Why quantum computing is a big deal

Photo by Joanna Kosinska
Kearney, London

KEARNEY

This paper is the first of a three-paper series: Why is quantum computing a big deal? How will quantum computing disrupt industries, and when? and What should you do about quantum computing now?

In December 2020, a research group from China announced that it had achieved **quantum supremacy**. The news echoed Google's well-publicized October 2019 announcement that its quantum computer had likewise solved a problem that no classical computer could reasonably solve.

But quantum computing is complex, and these experiments were arcane. The media has been left to talk about a quantum race between the US and China, reminiscent of the space race. Or maybe a similar race between Google and IBM, reminiscent of other corporate rivalries. The meaning of developments in quantum computing gets lost, even for most IT specialists. We're left scratching our heads (see sidebar on page 2: The story behind the news).

This is the problem with quantum computing: Few people understand it. The technology is complex—and so is the concept. As automakers tackle the technologically complex task of making electric vehicles, people are familiar with batteries, and with cars, so it's conceptually easy to combine them. Same for the 5G wireless standard: you may not understand the technology, but you can understand what it will do. With quantum computing, however, it's hard for non-specialists to even understand what it is, what it does, or what it's good for.

Misconceptions and reality

As a result, all the literature outside specialized technical journals is full of misconceptions and hype. Many pundits depict quantum computing as magically faster computing. Others claim it can overcome future limitations of Moore's law, the prediction that the power of new computers grows exponentially along the years. Still others create unrealistic expectations of what quantum computing can achieve in the next few years.

None of that is true. Quantum computing is not a magic formula for faster computing everywhere. It does make certain kinds of difficult problems easier to solve. But for most of the kinds of problems you currently solve with classical computers, quantum computing is not faster. Quantum computing will never run your payroll or recalculate your spreadsheets.

This is the problem with quantum computing: Few people understand it. The technology is complex—and so is the concept.

The story behind the news

In October 2019, Google's quantum computer performed a calculation in 200 seconds. That calculation would have taken a conventional computer 10,000 years, it said. But a few days later, IBM said a conventional computer could do that calculation in 2.5 days. Because the underlying science was too complicated to sort out, most people walked away with the impression that Google and IBM were locked in a corporate quarrel on the lead of a revolutionary new technology.

Google was right: its quantum computer achieved a task that no classical computer could do so quickly. Like the Wright Brothers' accomplishment of flight at Kitty Hawk, **quantum supremacy** marked an essential early milestone of technological development. IBM was also right: the **10,000 years** figure was overhyped. Google did not take into account other approaches to computing that could have been faster.

Like Google, the 2020 team from a Chinese university in Hefei designed a convoluted task that exploited the advantages of quantum computers while minimizing their shortcomings. Designed only to prove quantum supremacy, the tasks have no practical application. Furthermore, the Chinese computer could not be programmed, not used for any other tasks. In some ways it felt more like a gigantic physics experiment than an actual computer. Then again, the Wright Brothers at Kitty Hawk were far from ready to take passengers to O'Hare.

What it will do is solve problems that cannot currently be solved. For example, cryptography works because even the fastest computer on earth isn't fast enough to guess your password. Any such problem scales exponentially with the password size and quickly becomes too big for a classical computer to manage.[1] But quantum computing could use non-exponentially-scaling algorithms to quickly guess your password. It will thus break all existing Internet security. It even affects the blockchain and cryptocurrencies.

To take another example, despite our extremely accurate knowledge of all the fundamental laws underpinning chemistry, there are some chemical reactions and molecules that even chemists simply don't understand. The complexity of chemical systems scales exponentially. With today's technology, it would take centuries or millennia to compute most practical chemistry use cases. But quantum computing could model any chemical compound with absolute precision. This radical change will profoundly disrupt the materials, chemical, and pharmaceutical industries.

To take a third example, many **optimization problems** scale exponentially. If you need to find the most efficient delivery route, each time you add one more stop, the problem becomes exponentially harder. If you want to find the optimal location for your wind turbines to generate the most electricity, or the optimal stock portfolio to maximize gains, or the optimal price of your product to maximize profits, the more options you consider, the more your classical computer struggles to find the best answer. Quantum computing is great at optimization problems. It will thus disrupt logistics, finance, engineering, and medical research—perhaps the vaccine research of the future will be quantum.

[1] In technical terms, the problem scales **superpolynomially**.

Where we're going

Google's achievement of quantum supremacy was a **technical** milestone. But quantum computing will change our lives through business milestones, not technical ones. Today's most significant achievements are in the development of an ecosystem of companies that will soon make up a remarkably mature value chain: quantum device providers, quantum computer manufacturers, and quantum computing cloud service providers.

We're not there yet—nowhere near there. Quantum computing technology, now still in its infancy, will face huge stumbling blocks. The result will bring a great deal of uncertainty in what types of outcomes are feasible and when they will arrive.

This uncertainty is why public- and private-sector leaders must pay attention to quantum computing now. Given the combination of almost binary uncertainty and disruptive impact, it would be easy to make the wrong strategic and financial decisions. The only way to make the right decisions: understand what quantum computing is, what it's good for, and how that business ecosystem might evolve.

So, what is quantum computing?

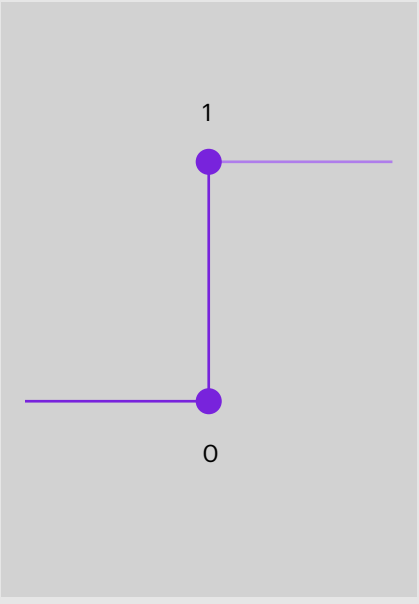
Quantum computing is a new paradigm of computing that uses the very fabric of reality to solve problems that could not be solved before. Quantum computing is based on quantum mechanics, the bizarre and counterintuitive laws of physics that prevail at subatomic scale, where things can be in several places or several distinct states at the same time.

Quantum computing is based on **qubits**. As you may know, classical computing is based on the bit, which can be a one or a zero. Like a bit, a qubit is a minimum unit of quantum information. But unlike a bit, a qubit can represent much more than ones and zeros.

It's hard to explain a qubit. Every simplification distorts its reality. Instead, let's consider a visualization of the qubit, to show why it has so much more representational power than a classical bit (see figure 1). Imagine a sphere. A classical bit can take only the value of its north or south pole, 0 or 1. But a qubit can take a value of any point of the surface of the sphere—every possible pair of latitude and longitude measurements. The qubit's latitude reflects its combination of the values 0 and 1. The qubit's longitude is called its **phase**.

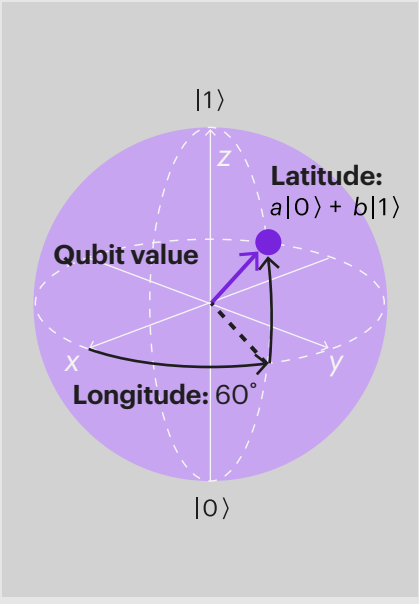
Figure 1
Bit versus qubit

Bit
Classical computing



Only two states: binary 0 or binary 1

Qubit
Quantum computing



Infinite number of hybrid states: any combination of |0⟩ and |1⟩ (latitude) with any phase (longitude)

Source: Kearney analysis

Let's consider the latitude first. The qubit is simultaneously taking intermediate positions between 0 and 1. So your computer's algorithm can perform calculations on all these values at the same time. If you have *n* qubits, you can do the same operation on all the possible combinations of 0 and 1 for all the qubits, that is 2^n. This way, you can address a problem that scales exponentially without having to scale up your number of steps. You can handle all those values with one quantum operation. This is called **quantum superposition**.

Now let's consider longitude, or phase—and we need to switch metaphors. Think of a wave. Think of two sets of waves moving toward each other, as if they've arisen from boats on opposite sides of a lake. If they collide in just the right way, the peak of one hits the bottom of the other, and they cancel each other out. The lake surface becomes calm. This is how phase works (although the math is far more complex): the values with opposite phase cancel each other as if they never existed. This is called **quantum interference**.

How does quantum computing work?

Quantum computing uses new computing paradigms to take advantage of the quantum properties of qubits—this **superposition** and **interference** that we have just defined. Not only does the qubit differ from the bit, but the paradigms to manipulate the qubit differ from paradigms of existing computers.

So let's take a closer look at a quantum computing paradigm. How does it cause algorithms to scale more slowly? The secret sauce is called **quantum parallelism**. Recall that quantum superposition allows us to make calculations on all possible values of an input at the same time in a single step. As we do so, quantum interference allows us to destroy any outcomes that are not part of the solution.

Again, an analogy may help. Instead of **0s and 1s**, consider different colors: red instead of 000, green for 001, yellow for 010, and so forth. We have a problem for which the answer is "purple." We can get to that answer by putting all the colors into superposition and mixing them. After all, when you perform operations on a superposition state, you are doing it in all possible states at the same time. Unfortunately, as you've seen if you've ever made a mistake mixing paint at the hardware store, color mixing often makes for yucky brown. Likewise, our calculations in superposition are mixing together the outcomes we need and the ones we don't need, giving us yucky brown instead of the purple we wanted. Here is where quantum interference comes to the rescue, because we can actually set up our algorithm in a clever way to destroy the unnecessary outcomes, transforming the brown into our desired purple. How? It's hard to explain without an understanding of quantum mechanics, but let's just say that it's achieved by rotating the qubits using **quantum gates**.

Again, these explanations of colors and lake waves are analogies. They're not entirely accurate. We offer them to show that designing quantum algorithms is totally different from designing classical algorithms. It's far more convoluted and requires a completely different set of skills. Where traditional algorithms are often common sense, quantum algorithms can be counterintuitive. They have little connection to reality. You're not going to pick them up at Algorithms R Us, nor will you be able to send your current IT staff to a weeklong training. Development of these algorithms will require mathematical genius.

But the algorithms are what give quantum computing its incredible power. For example, if you want to find a specific value in a randomly ordered list of 1,000,000 elements, it would take you on average 500,000 tries. **Grover's algorithm** finds it in just 1,000 tries. To achieve this counterintuitive result, it puts all 1,000,000 values in superposition and makes 1,000 qubit rotation sets. And Grover's algorithm is not the most powerful example of what quantum algorithms can do. It's merely the easiest to understand.

At this point, you may be thinking, why couldn't I make these "rotations" using a supercomputer and get the same result? In theory you could, but every time you add a qubit, the effort would grow exponentially. Indeed, simulating a quantum computer with only 80 qubits would require all the computing power that currently exists on Earth.

Are there different types of quantum computers?

So far we've been discussing a quantum computing paradigm called **universal gate-based quantum computers**. Again, it's based on a set of quantum logic gates operating with quantum parallelism over multiple qubits. They can implement any possible algorithm.

But there are other paradigms of quantum computing—other ways to use the properties of qubits to solve problems. Another current mainstream paradigm is called **quantum annealing**. In metalworking, **annealing** is the process of heating the metal to excite its atoms and then allowing them to relax into a more stable state. (If you want to make a sword, **annealing** softens the blade so that you can sharpen it without shattering it.) Quantum annealing uses a similar process to solve optimization problems. You cleverly model the solution to the problem as the most stable state—the ground state—of your qubit arrangement. Then, as you slowly set up the qubits and let them relax, they will find their way to the ground state—the solution of your real-world optimization problem.

There are some caveats to quantum annealing, much debated by today's scientists. One caveat is that it handles only optimization problems, not general-purpose computing. It is not universal. Furthermore, limitations in the underlying physics make a literal optimization implementation impossible. So today's annealing is an approximation, lacking a 100 percent guarantee that it will achieve the actual best solution. There's no scientific proof that quantum annealing has quantum advantage. On the other hand, quantum annealing is much farther along than the gate-based paradigm. It may be closer to being capable of solving real-world problems.

The Chinese computer that recently achieved quantum supremacy belongs to a third paradigm of quantum computing called **quantum simulators**. These are special-purpose quantum computers that simulate quantum systems for the purpose of solving very specific problems. To paraphrase famous physicist Richard Feynman, quantum problems are better solved by quantum computers—so if a simulator can solve these problems, it's valuable, although even more niche than annealers.

Where is quantum computing today?

Achieving quantum supremacy was a key milestone. We can think of it as resembling the Wright Brothers' milestone at Kitty Hawk, of achieving flight. But their plane that day couldn't travel more than seven miles per hour or get more than 10 feet off the ground. Likewise, quantum computers have yet to do anything useful, have yet to solve any practical problems.

The big issue is scale. Quantum computing needs to scale effectively to implement practical applications. Three factors affect how quickly scale can mature:

1. **Number of qubits.** How much quantum information can your system store? The more qubits you include in your system, the more practical applications you can have.

2. **Coherence time.** How long will your quantum system stay "quantum"? Quantum systems are inherently unstable. They quickly lose their superposition and interference. Depending on the technology, this **coherence time** can be milliseconds, tenths of seconds, or even one minute.[2] The more coherence time you have, the more steps you can do.

3. **Gate depth.** How many quantum gate operations can you include in your algorithm? The more gates you have, the more steps your algorithm can include. Obviously, gate depth is limited by coherence time. But a subtler limitation relates to what we call **gate fidelity**, how reliable is the gate. In general, gates are **noisy**, or unreliable. And these errors accumulate as you perform more operations. Today's gate reliability is in the order of 99.9 percent error free. Although this may not sound bad, it means that after only about 700 operations, you have a 50 percent chance of having an error.

Scientists are still learning the best ways to mitigate or correct those errors. For now, the plan is to rely on redundancy. For example, if you run 10 gates in parallel with a 10 percent error rate, you should get the right answer nine times on average. The problem with this approach is that you need 10 times as many qubits, and our quantum devices don't have many qubits yet (see figure 2 on page 6).

[2] However, we need to factor the speed of an operation when looking at coherence time. For example, trapped ion technology has coherence times of one minute, but its logic gate operations take longer. As a result, it ends up performing the same amount of operations as superconductor technology, which stays coherent for only fractions of milliseconds, but operates at a much higher speed.

Figure 2
Quantum computing scaling



	Number of qubits	Gate depth	Coherence time
Scaling dimensions	Determines the quantum info that can be processed	Determines number of steps to be executed in an algorithm	Limits the max duration of the algorithm
Current state:	50–60 qubits for gate computing 2,000–5,000 qubits for annealers[1]	Circuit with gate depth 20	Depends on technology
Cases:	Google Sycamore: 54 qubits D-Wave Advantage: 5,000 qubits	Google Sycamore: gate depth 20	Trapped ion: 1–10 seconds Superconductor: Microseconds

Notes: Annealers computing power requires more qubits.
Source: Kearney analysis

Today, the **gate-based** paradigm has reached a scale of 50 to 70 qubits. For example, Google used a 54-qubit Sycamore processor to demonstrate quantum supremacy. Quantum **annealers** have reached a scale of 5,000 qubits. However, the different paradigm brings in a power factor, such that this scale is equivalent to that of gate-based quantum computers.

Experts say we're in **the NISQ era**, referring to Noisy Intermediate-Scale Quantum computers. Although beyond beginner scale, these devices still have few qubits, limited gate depths, and short coherence times. Meanwhile, you can limit your need for scale by combining it with classical approaches. NISQ computers will most likely work as **co-processors** of classical computers. If you do a lot of gaming on your home computer, you know that you have a graphics processing unit (GPU) that works alongside your central processing unit (CPU); the CPU calls the GPU to handle your video and game graphics. Likewise, a huge computer could use a **hybrid algorithm**. A classical algorithm would occasionally make short function calls to the quantum processor. These hybrid algorithms are still being explored, but they may find particular applications in machine learning, materials science, or quantum chemistry.

Who is doing what and what is the current status of the industry?

In the earliest stages, quantum computing was necessarily pursued by fully integrated units within academia or big tech labs. Eventually, it will evolve into a highly differentiated value chain: R&D, manufacturers, plant equipment providers, and developers. Although that value chain remains immature, its structure is beginning to take shape. For example, recent developments at IBM and Microsoft have demonstrated the value of **cloud delivery**.

Today's quantum value chain has five key stages. Activities of the industry's major players fall into one or more of these value chain drivers.

— **Device providers**—including companies such as Rigetti, Intel, Honeywell, and IonQ—develop the fundamental components to create quantum computers: qubits, gates, and whole processors.

— **Plant equipment providers**—including Intel and Janis—develop the control, plant, and environmental infrastructure required to build and operate quantum computers. For example, unlike classical computers, quantum computers need to operate at extremely low temperatures, a hundred times colder than outer space, to maintain coherence. This requires special refrigerators.

— **Quantum computing manufacturers**—including D-Wave Systems, Google, and IBM—build quantum computers with commercial and research application for full-scale use. Google and IBM have bet on universal gate-based computers while D-Wave is providing quantum annealers.

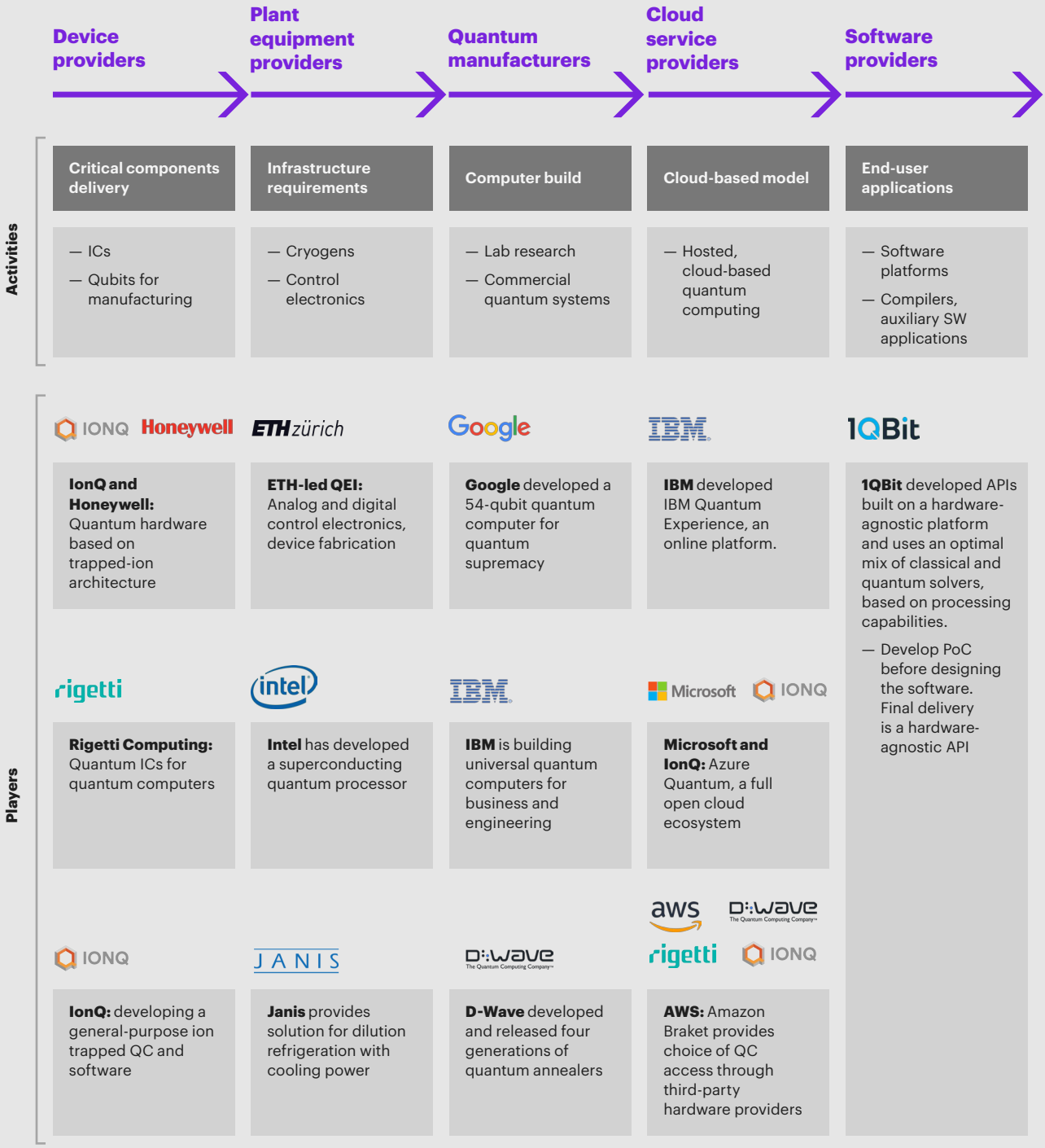
— **Cloud service providers**—including IBM, Microsoft, Amazon, and D-Wave—offer quantum computing as a service hosted on the cloud. Given the high costs of hosting and building quantum computing, this is the only practicable approach for most companies in the early days.

— **Software providers** such as 1Qbit are working to build end-user applications for quantum technology (see figure 3 on page 8).

Today's quantum value chain is beginning to take shape.

Figure 3

Quantum computing industry value chain



Notes: IC is integrated circuit. QC is quantum computing. QEI is Quantum Engineering Initiative. SW is software. API is application programming interface. PoC is proof of concept.

Source: Kearney analysis

What about quantum communication?

Quantum computing has a lesser-known sibling, **quantum communication**. Quantum communication is simpler to implement, which means that it has practical applications today. However, this application is very narrow—it addresses only secure cryptography.

Today, you're able to send credit-card information over the Internet because it's **encrypted**. Your browser establishes a secure connection by exchanging a key with the website through a secure mechanism and encrypting all transmissions with that key. Theoretically, somebody could eavesdrop on the exchange to break your encryption. With today's technologies, that's incredibly hard, but not perfectly impossible. Furthermore, these key exchange schemes can be broken with quantum computers. Quantum communication provides a new option for the key exchange—one that's fundamentally unbreakable.

To explain how, we need to go back to one of those weird properties of the qubit: coherence. The act of looking at a qubit destroys its coherence, its quantum state. As soon as I peer in, the qubit sphere collapses to its north or south pole. This leaves an indelible fingerprint. By fundamental properties of physics, the whole system will behave differently going forward. There's no way for me to cover my tracks.

So, if you encode your key in quantum states, you will always know if someone has eavesdropped on it. In effect, you can see a broken seal. You make a rule that you open a secure channel only if you know that the seal is unbroken and your key is uncompromised. If it's been compromised, you can try again, exchange another key. This is called **quantum key distribution** (QKD). QKD enables the development of encryption mechanisms that are perfectly secure, physically impossible to break.

QKD is much simpler than quantum computing, because you are merely producing and transmitting sequences of qubits, rather than performing operations on them. You can transmit them through space or through the fiber used for telecommunications. Thus, in 2017, China implemented QKD in a satellite. It distributed encryption keys to participants in a videoconference between Beijing and Vienna. On fiber, South Korea's SK Telecom used QKD to distribute encryption keys across a 400,000-subcriber 4G network that used 38 kilometers of fiber. Verizon did something similar in the Washington, D.C., area.

Thus, quantum communication is far ahead of quantum computing in implementation. QKD requires no quantum computers.[3] But its applications are quite narrow, limited to cybersecurity.

Conclusion

Although the technical milestone of quantum supremacy garnered the headlines, the real progress in quantum computing is coming from the entire industrial ecosystem being developed to exploit it. Not all of these companies will thrive, but their competition will change the world.

Why? Not because quantum computing is **faster**, but because it's a new paradigm that solves problems that humanity could not previously solve. These problems—including optimization, cryptography, engineering, and chemistry—permeate many industries. Solving them generates huge disruptive potential. Perhaps the biggest disruptions will come from breaking the entire security scheme underpinning the Internet and the digital economy.

Quantum computing faces technical challenges. But the challenge for business isn't technical, it's conceptual. This new paradigm is based on subatomic quantum mechanics, which is not only invisible but also defies logic and intuition. Thus, too many practically-oriented experts get intimidated. Yet as with any scary new idea, you need to build skills in advance to prepare for it.

[3] However, quantum memory would be needed if repeaters are implemented to relay the qubits across sections to achieve longer distances.

These are early days still. Quantum computing is at the start of a journey. It's not yet clear what will happen on that journey—unexpected roadblocks may cause detours, and unexpected breakthroughs may lead to shortcuts. But these uncertainties are precisely why business leaders, heads of technology, CIOs, and other digital leads should pay attention. You can't just go to an expected destination and wait for the explorers to arrive—you need to be closer to the journey itself.

This paper is the first of a three-part series. Part II will address in greater detail how quantum computing can disrupt industries, and when. Part III will further explore business implications and what you as business leaders can do to seize the opportunity.

Authors

Vidisha Suman
Partner, Chicago
vidisha.suman@kearney.com

Carlos Oliver
Director, Singapore
carlos.oliver@kearney.com

Arjun Bhalla
Consultant, New York
arjun.bhalla@kearney.com

Kearney's software expertise

Kearney's software team works with a wide range of firms, including software companies, firms backed by private equity or venture capital, and the many sectors such as automotive, consumer, healthcare, and manufacturing to which software has become so vital. In addition to operations benchmarking and optimization, the new practice's offerings also include products, go-to-market and channel strategy, merger-and-acquisition and due diligence, post-merger integration, exit and initial public offering strategies, and procurement and third-party spend optimization.

As a global consulting partnership in more than 40 countries, our people make us who we are. We're individuals who take as much joy from those we work with as the work itself. Driven to be the difference between a big idea and making it happen, we help our clients break through.

kearney.com