What is quantum computing?

Quantum computing is a new approach to calculation that uses principles of fundamental physics to solve extremely complex problems very quickly.

Flip a coin. Heads or tails, right? Sure, once we see how the coin lands. But while the coin is still spinning in the air, it's neither heads nor tails. It's some probability of both.

This grey area is the simplified foundation of quantum computing. Digital computers have been making it easier for us to process information for decades. But quantum computers are poised to take computing to a whole new level. Quantum computers represent a completely new approach to computing. And while they won't replace today's computers, by using the principles of quantum physics, they will be able to solve very complex statistical problems that today's computers can't. Quantum computing has so much potential and momentum that McKinsey has identified it as one of the next big trends in tech. Quantum computing alone—just one of three main areas of emerging quantum technology—could account for nearly $1.3 trillion in value by 2035.

Here's how it works: classical computing, the technology that powers your laptop and smartphone, is built on bits. A bit is a unit of information that can store either a zero or a one. By contrast, quantum computing is built on quantum bits, or qubits, which can store zeros *and* ones. Qubits can represent any combination of both zero and one simultaneously—this is called a superposition.

When classical computers solve a problem with multiple variables, they must conduct a new calculation every time a variable changes. Each calculation is a single path to a single result. Quantum computers, however, have a larger working space, which means they can explore a massive number of paths simultaneously. This possibility means that quantum computers can be much, much faster than classical computers.

But the first real proof that quantum computers could handle problems too complicated for classical computers didn't arrive until 2019, when Google announced that its quantum computer had made a major breakthrough: it solved a problem in 200 seconds that would have taken a classical computer 10,000 years.

Although this was an important milestone in computing, it was more of a theoretical leap forward rather than a practical one, since the problem the quantum computer solved had no real-world use at all. But we're rapidly approaching a time when quantum computers *will* have a real impact on our lives.

How do quantum computers solve problems?

Today's classical computers are relatively straightforward. They work with a limited set of inputs and use an algorithm and spit out an answer—and the bits that encode the inputs do not share information about one another. Quantum computers are different. For one thing, when data are input into the qubits, the qubits interact with other qubits, allowing for many different calculations to be done simultaneously. This is why quantum computers are able to work so much faster than classical computers. But that's not the end of the story: quantum computers don't deliver one clear answer like classical computers do; rather, they deliver a range of possible answers.

For calculations that are limited in scope, classical computers are still the preferred tools. But for very complex problems, quantum computers can save time by narrowing down the range of possible answers.

When will quantum computers arrive?

Quantum computers aren't like your average desktop computer. It's unlikely that you will be able to wander down to a store and pick one up. The kind of quantum computers that are capable of solving major problems will be expensive, complicated machines operated by just a few key players.

Over the next few years, the major players in quantum computing, as well as a small cohort of start-ups, will steadily increase the number of qubits that their computers can handle. Progress is expected to be slow: McKinsey estimates that by 2030, only about 5,000 quantum computers will be operational. The hardware and software required to handle the most complex problems may not exist until 2035 or later.

What are some obstacles that impede the development of quantum computing?

One major obstacle to the advancement of quantum computing is that qubits are volatile. Whereas a bit in today's computers can be in a state of either one or zero, a qubit can be any possible combination of the two. When a qubit changes its status, inputs can be lost or altered, throwing off the accuracy of the results. Another obstacle to development is that a quantum computer operating at the scale needed to deliver significant breakthroughs will require potentially millions of qubits to be connected. The few quantum computers that exist today are nowhere near that number.

How can classical computers and quantum computers work together?

Slowly, at first. For the time being, quantum computing will be used alongside classical computing to solve multivariable problems. One example? Quantum computers can narrow the range of possible solutions to a finance or logistics problem, helping a company reach the best solution a little bit faster. This kind of slower progress will be the norm until quantum computing advances enough to deliver massive breakthroughs.

What are some potential business use cases for quantum computers?

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

1. *Quantum simulation*. Quantum computers are able to model complex molecules, which may eventually help reduce development time for chemical and pharmaceutical companies. Scientists looking to develop new drugs need to examine the structure of a molecule to understand how it will interact with other molecules. It's almost impossible for today's computers to provide accurate simulations, because each atom interacts with other atoms in complex ways. But experts believe that quantum computers are powerful enough to eventually be able to model even the most complex molecules in the human body. This opens up the possibility for faster development of new drugs and transformative new cures.
2. *Optimization and search*. Every industry relies in one way or another on optimization. Where should I place robots on the factory floor? What's the shortest route for my delivery truck? There are almost infinite questions that need to be answered to optimize for efficiency and value creation. With classical computing, companies must make one complicated calculation after another, which is a time-consuming and costly process given the many variables of any situation. Since quantum computers can work with multiple variables simultaneously, they can be used to quickly narrow the range of possible answers. From there, classical computing can be used to zero in on one precise answer.
3. *Quantum AI*. Quantum computers have the potential to work with better algorithms that could transform machine learning across industries as diverse as pharmaceuticals and automotive. In particular, quantum computers could accelerate the arrival of self-driving vehicles. Companies like Ford, GM, Volkswagen, and numerous mobility start-ups are running video and image data through complex neural networks. Their goal? To use AI to teach a car to make crucial driving decisions. Quantum computers' ability to perform multiple complex calculations with many variables simultaneously allows for faster training of such AI systems.
4. *Prime factorization*. Businesses today use large, complex prime numbers as the basis for their encryption efforts, numbers too large for classical computers to process. Quantum computing will be able to use algorithms to solve these complex prime numbers easily, a process called prime factorization. (In fact, a quantum algorithm known as Shor's algorithm theoretically already can; there's just not a computer powerful enough to run it.) Once quantum computers have advanced enough, new quantum-encryption technologies will be needed to protect our online services. Scientists are already at work on quantum cryptography to prepare for this eventuality. McKinsey estimates quantum computers will be powerful enough for prime factorization by the late 2020s at the very earliest.

As these capabilities develop at pace with quantum computing power, use cases will proliferate.

Experts believe that quantum computers are powerful enough to eventually be able to model even the most complex molecules in the human body.

What industries stand to benefit the most from quantum computing?

Research suggests that four industries stand to reap the greatest short-term benefits from quantum computing based on the use cases discussed in the previous section. Collectively—and conservatively—the value at stake for these industries could be as much as $1.3 trillion.

- *Pharmaceuticals*. Quantum computing has the potential to revolutionize the research and development of molecular structures in the biopharmaceuticals industry. With quantum technologies, research and development for drugs will become less reliant on trial and error, and therefore more efficient. (Read more on how quantum computing stands to affect the pharmaceutical industry.)
- *Chemicals*. Quantum computing could be used to improve catalyst design, which could enable savings on existing production processes. Innovative catalysts could also enable the replacement of petrochemicals with more sustainable feedstock or the breakdown of carbon for CO_2 usage. (Read more on how quantum computing might affect the chemicals industry.)
- *Automotive*. The automotive industry could benefit from quantum computing in its R&D, product design, supply chain management, production, and mobility and traffic management. For example, quantum computing could be applied to decrease manufacturing costs by optimizing complex multirobot processes including welding, gluing, and painting. (Read more about how quantum technologies could affect the automotive industry.)
- *Finance*. Quantum-computing use cases in finance are slightly further in the future. The long-term promise of quantum computing in finance lies in portfolio and risk management. One example could be quantum-optimized loan portfolios that focus on collateral to allow lenders to improve their offerings. (Read more about how quantum computing could affect financial services.)

These four industries likely stand to gain the most from quantum computing. But leaders in every sector can—and should—prepare for the inevitable quantum advancements of the next few years.

What are some other quantum technologies aside from computing?

According to McKinsey's analysis, quantum computing is still years away from widespread commercial application. Other quantum technologies such as quantum communication (QComms) and quantum sensing (QS) could become available much earlier. Quantum communication will enable strong encryption protocols that could greatly increase the security of sensitive information. QComms enables the following functions:

- *Full security* when information is transferred between locations. Quantum-encryption protocols are more secure than classical protocols, most of which will likely be able to be broken once quantum computers attain more computing power or can work with more efficient algorithms.
- *Enhanced quantum-computing power* in two important types of quantum processing: parallel quantum processing (where multiple processors are connected and simultaneously execute different calculations from the same problem) and blind quantum computing (where quantum communications provide access to remote, large-scale quantum computers in the cloud). Both types of processing are made possible by the entanglement of quantum particles. Entanglement is when quantum particles like qubits have connected properties, which means one particle's properties can be manipulated by actions done to another.

Quantum sensing allows for more accurate measurements than ever before, including of physical properties like temperature, magnetic fields, and rotation. Plus, once optimized and decreased in size, quantum sensors will be able to measure data that can't be captured by current sensors.

The markets for QComms and QS are currently smaller than those for quantum computing, which has so far attracted most of the headlines and funding. But McKinsey expects both Qcomms and QS to attract serious interest and funding in the future. The risks are significant, but the potential payoff is high: by 2030, QS and QComms could generate $13 billion in revenues.

Learn more about quantum sensors and quantum communications.

How can organizations ensure that they have the quantum-computing talent they need?

A wide talent gap exists between the business need for quantum computing and the number of quantum professionals available to meet that need. This skill gap could jeopardize potential value creation, which McKinsey estimates to be as much as $1.3 trillion.

McKinsey research has found that there is only one qualified quantum candidate for every three quantum job openings. By 2025, McKinsey predicts that less than 50 percent of quantum jobs will be filled, unless there are significant changes to the talent pool or predicted rate of quantum-job creation.

Here are five lessons derived from the AI talent journey that can help organizations build the quantum talent they need to capture value:

1. *Define your talent needs clearly*. In the early days of AI, some organizations hired data scientists without a clear understanding of what skills were needed. To avoid

making the same error with quantum, organizations should first identify possible fields of applications that a quantum-computing team would work on and then ensure that new hires come from diverse backgrounds (reflecting best practices).

2. *Invest early in translators.* As buzz built up around AI, the role of analytics translators became crucial to helping leaders identify and prioritize challenges best suited for AI to solve. With quantum, there's a similar need: for translators with engineering, application, and scientific backgrounds who can help organizations understand the opportunities and players in the rapidly expanding ecosystem.
3. *Create pathways for a diverse talent pipeline*. Many of the first AI models reflected the same biases that were present in the information that was used to train them. There often was also a lack of people with diverse perspectives and experience building and testing the models, which contributed to the bias issue. While it's too early to know what risks will emerge from quantum technologies, we can expect similar challenges if we don't build and empower a diverse quantum workforce. Efforts are needed at the university level, as well as in K–12 education.
4. *Build technology literacy for all.* In order for employees at all levels of an organization to understand the potential of a new technology, they need a basic understanding of how it works and what it can do. With quantum, business leaders as well as workers up and down the supply chain, in marketing, IT infrastructure, finance, and more will require basic fluency in quantum topics.
5. *Don't forget talent development strategies.* Companies focus heavily on talent attraction during times of technological foment—but that's just one piece of the talent puzzle. In order to retain specialists, companies need to carve out clear paths for talent development. One pharmaceutical company leans into both the purpose of its work—developing use cases that will help save lives—and the freedom it offers its team.