A business leader’s guide to quantum technology
Understanding potential quantum use cases to move forward with confidence

Scott Buchholz, Deborah Golden, and Caroline Brown
A quantum-powered future is an increasingly likely scenario.

Quantum technology is getting ready for its close-up. By leveraging the quirky properties of quantum mechanics—a branch of physics that describes the behavior of such particles as atoms, photons, and electrons—quantum technologies are expected to enable innovations in drug and materials discovery, financial portfolio management, climate and weather modeling, fabrication optimization, and behavioral analytics, among many others. Technology giants, governments, and early-stage startups are investing billions in a race to achieve quantum breakthroughs, while experts debate claims of quantum advances. Meanwhile, the threat posed by quantum to current encryption technology hangs overhead like the sword of Damocles.

As quantum technologies prepare to make their grand enterprise entrance, how should business leaders proceed? In this article, we seek to demystify quantum technology for business leaders and shed light on three key quantum use cases—complex computing problems, communication, and sensing. We’ll explore promising applications in each of these areas, paying particular attention to quantum computing (figure 1).

**FIGURE 1**

**Three key quantum use cases: Computing, communication, and sensing**

**Quantum computing**
Quantum computing solves advanced computational problems by leveraging quantum phenomena to process information and make calculations. Enterprise use of quantum computers is expected to ramp up over the next several years, likely growing dramatically within a decade with the appearance of fault-tolerant quantum machines.

**Quantum communication**
Quantum communication creates secure, theoretically tamper-proof communication networks that can detect interception or eavesdropping. Several quantum communication networks either have been deployed or are in progress, but it likely will be several years before they can overcome the unpredictability of quantum particles.

**Quantum sensing**
Quantum sensing devices provide higher responsiveness, accuracy, and performance than conventional sensors, due to the nature and sensitivity of subatomic particles. Quantum sensors are available today for limited production use cases and their availability and capability likely will increase substantially within five to 10 years.

Source: Deloitte analysis.
Quantum computing: Accelerating complex computational workloads

Sometimes characterized as computing’s next great evolution, quantum computing is touted for its potential to solve problems previously thought of as intractable, i.e., those that can be solved in theory, but whose complexity far exceeds the capabilities of today’s most powerful supercomputers. While it’s possible that classical computers—from the humblest laptop to the highest-performing supercomputer—could eventually solve these problems, it would take them potentially hundreds or even thousands of years. Quantum machines will be able to crack some of these advanced computational problems in hours or even minutes.

Quantum computers exploit quantum phenomena for information processing and calculations, using quantum bits or “qubits”—loosely analogous to traditional computing bits but far more versatile. And there’s a key difference between the qubits at the heart of quantum systems and the traditional computing bits under the average laptop’s hood: Classical computer bits linearly increase computing capability, whereas each qubit doubles a quantum system’s computing capability.

Unfortunately, due to the underlying physics, it’s incredibly challenging to keep collections of qubits working together. Qubits are notoriously unstable and are required to be isolated in a controlled quantum state. Some quantum machines do this by cooling qubits to temperatures of hundreds of degrees below freezing—colder than even outer space—while others entrap them in ultra-high vacuum chambers. As a result, today’s quantum machines are custom-made and exist primarily in lab environments.

In addition, duplicating qubits or even reading them collapses the delicate quantum state, complicating the process of programming, testing, and debugging. Furthermore, they’re highly sensitive to such outside interferences as temperature and vibration, which can cause noise and lead to computation errors. Because of these technical demands, the availability of a sophisticated, fault-tolerant quantum system at enterprise scale will take some time, as it relies on the unpredictable timetables of research and development in progress in labs across the globe.

While most laptops today can solve the same problems as early-stage quantum computers, quantum capability is growing exponentially. Within a decade, quantum computers are expected to be able to accelerate solutions to a large range of problems in numerous industries. To date, both Google and a group of Chinese researchers have announced successful demonstrations of quantum advantage—also known as quantum primacy or quantum supremacy—the point at which a quantum computer’s ability to solve a computational task outstrips the abilities of the fastest supercomputer to do the same. Both organizations say their quantum computers completed in less than 5 minutes carefully constructed tasks that would have taken classical supercomputers thousands or even billions of years to complete. Eventually, when quantum computers are able to easily solve complex real-world problems, they could upend the traditional long-term relationship between risk and return, potentially requiring business and government leaders to rethink the organizational and societal implications of quantum problem-solving.

What does the future look like? As special-purpose tools for completing highly specialized calculations, quantum computers are probably not going to replace classical computers. It’s more likely that they will coexist with their classical counterparts,
providing access to quantum technologies when advanced calculations are required. For a similar comparison, consider the coexistence of graphics processing units (GPUs) and central processing units (CPUs): The CPU executes most tasks while the GPU supports sophisticated graphics, video rendering, and, increasingly, machine learning.

Similarly, quantum is likely to supplement—not supplant—the cloud. In the same way that quantum computing will coexist with classical computing, it will also exist alongside cloud capabilities. More importantly, many organizations will take advantage of quantum via the cloud—65% of participants in an International Data Corporation (IDC) survey on quantum adoption say they are using or plan to use cloud-based quantum computing. This will give them access to hyperspecialized horsepower for unique workloads as part of their broader technology landscape without requiring investments in dedicated quantum computers within the enterprise.

Meanwhile, the promise of tantalizing speed continues to drive investment. And the quantum startup ecosystem is flourishing. One research firm projects the quantum computing market to grow at a CAGR of 56.0%, eventually reaching nearly US$65 billion by 2030. Another forecasts that quantum computing will give a competitive advantage to 25% of Fortune 500 companies in less than three years—a bold assertion given the maturity of the technology, although a variety of experiments in numerous industries are driving quantum computing momentum.

In fact, quantum computing has relevant use cases in nearly every industry; becoming familiar with these can help your organization understand how to prepare for quantum computing before making significant investments in the technology. Figure 2 outlines three key applications in which quantum computing is expected to dramatically accelerate workloads: optimization algorithms, data science and mathematical modeling, and quantum chemistry and materials science—all of which have an impact on multiple industries and sectors.

**Optimization algorithms.** Optimization algorithms help identify the best solution or process among multiple feasible options. As such, quantum computers are expected to have major implications on industries that rely on optimization to assess multiple potential outcomes, each with numerous dependencies and constraints.

For example, quantum computers could tackle routing challenges in real time by using live data from connected vehicles, containers and packages, roads and railways, warehouses, point-of-sale systems, and weather satellites, among others. ExxonMobil is researching how to use quantum computers to optimize routes for the global maritime shipping fleet of more than 50,000 merchant ships, each carrying up to 200,000 containers. Determining how to minimize the distance and time traveled by merchant ships—involveing calculations related to such variables as routes traveled, weather, and feasible movements between ports—is an intractable problem for classical computers.

Using similar principles, quantum computing can help companies streamline operations and manufacturing processes by solving supply chain optimization problems, such as determining the availability and pricing of manufacturing components without interrupting multifaceted supply chains.
FIGURE 2
Quantum computing: Example applications and industries

<table>
<thead>
<tr>
<th>Cross industry</th>
<th>Optimization algorithms</th>
<th>Data science/mathematical modeling</th>
<th>Quantum chemistry/materials science</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supply chain optimization</td>
<td>Cyber risk management and detection</td>
<td>Reduced data center energy consumption</td>
</tr>
<tr>
<td></td>
<td>Logistics optimization, vehicle routing</td>
<td>Fraud detection and anomaly analysis</td>
<td>Materials discovery</td>
</tr>
<tr>
<td></td>
<td>Process planning and optimization</td>
<td>Advanced predictive models</td>
<td>Quantum LIDAR/improved sensors</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consumer</th>
<th>Optimization algorithms</th>
<th>Data science/mathematical modeling</th>
<th>Quantum chemistry/materials science</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Distribution supply chain</td>
<td>Freight forecasting</td>
<td>Surfactants and catalyst discovery</td>
</tr>
<tr>
<td></td>
<td>Pricing and promotion optimization</td>
<td>Disruption management</td>
<td>Process simulation/optimization</td>
</tr>
<tr>
<td></td>
<td>Product portfolio optimization</td>
<td>Consumer offer recommender</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Natural resources and industrial production</th>
<th>Optimization algorithms</th>
<th>Data science/mathematical modeling</th>
<th>Quantum chemistry/materials science</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fabrication optimization</td>
<td>Seismic imaging</td>
<td>Surfactants and catalyst discovery</td>
</tr>
<tr>
<td></td>
<td>Energy distribution optimization</td>
<td>Drilling location detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Structural design and fluid dynamics</td>
<td>Process simulation/optimization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial services</th>
<th>Optimization algorithms</th>
<th>Data science/mathematical modeling</th>
<th>Quantum chemistry/materials science</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Financial modeling and recommendations</td>
<td>Credit, asset, financial product valuation</td>
<td>Advanced materials research</td>
</tr>
<tr>
<td></td>
<td>Credit origination and onboarding</td>
<td>Investment, product risk analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insurance pricing optimization</td>
<td>Trading strategies</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Government</th>
<th>Optimization algorithms</th>
<th>Data science/mathematical modeling</th>
<th>Quantum chemistry/materials science</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>City planning and emergency management</td>
<td>Health outcome predictions</td>
<td>Precision medicine therapies</td>
</tr>
<tr>
<td></td>
<td>Case assignments optimization</td>
<td>Climate change simulation</td>
<td>Protein structure prediction</td>
</tr>
<tr>
<td></td>
<td>Command logistics</td>
<td>Weather prediction</td>
<td>Molecule interaction simulation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health care and life sciences</th>
<th>Optimization algorithms</th>
<th>Data science/mathematical modeling</th>
<th>Quantum chemistry/materials science</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Medical/drug supply chain</td>
<td>Accelerated diagnosis</td>
<td>Precision medicine therapies</td>
</tr>
<tr>
<td></td>
<td>Improving patient outcomes</td>
<td>Genomic analysis</td>
<td>Protein structure prediction</td>
</tr>
<tr>
<td></td>
<td>Protein folding predictions</td>
<td>Disease risk predictions</td>
<td>Molecule interaction simulation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology, media, and telecommunications</th>
<th>Optimization algorithms</th>
<th>Data science/mathematical modeling</th>
<th>Quantum chemistry/materials science</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network optimization</td>
<td>Fault analysis in circuits and systems</td>
<td>Semiconductor materials discovery</td>
</tr>
<tr>
<td></td>
<td>Semiconductor chip layout</td>
<td></td>
<td>Materials process optimization</td>
</tr>
</tbody>
</table>

Source: Deloitte analysis.
Data science and mathematical modeling. Modern enterprises manipulate enormous amounts of data to identify and understand patterns, make predictions, and solve problems. As datasets become larger and more complex, and businesses increasingly use live data feeds, mathematical modeling likely will prove more and more challenging for classical computers. After all, unlike classical computers, quantum machines can effectively perform complex parallel calculations almost instantaneously.

Quantum computing has the potential to transform industries that use large amounts of data and calculations that are too complex to be efficiently performed on classical machines. For instance, in financial services, banking and securities firms are exploring the application of quantum computing to credit scoring, asset valuation, irregular behavior analysis and fraud detection, trading strategies, and investment risk analysis.

Quantum chemistry and materials science. Classical computers cannot efficiently complete the calculations required to accurately calculate and finely tune molecular properties, predict the behavior of materials, or understand how this behavior will vary with the slightest molecular changes. To learn how molecules behave, most scientists conduct time-consuming trial-and-error lab experiments. Future quantum computers are expected to conduct molecular simulations more efficiently than classical computers, making them a critical discovery tool for industries that need to predict the properties and performance of materials and simulate or optimize materials and their development processes.

Similarly, quantum computers could prove more capable and efficient than their classical counterparts in performing the complex simulations of molecular interactions that are foundational to drug discovery. Pharmaceuticals can take a decade or longer to bring to market because companies must assess billions of possible drug reactions and side effects in different human systems that vary from person to person. Improving early-stage drug discovery through quantum computing could lower the costs and reduce the time it takes to bring life-saving pharmaceuticals to market.

Future quantum computers are expected to conduct molecular simulations more efficiently than classical computers, making them a critical discovery tool for industries that need to predict the properties and performance of materials and simulate or optimize materials and their development processes.

Today’s quantum computers only allow realistic simulations of simple molecules with a couple of atoms; they don’t yet have enough qubits to compete with classical machines. Research is ongoing and rapidly advancing. For example, a recent collaboration between the US Department of Energy’s Argonne National Laboratory and the University of Chicago has resulted in a new calculational method that improves the accuracy of quantum simulations of the structures and behaviors of chemical molecules and complex materials.
SECURITY IMPLICATIONS OF QUANTUM COMPUTING: POSTQUANTUM CRYPTOGRAPHY

Current encryption protocols, such as Secure Socket Layer (SSL) and Transport Layer Security (TLS), based on existing public-key algorithms, are capable of protecting network communications from attacks by classical computers. A fault-tolerant quantum computer, however, could break the mathematical challenges that underlie these and other protocols in a matter of hours or even seconds. Postquantum cryptography—a software-based algorithmic technique also referred to as quantum-proof, quantum-safe, or quantum-resistant cryptography—likely will grow in importance as quantum computing systems mature and become more widely available. Postquantum cryptographic systems, which will need to run on classical computers, will rely on more complex mathematical problems that cannot be easily solved by quantum computers and will be interoperable with current communication protocols and networks.

The US National Institute of Standards and Technology (NIST) estimates that within about 20 years, “sufficiently large quantum computers will be built to break essentially all public key schemes currently in use,” further noting that the existing public key cryptography infrastructure was 20 years in the making. Therefore, suggests NIST, the time to prepare cybersecurity systems for quantum computing is now.

Others expect quantum computing to become a threat on an even earlier timeframe. Speaking at the 2020 World Economic Forum’s Annual Meeting, Google CEO Sundar Pichai warned that quantum computing will be able to break current encryption methods within five years.

The NIST began soliciting quantum-resistant public-key cryptographic algorithms in 2016 and has gone through three rounds of examination and evaluation, winnowing the list of algorithms down to seven finalists and eight alternates. It is planning at least one more round of testing and hopes to release the initial standard by 2022.

In the meantime, there’s no need to panic; instead, get prepared. While awaiting the release of the NIST standards, organizations can take four actions to increase their crypto-agility—the ability to easily and securely replace cryptographic algorithms and parameters.

- **Audit data and cryptographic assets** to provide an accounting of sensitive data, its retention requirements, and location (e.g., on-premises or in the cloud).

- **Identify the types of cryptographic keys** being used, their characteristics, and their location in existing computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures, and access control mechanisms.

- **Identify potential future infrastructure limitations** (e.g., bandwidth and latency).

- **Maintain situational awareness**, as always, of data, infrastructure, and other assets and practice good cyber hygiene.
Quantum communication: Protecting communication networks

Unlike postquantum cryptography—which uses new quantum-safe encryption algorithms that run on classical computers, as discussed in the sidebar, “Security implications of quantum computing: Postquantum cryptography”—quantum communication is a hardware-based solution leveraging the principles of quantum mechanics to create secure, theoretically tamper-proof communication networks that can detect interception or eavesdropping.

While there are different techniques to achieve quantum communication, quantum key distribution (QKD) is one of the most mature. In QKD, parties use quantum-based techniques to exchange encryption keys, which are then used to transmit data across traditional optical networks. Because the key exchange cannot be changed, cloned, copied, or intercepted without detection, QKD can provide a very high level of network security.

The first commercial QKD systems began to appear in the early 2000s, and ongoing global projects aim to extend the distance of viable QKD transmissions. In the United States, organizations have achieved QKD using more than 600 miles of existing optical fiber that connects Washington, D.C., New York City, and Boston. The solution, which links Wall Street financial markets to New Jersey–based back-office operations, supports not only QKD and other physics-based encryption methods but also math-based techniques (such as postquantum cryptography).

Chinese researchers have several QKD initiatives using both in-ground optical fiber and over-the-air satellite links, including a recently completed 2,900-mile network that combines the two transmissions technologies. These networks serve more than 150 industrial users. Chinese organizations have also experimented with short-range quantum communication networks that rely on drones to carry signals.

Current technology limitations make QKD impractical for immediate widespread adoption: It’s slow and requires expensive transmitters and receivers. In addition, because messages can degrade after traveling about 60 miles, QKD requires the use of signal repeaters, relays, and routers that could be vulnerable to attack. However, as quantum communication technologies (including QKD) continue to improve, we expect them to be a key component in securing vital communications.

Quantum sensing: More accurate sensing and measurement

Subatomic particles are sensitive to rotation, acceleration, time, and electric, magnetic, and gravitational fields, among other external effects. This allows them to be used to make very responsive sensors whose accuracy and performance exceed that of conventional sensors. Ongoing research initiatives are focused on developing cheaper, lighter, more portable, and more energy-efficient quantum sensors.

Quantum sensors have the potential to replace existing sensors in many applications, including...
locating and monitoring oil, gas, and mineral deposits; surveying construction sites; and detecting the slightest environmental, seismic, or weather changes. In the transportation sector, quantum sensors promise to dramatically improve precise navigation and positioning systems. For example, Airbus is exploring the use of quantum sensors to more accurately measure attributes such as frequency, acceleration, rotation rates, electric and magnetic fields, and temperature to improve its navigation systems.

Quantum technologies are gaining momentum and are expected to migrate from research labs to real-world commercial environments within this decade.  

In the medical field, quantum sensors likely will be used to analyze temperature, heart rate, and other vital signs and to advance the accuracy of magnetic resonance imaging, furthering the ability to track the progress of cancer treatments and diagnose and monitor such degenerative diseases as multiple sclerosis.

Quantum sensors are available today for limited production use cases; their availability and capability likely will grow dramatically within five to 10 years.

Get prepared

Scientists have been musing about quantum technology for decades, and quantum dynamics is fraught with obstacles. But quantum technologies are gaining momentum and are expected to migrate from research labs to real-world commercial environments within this decade. And in terms of potential scale and impact, quantum technologies have much in common with cloud computing. A wait-and-see attitude could cause organizations to miss critical opportunities to test and experiment with the technology while their competitors gain ground.

We encourage a more strategic approach, heavily seasoned with pragmatism.

- **Understand industry impact.** Learn about quantum’s potential repercussions in your industry. What complex problems could quantum help you solve? Be aware of important technology developments and pay attention to how others in your field are investing in and experimenting with quantum technologies.

- **Develop a strategy.** Bring together existing talent with the appropriate skills and knowledge to develop a quantum strategy. Even if the strategy is to take no immediate action, determine a trigger event—such as a competitive or technology development—that will serve as a prompt for further quantum investments and exploration. Decide who will lead the quantum charge when it’s time to engage.

- **Monitor technology and industry developments.** Refine your strategy as events warrant and don’t let your stated trigger event pass by without taking the appropriate action.

- **Improve your crypto-agility.** Come up with a plan for addressing the security implications of quantum computing and make headway in improving your organization’s crypto-agility.

Although quantum technologies are in their infancy, their potential impact on industries and businesses is too great to ignore. Respect the risk of falling behind and be proactive in preparing for the quantum future.
Endnotes


2. Absolute zero on the Kelvin scale, or approximately –460°F.


19. Ibid.


Acknowledgments

The authors would like to thank Colin Soutar, Scott Wilkie, Jacob Alexsen, Matt Caccavale, Markus Stulle, Itan Barmes, Daniel Beaulieu, Shannon Gray, Stefanie Heng, Mary Hughes, Maria Wright, and Aaron Dozzi for their contributions to this article.
About the authors

Scott Buchholz | sbuchholz@deloitte.com

Scott Buchholz is a managing director with Deloitte Consulting LLP and serves as the Government and Public Services chief technology officer and the US Quantum leader. A leader and visionary with more than 25 years of experience, he advises clients on how to navigate the future using existing and emerging technologies. Buchholz also leads Deloitte’s efforts to explore quantum computing and quantum technologies.

Deborah Golden | debgolden@deloitte.com

Deborah Golden, a principal with Deloitte & Touche LLP, is the US Cyber & Strategic Risk leader for Deloitte Risk & Financial Advisory. Golden has more than 25 years of cross-industry experience, focused predominantly within government, life sciences and health care, and financial services industries. She primarily helps commercial organizations and government agencies navigate multifaceted cyber problems and transform business or mission strategies and operations. She received a bachelor’s degree in finance at Virginia Tech and a master’s degree in information technology at George Washington University.

Caroline Brown | carolbrown@deloitte.com

Caroline Brown is a manager and senior writer with Deloitte LLP, where she writes research reports, articles, and other content for CIO Research and Insights and CIO Journal. She specializes in enterprise technologies, technology and industry trends, IT capabilities and competencies, organizational culture, and business processes.
Contact us

Our insights can help you take advantage of change. If you’re looking for fresh ideas to address your challenges, we should talk.

Scott Buchholz
US Quantum leader | Emerging technology research director
Government & Public Services chief technology officer | Deloitte Consulting LLP
+1 571 814 7110 | sbuchholz@deloitte.com

Scott Buchholz is a managing director with Deloitte Consulting LLP and serves as the Government and Public Services chief technology officer, US Quantum leader, and the national emerging tech research director.
Quantum technologies, and their heady promise, are in the news. With the promise of breakthrough innovations in drug development, financial modeling, climate change, traffic optimization, machine learning, batteries, and more, is now the time to invest? And how much worry is warranted about quantum computing's future ability to break today's encryption? Today, the current state of the mind-bending technology remains limited. Yet tomorrow's breakthroughs are unknown. How should business leaders think about the potential and the promise of these technologies? Learn more.