. As a result, companies must make one complicated calculation after another, a costly, time-consuming process given the multiplicity of variables. But, since quantum computers work with multiple variables simultaneously, they can be used first to dramatically narrow the range of possible answers in a very short time. Classical computing can then be called in to zero in on one precise answer, and its work will still seem slow compared with that of quantum. But, since quantum has eliminated so many possibilities, this hybrid approach will drastically cut the time it takes to find the best solution.

3. Accelerate autonomous vehicles with quantum AI

It's possible that quantum computers could speed the arrival of self-driving vehicles. At Ford, GM, Volkswagen, and other car manufacturers, and at a host of start-ups in the new mobility sector, engineers are running hours upon hours of video, image, and lidar data through complex neural networks. Their goal: use AI to teach a car to make crucial driving decisions, such as how to take a turn, where to speed up and slow down, and, crucially, how to avoid other vehicles, not to mention pedestrians. Training an AI algorithm this way requires a set of computationally intensive calculations, which become increasingly difficult as more data and more complex relationships within the variables are added. This training can tax the world's fastest computers for days or even months. Since quantum computers can perform multiple complex calculations with multiple variables simultaneously, they could exponentially accelerate the training of such AI systems. It's not going to happen anytime soon. Translating classical data sets to quantum ones is arduous work, and early quantum AI algorithms have resulted in only modest gains.

4. Transform cybersecurity

Quantum computing poses a serious threat to the cybersecurity systems relied on by virtually every company. Most of today's online-account passwords and secure transactions and communications are protected through encryption algorithms such as RSA or SSL/TLS. These systems make it easy for businesses to create data that can be shared by authorized users while also being protected from outsiders. Breaking through that encryption requires massive computational power. It's virtually impossible for today's computers to solve the math problem behind well-architected encryption quickly enough to be of practical use. (That math problem is known as prime factorization, since encryption is built around the manipulation of large prime numbers.) When data theft does occur, it's often because of poor implementation of cybersecurity protocols.

Since quantum computers can perform multiple calculations simultaneously, they have the potential to break any classical encryption system. In fact, a quantum algorithm to do just that already exists. (It's called Shor's algorithm.) Luckily, there's no quantum computer capable of managing the hundreds of thousands to millions of qubits it would take to execute Shor's algorithm—as we said earlier, today's versions can handle a dozen or so qubits. But somewhere between ten and 20 years from now, that might change, and at that point a new wave of quantum encryption technologies would be required to protect even our most basic online services. Scientists—as well as forward-thinking policy makers—are already at work on this quantum cryptography, trying to prepare for this tipping point.

When will quantum arrive?

Quantum computing is a complex technology. It's not an app that's going to appear one day and be adopted by millions of people the next. After speaking with dozens of experts in the rapidly growing quantum ecosystem, we've developed a clear estimate of how the technology will progress over the next couple of decades.

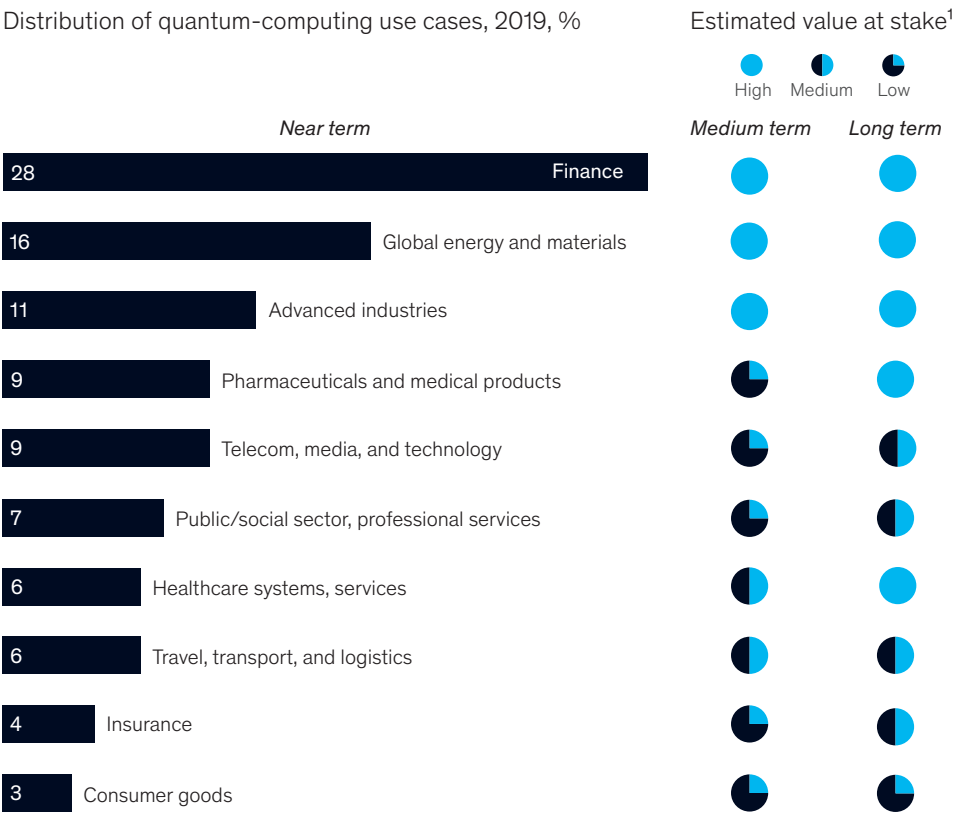
Quantum computers will be expensive machines developed and operated by a few key players. Companies such as Google and IBM hope to double the capabilities of quantum computers, in a Moore's law–like fashion, every year. Along with a small but significant cohort of promising start-ups, they will steadily drive up the number of qubits that can be handled by their computers. Since the technology is nascent, their progress may be slow: our estimate is that by 2030 only 2,000 to 5,000 quantum computers will be operational. Since there are many pieces to the quantum-computing puzzle, the hardware and software needed to handle the most complex problems may not exist until 2035 or beyond.

Nevertheless, quantum will start delivering value to some businesses well before then. Initially, and perhaps in the long term as well, businesses will receive quantum services via the cloud from the same providers they rely on now. Amazon Web Services, Microsoft Azure, and others have already announced quantum offerings. These cloud offerings could quickly expand adoption and demand.

Between 2022 and 2026, we expect many businesses with optimization issues to adopt hybrid approaches, in which parts of the problem would be handled by classical

Exhibit

Who could create value with quantum computing?



[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

computing and parts by quantum. In that same time frame, quantum computers are likely to become powerful enough to start handling meaningful simulations of molecular structures for chemical, materials, and pharmaceutical companies. The arrival of quantum AI is further off, and we don't expect quantum computers to be powerful enough for prime factorization until the very late 2020s at the earliest.

This timeline for the development of the technology informs our estimates of when different industries are likely to benefit most from quantum computing. The experts we spoke with expect that pioneers in advanced industries, global energy and materials, finance, and (to a lesser extent) travel and logistics might start generating significant value from quantum by 2025. The big payoff for pharmaceuticals may not come until the following decade, given that solving the most complex medical problems involves mimicking deeply complex molecules. As shown in the exhibit, by the mid-2030s a wide range of industries will have the potential to create significant value from quantum computing.

Preparing your business for quantum

Obviously, preparing for major technological advances is a key part of any executive's portfolio. That's especially true for quantum, which has the potential to be greatly disruptive. By solving calculations that are impossible with classical computing, quantum could make explicit all kinds of currently implicit knowledge. This wouldn't just revolutionize processes; it could also radically alter the workforces of different industries.

In chemicals and pharmaceuticals, for example, today's synthetic chemists must create actual molecules or solids to test hypotheses about potential new drugs or materials. These substances often don't work as expected, which leads to further cycles of costly and time-consuming synthesis and testing. If quantum computers can model such substances exponentially faster, as expected, companies may well need fewer synthetic chemists. It's not hard to envision such mathematical certainty replacing the expertise and judgment of career professionals in other industries with multivariable problems, such as finance, insurance, transportation, and more.

Even though we're unlikely to feel that kind of societal impact for decades, prescient business leaders in almost every industry should develop some kind of quantum strategy now. The kind of preparation depends on whether you're in the first wave of industries that can benefit from the technology, whether your business has use cases that map to the incipient strength of quantum, and whether you believe you might reap transformative or merely incremental gains.

Understanding first-wave industries

We believe that industries such as finance, travel, logistics, global energy and materials, and advanced industries will start reaping significant value from the hybrid classical/quantum approach in the early 2020s. Business leaders in these first-wave sectors need to develop a quantum strategy quickly or they will be left behind by innovative companies such as Barclays, BASF, BMW, Dow, ExxonMobil, and others that already have taken strategic steps into quantum computing. These leaders should think about how their businesses can tap into the burgeoning quantum infrastructure. Some may want to get into the labor market now and hire quantum developers to build an in-house team to create algorithms that target pressing systemic problems. Quantum talent is in short supply right now, and it's unlikely that research universities will be able to turn out enough top quantum engineers to keep up with the rapidly expanding demand.

Other first-wave companies may find it useful to partner directly with the technology companies developing quantum. We are in the early stages of a long process of adapting quantum to the needs of business, so companies still have the potential to influence that development in ways that serve their particular needs.

Safeguarding long-lived data assets

Besides companies in these first-wave industries, there's another cohort that should actively monitor the progress of quantum. According to Louisiana State University professor Jonathan Dowling, "If you have business and trade secrets that you

would want to keep secret for ten to 50 years, then you need to start worrying now." Companies whose business depends on decades of data must be on high alert about the cybersecurity issues that quantum computing raises. At the very least, the topic should be at the top of the chief information officer's agenda, and business leaders need to be confident that their companies have a plan for making a safe transition from current cryptography to quantum cryptography.

Even if your business doesn't fall into one of these two groups, quantum computing is a technology that your key technology experts should be monitoring. Quantum is not just an iterative technology that enables marginal improvements. It has the potential to be both transformative and disruptive. Technologies this potent can emerge at unpredictable speed and cause unpredictable impact. Business leaders who don't want to be caught unaware should start getting ready for quantum computing now. Q

Alexandre Ménard is a senior partner in McKinsey's Paris office, **Ivan Ostojic** is a partner in the Zurich office, **Mark Patel** is a senior partner in the San Francisco office, and **Daniel Volz** is a consultant in the Frankfurt office.

The authors wish to thank Maximilian Charlet, Anna Heid, and Lorenzo Pautasso for their contributions to the development of this article, as well as Miklós Dietz, Mathis Friesdorf, Eric Hazan, Nicolaus Henke, Anika Pflanzer, and Henning Soller for their input.