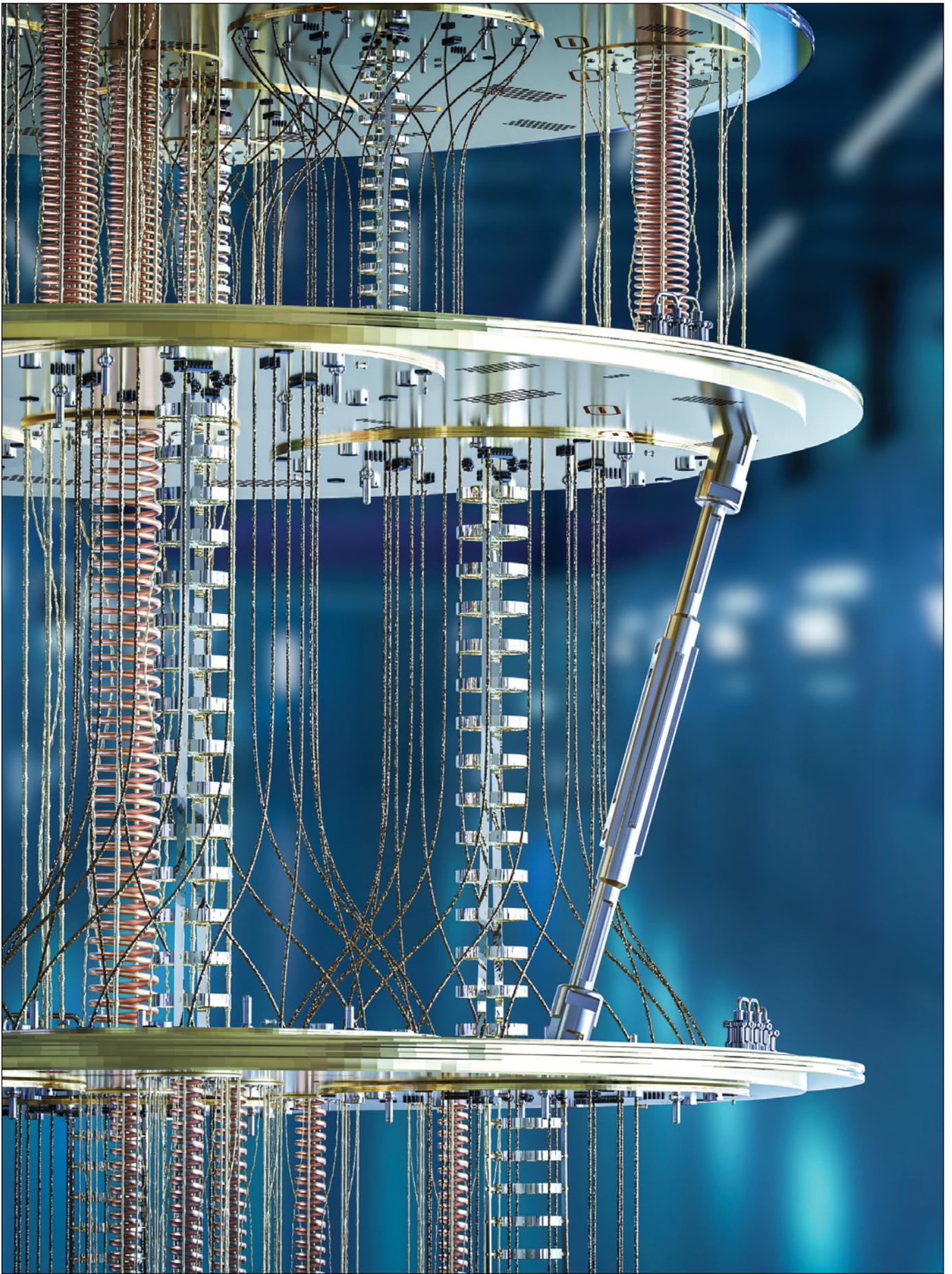STANFORD UNIVERSITY

# THE STANFORD EMERGING TECHNOLOGY REVIEW 2026
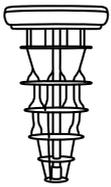
A Report on Ten Key Technologies and Their Policy Implications

**CO-CHAIRS** Condoleezza Rice, Jennifer Widom, and Amy Zegart
**DIRECTOR AND EDITOR IN CHIEF** Herbert S. Lin | **MANAGING EDITOR** Martin Giles

# QUANTUM TECHNOLOGIES

## KEY TAKEAWAYS

- Quantum computing is advancing rapidly, making clear progress toward solving practical problems such as breaking existing public-key encryption algorithms, enabling new materials design, and supporting applications in chemistry. More speculative uses include machine learning, weather modeling, and financial portfolio optimization.

- Quantum networking and sensing are emerging as powerful technologies—networking may be critical for scaling computers to utility levels, while sensors are already transforming fields such as medical imaging and gravitational detection.

- Government-funded basic research in academic labs remains the foundation for breakthroughs, and sustained investment is essential to maintain leadership as companies push applications toward real-world utility.

## Overview

Quantum technologies are based on the physics of quantum mechanics, which emerged early in the twentieth century. Since then, quantum mechanics has shaped many technologies, from nuclear weapons to the transistors in smartphones to magnetic resonance imaging (MRI) machines in hospitals. But in these applications, the constituent atoms have been controlled in aggregate, with large, uncontrolled groups of particles all in multiple states manipulated together as an ensemble.

Modern quantum technology seeks to control the components of an ensemble particle by particle. In 2025, the Nobel Prize in Physics was awarded for "the discovery of macroscopic quantum mechanical tunnelling and energy quantization in an electric circuit."[1] The goal is to develop real-world applications by precisely controlling many particles that are all doing many things simultaneously, which requires an enormously complex effort. In the past twenty years, several different hardware approaches have

emerged to control and detect individual particles and their states. In just the past five years, this control has become strong enough that useful quantum technologies are starting to be built and used (see sidebar on entanglement).

Precise control allows for the management of superposition and entanglement. Superposition is an empirically validated principle of quantum mechanics stating that particles can be in different states (e.g., in different places or spinning different ways) simultaneously. Entanglement is the quantum phenomenon in which particles are linked in a correlational sense. This means that measuring a property of one reveals a correlated property of the other instantly, even if they are separated by very long distances and their properties have not been individually determined beforehand (see sidebar).

A particularly important aspect of this new quantum paradigm is that measuring a quantum system disturbs it. Therefore, it does not work to measure everything and process the data later. Instead, it is necessary to carefully craft new types of hardware that measure directly and exclusively what we want to know and do so only when we want to know it. Violating any of these principles (e.g., by making a query at the wrong time) reduces the quantum-enhanced accuracy in measuring items of interest. This insight is important to all of the technologies discussed below.

While there are many potential technologies based on quantum principles, the three most mature are **quantum computing**, **quantum communication**, and **quantum sensing**. In the long run, it is most likely that these quantum technologies will complement rather than replace their classical counterparts.

⊶ **Quantum computing** will be useful primarily for solving problems that classical computing cannot, but these problems for the most part will be niche problems rather than general ones of broad interest.

---

## ON ENTANGLEMENT

Alice and Bob share a coin cut perfectly into two halves, one showing heads and the other tails. Alice keeps the tails half and places the heads half into an opaque envelope, which she gives to Bob without revealing its content. From Bob's perspective, before opening the envelope, the coin inside could be either heads or tails, resembling a quantum superposition. When he eventually observes heads, he instantly knows Alice's half must be tails, no matter the distance between them.

This correlation illustrates the essence of quantum entanglement: Bob's measurement does not cause Alice's outcome but instead reveals an existing relationship that manifests instantly without any transfer of information faster than light.

Although the coin analogy is helpful for understanding entanglement, it is not perfect. In the analogy, the coin halves have definite states regardless of whether they are observed—the outcome is simply hidden until revealed. In contrast, entangled quantum particles do not have definite states before measurement. Instead, their joint state exists as a superposition, meaning that the properties of both particles are fundamentally linked and undefined until one is measured. When a measurement is made on one particle, the outcome of a corresponding measurement on its partner is instantly determined—no matter how far apart they are.

This behavior cannot be fully understood using everyday, classical intuitions. It is a uniquely quantum phenomenon, confirmed by decades of rigorous experiments. Importantly, this "spooky" correlation is not just a scientific curiosity or a matter of philosophy—it is the foundation for groundbreaking quantum technologies in computing, communication, and sensing.

- **Quantum communication** may also have niche applications, such as for cryptographic key distribution and distributed quantum computing; these are discussed later in this chapter. However, it is unlikely to be a broadly applicable technology for communications infrastructure because it requires specialized hardware to implement.

- **Quantum sensors** will not render classical sensors obsolete in the short to medium term. Rather, they will be used primarily in application areas where they have particular advantages, such as greater sensitivity or measurement stability. To the extent that quantum sensors push the limits of what quantum mechanics allows in terms of power usage, sensitivity, size, and so on, most sensors are likely to eventually incorporate quantum technology in some form (though not necessarily as quantum networked sensors).

# Quantum Computing

## Essential Points

- Quantum computers promise major speedups for factoring large numbers and simulating quantum particles and processes—essential for breaking certain kinds of encryption and for chemistry and materials science. Quantum computing will remain a specialized, niche technology rather than one with broad real-world impact unless and until practical and effective algorithms for finance and other fields are developed.

- All known applications of quantum computers will require error correction to outperform traditional, classical computers. Quantum computing hardware has reached the "break-even" point (i.e., where error correction is feasible) enabling practical scaling.

- The main scaling challenge is not simply in increasing the number of quantum bits, or qubits, in a module. Rather it is in controlling individual qubits. Scaling of quantum computers comparable to what has been achieved for classical computers depends on the availability of robust error-correction approaches—expected within the next few years—and on leveraging established techniques from semiconductor and photonics engineering.

## About Quantum Computing

Quantum technology offers a fundamentally new computational paradigm. Classical computers use individual bits as the smallest unit of information, with each being 0 or 1. In contrast, qubits—the smallest unit of information for a quantum computer—can be in multiple states simultaneously; that is, qubits can exist in superposition. This reality is one aspect of what allows quantum computers (like the one shown in figure 7.1) to process a vast number of possibilities at once, a phenomenon called quantum parallelism. This capability makes quantum machines a potentially game-changing advance in the field of computing.

In gate-based quantum computing—in contrast to quantum simulation, discussed later in this chapter—qubits are manipulated through discrete operations performed by quantum gates. These gates alter the state of the qubits they act upon. Serving as the quantum analog of logic gates in classical computers, they form the fundamental building blocks of quantum circuits that execute calculations by chaining together individual gate operations.

**FIGURE 7.1**    The wiring infrastructure of a quantum computer
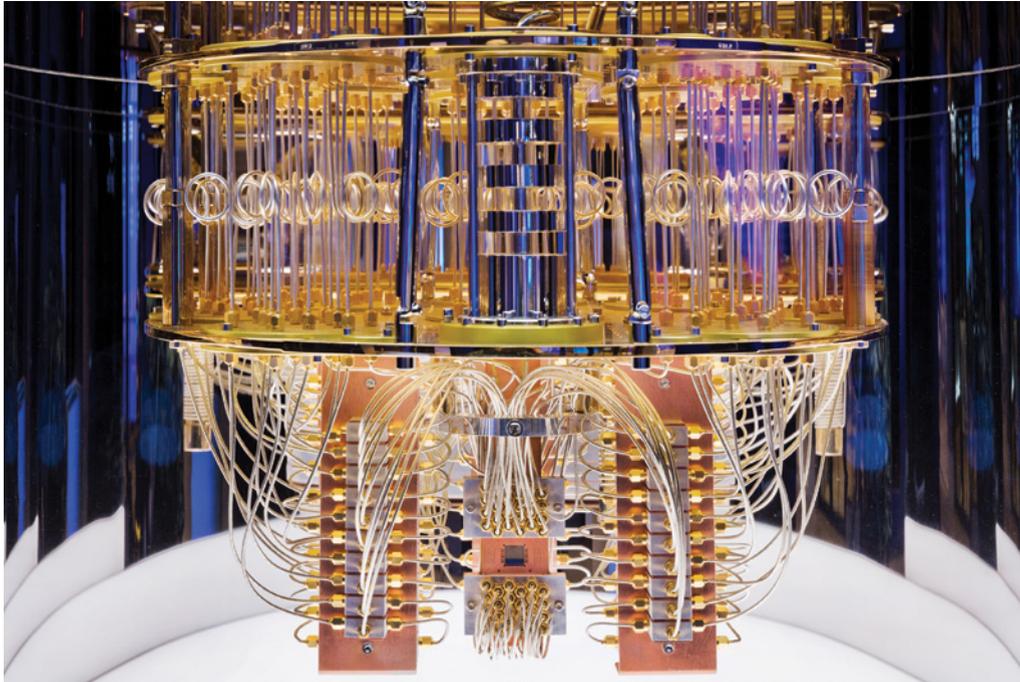


Source: IBM, CC BY-ND 2.0

By carefully sequencing these operations, gate-based quantum computers can, in principle, perform a very specific set of calculations, including for quantum chemistry and certain kinds of codebreaking, much faster than their classical counterparts. This possibility and the potential for a broader array of applications down the line have driven up public and private investment in quantum computing in recent years. (Figure 7.2 shows statistics on venture capital investment.) This rapid growth reflects investor interest in the field, though significant challenges must be resolved before quantum computing's value can be realized.

Chief among these challenges is obtaining the answer to a problem once a quantum computation has been performed. Because the qubits are in a superposition state, a computation that is performed on them generates many possible results. However, nearly all of these will not be useful to solving the problem at hand. Realizing the advantage of a quantum computer requires developing algorithms that surface the useful result often enough that it's possible to identify it without having to repeat the calculation too many times. This is fundamentally different from classical computing, which produces deterministic results of computations.

A second important challenge is that quantum computing operations can be disrupted by errors caused by small amounts of "noise" in the environment, such as atomic decay, small vibrations, or tiny changes in temperature. This noise can disrupt the delicate quantum state of qubits and lead to errors. In other words, interaction with the outside world generally destroys superposition states that enable quantum parallelism, so it's crucial to minimize this noise as much as possible and to correct the errors that cannot be avoided.

**FIGURE 7.2** Funding trends in quantum computing and quantum technologies

**Venture Funding of Quantum Computing**
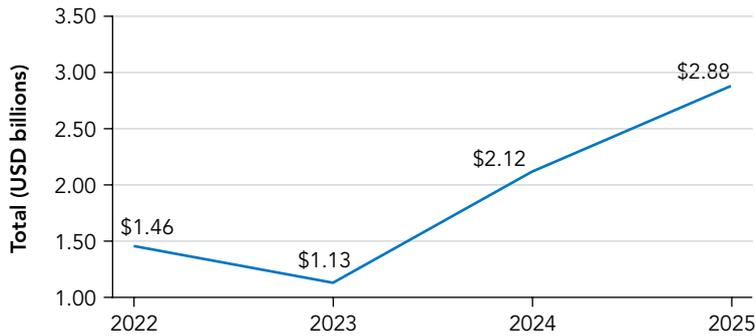


**Venture Funding of Quantum Technologies**
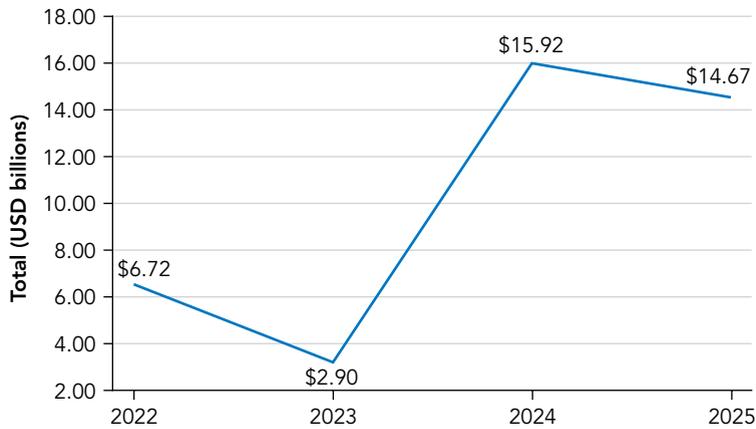


Note: 2025 numbers are partial-year data.

Source: CB Insights

Compensating for these errors—a process called error correction—accounts for upward of 90 percent of what a quantum computer actually does; the remaining 10 percent, or less, is spent actually computing. Error correction is the process of storing information in a way that it is resilient to noise and other error mechanisms. This encoding uses many physical qubits in the quantum hardware to encode one logical qubit, which is a qubit that is robust against noise. A quantum computer performs its algorithms

between these logical qubits while continuously correcting the errors within them that emerge through the processing. With current approaches, hundreds to thousands of physical qubits are needed to encode every logical qubit used for computation.

A third challenge is the fact that today, there are few problem-solving algorithms to run on quantum computers that have any practical value. The quantum research community still lacks a complete

understanding of the algorithms that would ensure quantum computing provides any speedup at all over classical computers.

Put differently, an important constraint on accomplishing useful tasks with quantum computers is the current lack of suitable algorithms for those purposes; this is in addition to the lack of sufficiently powerful quantum computers themselves. The lack of algorithms is partly due to a chicken-and-egg problem: It is extremely challenging to invent and test new algorithms without the underlying hardware to rapidly test and guide the process. Error-corrected hardware, when available, will enable empirical development and benchmarking of quantum algorithms; currently, this can be done only by formal mathematical proofs of correctness and speed.

## *Key Developments*

### QUBIT TECHNOLOGY

Numerous hardware approaches are under active exploration for construction of physical qubits. At the time of this writing, the most visible candidates include the following:

- **Trapped ions**  Atoms that are missing an electron (i.e., ions) are not electrically neutral, so they can be trapped by radio-frequency electric fields. The ion encodes information in its internal states, and the information can be read out using laser beams. Computations are performed through conducting controlled collisions between ions.

- **Superconducting circuits**  Composed of nano-fabricated chips, these circuits must be kept cold at temperatures near absolute zero (–273.15°C). Like traditional electronics, computations are performed by running currents through the chips. However, the fabrication procedures are different from those of ordinary semiconductors.

- **Neutral atoms**  These are atoms that are not missing any electrons and hence must be trapped with laser beams. Moving these laser beams

around allows the atoms to collide and perform computations. The laser traps are weak, so the atoms must be held in an extreme vacuum that is comparable to interplanetary space.

- **Silicon spin qubits**  These are single electrons trapped in structures resembling modern silicon transistors that often use standard semiconductor foundry processes. These qubits also operate at temperatures near absolute zero. They are somewhat less developed than the approaches described above due to their extreme sensitivity to small material defects. However, they are advancing rapidly and have the potential to take advantage of the large investments and rapid learning rates in the semiconductor industry.

- **Photonic qubits**  These qubits encode information in states of optical frequency light fields (usually telecom-band photons), perform operations running at room temperature, and interface naturally with fiber networks. Proponents claim scalability through wafer-scale photonics, low-loss fiber, and other factors. In practice, progress has been constrained by the inability to develop an appropriate test environment that could provide convincing evidence of practical advantage.

In the early days of quantum computing, trapped ions and superconducting circuits were seen as the leading candidates. In the past decade, neutral atom quantum technology has become a true competitor to them. This development demonstrates that the "horse race" for the quantum transistor remains open, leaving opportunities for the emergence of alternative approaches that scale more easily and deliver improved underlying performance.

Two dark horses in this category are photonic and topological qubits. Photonic qubits aim to leverage silicon photonics manufacturing to achieve fault tolerance, but using them in quantum gates is technically challenging. Topological qubits aim to store information in a naturally protected form that, under ideal conditions, should be less sensitive to changes

in the external environment—though recent research on this technology has been challenged.[2] Both platforms have attracted significant public and private investment and have promised compelling pathways to leapfrog current leaders in demonstrated quantum capabilities. However, neither platform has yet demonstrated computation at even the scale of a few qubits, and both face substantial technical roadblocks.

One of the primary determinants of front-runner status of any physical qubit technology is its fidelity. Fidelity refers to how accurately a quantum gate executes its intended operation compared to an ideal error-free gate—the greater the similarity between the two, the higher the fidelity of the gate under examination. This is important because the computation needed to perform error correction in a quantum computer is itself vulnerable to error.

For a given qubit technology and error-correcting algorithm, a process called "co-design" for the code and platform establishes a break-even threshold for fidelity. This means that the errors corrected by the error-correction circuitry are barely equal in number to the errors introduced because of the operation of that circuitry. Higher gate fidelities increase the former number relative to the latter (more and more errors corrected compared to the number of errors introduced). In practice, this break-even threshold across a number of technologies is around 99 percent.[3]

From a practical standpoint, there is a broad consensus in the field that gate fidelities above 99.9 percent (that is, significantly better than the break-even threshold) will enable the construction of practical quantum computers that do not require a prohibitive amount of error correction or a prohibitive number of physical qubits to implement that error correction.

The most important development in qubit technology is that trapped ions, neutral atoms, and superconducting circuits have all now crossed the "break-even" threshold. However, quantum computing faces uncertainty over which of these—or perhaps one of the dark horse possibilities—will lead to the best scalable architecture. Unlike classical computing, in which transistors proved superior to vacuum tubes and became the technological foundation for a fabrication industry that set classical semiconductors on the path of rapid and sustained cost reductions over decades,[4] the "quantum transistor" has yet to be identified. Indeed, rather than a single winner, multiple platforms may well coexist, each with unique strengths and challenges. As a result, quantum computing progress is likely to depend on hardware innovation, error correction, and application-specific advances.

## QUANTUM MEMORY

Memory in quantum computers serves approximately the same function as it does in classical computers: It holds quantum information in qubits while preserving their quantum properties like superposition and entanglement until operations can be performed on that information. An example of recent

Unlike classical computing, in which transistors proved superior to vacuum tubes . . . the "quantum transistor" has yet to be identified. Indeed, rather than a single winner, multiple platforms may well coexist.

progress is the development of quantum memory that extends storage times of quantum states by a factor of up to thirty.[5] Quantum memory also plays a critical role in quantum repeaters, which are discussed in the Quantum Communications section later in the chapter.

## SCALE-UP OF QUANTUM COMPUTERS

At present, the state of the art is computers with thousands of atomic qubits and hundreds of superconducting and ionic qubits. In each of these platforms, these physical qubits have been combined to redundantly encode dozens (currently up to forty-eight) logical qubits,[6] albeit at error rates orders of magnitude too high for scalable computation. To achieve the error rates and computer sizes necessary for scalable computing, more logical qubits to perform computations and more encoding redundancy to reduce the error rates of the logical qubits are required. In other words, many, many more physical qubits are going to be needed.

Current resource estimates indicate that thousands of logical qubits, and thus millions of physical qubits,[7] will be required to build quantum computers that can break current public-key encryption schemes. Achieving systems at this scale requires innovation in qubit design and performance, and substantial progress in the ability to manipulate so many qubits simultaneously.

Thus, from here, the game is to scale, increasing the qubit count without sacrificing qubit performance. As mentioned above, a gate fidelity of 99.9 percent (corresponding to an error rate of 0.1 percent per gate operation) is expected to be sufficient for quantum computation at scale. Along similar lines, a million physical qubits, either distributed across networked modules or in a single large quantum computer, will be required to perform practically useful computation.[8] Present-day industry road maps suggest that individual quantum computing modules with tens of thousands to hundreds of thousands of physical qubits are feasible within the next decade or so.[9]

Controlling the operations in which these qubits are involved is another key task in scaling up. A quantum computer must be able to control each qubit it uses. To do so, a control channel needs to be established that sends signals to every qubit; if a quantum computer with a million qubits requires each individual qubit to be manipulated on a microsecond timescale, a control bandwidth of around one terabit per second is needed.

Such rates are usually achieved, but they exceed the internal memory bandwidth of a standard microprocessor chip. Both the processing power to generate this control and the physical control hardware require technology development. This will likely be in the form of applications-specific integrated circuits for all quantum computing platforms, faster cameras, and other supporting technologies. Today, control technology for large numbers of qubits lags behind the ability to fabricate and trap them. Developing tools for control is likely to be a broad effort, requiring deep understanding of hardware architectures, significant expertise in various hardware development paradigms, and novel solutions combining them.

## QUANTUM SIMULATION

Despite a huge amount of contemporary discussion and excitement about the revolutionary importance of quantum computing, there are currently few real-world applications of the technology. Those that do exist are examples of quantum simulation.

Quantum simulation works by creating a physical system—in this case, physical qubits—whose behavior is mathematically analogous to the problem being solved. The key insight is that the equations governing the physical system must have the same mathematical structure as those governing the problem; the specific physical details are irrelevant. Since the system's evolution is determined by its governing equations (and its starting conditions), the physical realization of the original problem becomes a simulator of it. Observations of the system's behavior can then be interpreted as the problem's solution.

By applying carefully controlled stimuli, such as electromagnetic fields or laser pulses, to qubits and observing their subsequent behavior, it is possible to drive the system to evolve naturally. Quantum simulations are also sensitive to fluctuations in the external environment. However, they typically do not employ active error-correction protocols. Instead, their design emphasizes minimizing external disturbances as much as possible.

Quantum simulation is most suitable for specific, narrowly defined problems. Perhaps the most prominent application is the modeling of the quantum properties of complex materials. This effectively mimics those materials using qubits, thereby allowing researchers to explore material behaviors otherwise exceedingly difficult to study classically.[10]

For example, French research teams have similarly shown how quantum simulation using neutral atoms for qubits can be used to model solvent interactions in proteins, which is critical for advancing drug discovery.[11] Additional work has demonstrated the usefulness of quantum simulations in clarifying the conditions required for high-temperature superconductivity and in refining classical numerical models of material behavior.[12]

### Over the Horizon

#### APPLICATIONS AND SOFTWARE

Although gate-based quantum computing could in principle be a general-purpose computing technology, its specialized hardware and software requirements currently make it impractical as one. The expense and effort of meeting such requirements are worth it only when the problems being solved are sufficiently important or have enough economic value.

Below we describe two of the most promising known applications for gate-based quantum computing:

○─ **Breaking certain algorithms for asymmetric cryptography**  Discussed in more detail in chapter 3, on cryptography and computer security, the most commonly used algorithms in asymmetric cryptography are based on the difficulty of factoring large numbers and related problems. Classical computers factor numbers by testing one set of possible factors at a time, a process whose time to completion grows very rapidly as the numbers get very large. Shor's algorithm, developed in 1994 by Peter Shor (see figure 7.3), exploits quantum parallelism to efficiently perform such tests over all possible inputs simultaneously. This reduces the time needed to break encryption from thousands of years to potentially hours or minutes with a sufficiently powerful quantum machine.

Shor's algorithm is expected to provide exponential speedup over what is possible with classical computing, making it a top candidate application for quantum computing. The best current estimates suggest that the most commonly used asymmetric cryptographic algorithm—RSA-2048—could be breakable in days to weeks on a quantum computer coming online in five to fifteen years.[13] (Note, however, that Shor's algorithm is not an algorithm that works against all possible asymmetric cryptography algorithms. It only works against

**FIGURE 7.3**  Peter Shor, creator of Shor's algorithm
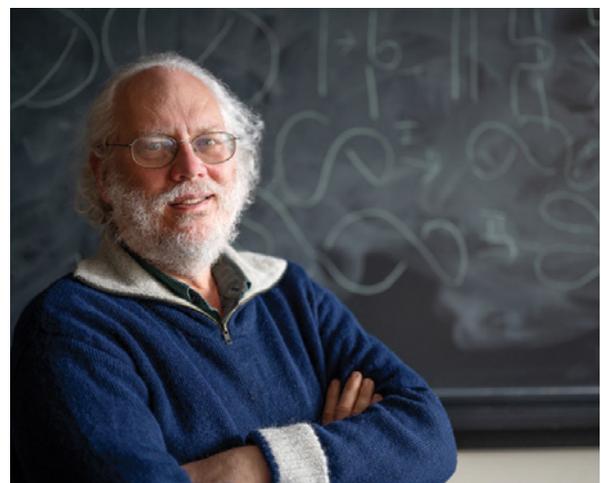


Source: Christopher Harting, *MIT News*

asymmetric algorithms based on the difficulty of factoring large numbers and related problems.)

- **Simulating the quantum world**  From chemistry to materials science, simulations using quantum computers are expected to be exponentially faster than ones using classical computers. They are expected to have significant positive impacts on problems like nitrogen fixation, drug development, and superconductivity[14] and enable breakthroughs in chemical, drug, and catalyst design. The analog simulators currently solving these problems are likely to be replaced by more precise simulations on gate-based quantum computers.[15] Ultimately, quantum computers may generate complex quantum data that classical computers can then use to efficiently manage more routine quantum chemistry simulations.[16]

These application areas have significant economic or national security value, and gate-based quantum computing potentially offers substantial speedups for the above problems over classical computing.

How substantial? Most desirable is an exponential speedup. When this is possible, a quantum computer can finish a task in a practical amount of time that would take a classical computer so long that it's essentially impossible—sometimes longer than the age of the universe. An example would be a classical computer taking a billion years to solve a complex chemistry problem that a quantum computer with exponential speedup could do in a few minutes. When they are possible, exponential speedups are transformational.

By contrast, a polynomial speedup can still be substantial.[17] However, polynomial speedup gains in practice are limited by the much slower clock speeds of quantum computers (that is, the number of operations per second that a quantum computer can perform compared to a classical computer). Equally important, continuing improvements in classical computing hardware over the next decade are likely to deliver performance gains of a similar magnitude and offer a more probable near-term path to achieving them.

For many computational problems that need to be solved, the consensus among experts seems to be that if speedups using quantum computing exist at all, they will most likely be polynomial in nature.[18] In addition, such speedups may require careful optimization of quantum computers and significant hardware development to realize practical gain. Shor's algorithm for factoring (and thus for certain types of codebreaking) and quantum simulation for chemistry and materials science are among the few notable examples of exponential speedups currently known to exist over the best classical algorithm.

In parallel with these algorithmic advances, work is ongoing at a number of companies to develop unified (and often cloud-based) frameworks that are qubit-hardware-agnostic and programmable by non-specialists, thereby making quantum computing more widely accessible. Broad adoption of such tools is predicated on quantum hardware advances that provide fault-tolerant quantum computers and algorithmic advances that clarify commercial use cases.

It is difficult to predict which problems will be most directly impacted by quantum computing. However, what seems clear from the evolution of both classical computers and neural networks is that new computing paradigms always lead to new opportunities. Further research in quantum algorithms is thus essential and is likely to accelerate as quantum computing hardware for testing the algorithms becomes more sophisticated and accessible.

## ON QUANTUM SUPREMACY AND ADVANTAGE

While fault-tolerant quantum computers capable of useful computation for codebreaking, quantum chemistry, and other uses remain some years out, an ongoing effort exists to demonstrate *quantum supremacy*. This refers to the quantum computation of any quantity sufficiently complex that a classical computer cannot replicate the same result.

The endeavor to demonstrate quantum supremacy has resulted in an extremely productive race between quantum computing teams and classical computing teams, with the former running ever-more-complicated "random quantum circuits" and the latter demonstrating that they can in fact predict the output of these circuits on classical computers.

The latest generation of superconducting quantum processors are large enough that they can now perform certain calculations that are difficult or impossible to replicate on classical computers.[19] However, this is a benchmark—the calculated quantity is not inherently useful, even if it is beyond the reach of a classical computer to calculate. Nonetheless, this work points to classes of problems where quantum supremacy is indeed possible and drives progress in understanding the quantum/classical computability boundary.

By contrast, the term *quantum advantage* is generally used to denote the superiority of a quantum computer in solving a practical, useful problem faster or more accurately than a classical computer. In addition, it signals a relevance to real-world tasks and potential commercial applicability. To date, true quantum advantage in computing has not been achieved on any useful real-world problem.

# Quantum Communication

## Essential Points

○— Post-quantum encryption algorithms are already being deployed and used to protect against attacks based on factoring and related problems. Quantum communication for key distribution will be broadly useful only if it turns out that these algorithms are flawed in practice.

○— Quantum networking for connecting individual quantum computing modules will likely be necessary at least in the shorter term to solve useful or meaningful problems.

## About Quantum Communication

Quantum communication uses the principles of quantum mechanics, such as superposition and entanglement, to encode, transmit, and secure information between separate systems. It has two primary applications: One is related to privacy and security in data transmission and identification. The other is transmission of intrinsically quantum data, essential for tasks in scalable quantum computing and networks of sensors linked through quantum entanglement.

## Quantum-Enabled Data Security

The security afforded by quantum communication is based on its application to what is known as the key distribution problem, an essential element of secure digital communication.

Today's public-key cryptography, discussed in chapter 3, on cryptography and computer security, is susceptible to attacks from future quantum computers. This is because, as discussed earlier, it relies upon the difficulty of factoring large numbers (or other related problems) for its security. Cryptographers are developing quantum-resistant algorithms—more precisely, algorithms that will resist Shor's algorithm running on quantum computers. However, if they are unsuccessful, alternative key distribution methods, such as quantum key distribution (QKD), will be necessary.

QKD does not rely on the infeasibility of obtaining private keys from public keys. The security it affords is based on the fact that quantum information cannot be copied.[20] That is, it is impossible to create an exact, independent copy of an arbitrary and unknown quantum state—a statement known as the no-cloning theorem. Copying quantum information always perturbs the original in detectable ways. By contrast, classical information can be perfectly copied without perturbation to the original.

If quantum information cannot be copied, it means that it is impossible to eavesdrop on communications

conducted with quantum data. Eavesdropping entails a third party—say, someone called Eve—listening in to a communication from Alice to Bob. If that communication is conducted with classical data, Eve can intercept it in transit without Alice's or Bob's knowledge. Interception implies making a copy of the information that is in transit: The original version is what Alice sends to Bob and is in Bob's possession, and the copy is what Eve has after the interception.

But if the communication is conducted with quantum data, the impossibility of copying quantum information means that if Eve attempts to intercept the message, her interaction will perturb the quantum state of it. As a result, Bob will be able to detect Eve's presence either by a failure to receive the information or by observing measurable errors or anomalies in the received data caused by the perturbation. If Bob receives the quantum information without any such disturbance, it indicates that no third party has accessed the message. In this case, Alice and Bob can use the received quantum information to securely establish a shared cryptographic key, which can then be used to protect subsequent communications between them. This is the process known as QKD.

Quantum communication is often regarded as a guarantor of perfect data security. For example, the European Telecommunications Standards Institute asserts that "QKD is secure now and always will be. By enabling provable security based on fundamental laws of quantum physics, QKD remains resilient even to future advances in cryptanalysis or in quantum computing."[21]

This claim is true as far as it goes, but it omits several important points:

- ○— QKD securely distributes only shared keys that can be used with existing symmetric encryption algorithms. The physical endpoints of the communication system must still be secured. QKD does not by itself solve related challenges such

as authentication, side-channel attacks, and man-in-the-middle attacks.[22]

- ○— Existing symmetric encryption algorithms using long keys already provide effectively unbreakable protection for data in transit, and Shor's algorithm provides no leverage in breaking symmetric algorithms. Other quantum algorithms provide modest (polynomial) assistance that is still entirely insufficient to break the encryption algorithms in any reasonable time frame.

- ○— As noted earlier, quantum communication in the form of QKD provides a hedge against a failure to develop public-key encryption algorithms resistant to being broken by quantum computers. But by and large, the cryptographic community has considerable confidence that the attempt to develop such algorithms will be successful.

- ○— QKD's security is effective only when two parties share an already-established trust relationship (e.g., through an initial face-to-face meeting in which they share a secret key so they can later verify their identities to each other). Using QKD, strangers without such a relationship will be able to communicate securely only by relying on trustworthy third parties to establish that initial trust relationship.

## Quantum Networking

The security benefits for quantum-enabled data security described above will require the ability to transmit and share quantum information at a range of distances: QKD between continents would require establishing links over very long distances. Building multi-node quantum supercomputers, on the other hand, may require networking over only tens of meters. Such distributed quantum computing can help to overcome individual quantum devices' hardware limitations. Quantum networking can also enhance quantum sensors through coordinated operation. (More details on this can be found in the Quantum Sensing section later in this chapter.)

Quantum networking entails many technical challenges, all focused on how to transfer quantum information between quantum computers or other quantum devices without loss. Because quantum information cannot be copied, it must be moved from point to point rather than replicated and then sent; this makes any losses during transmission extremely detrimental to quantum computers' operation.

One of these approaches depends on the computers involved being of the same design, thus eliminating the need to convert information from one form to another. This avoids the losses inherent in any such conversion. For example, to move information between quantum computers based on superconducting circuits, a networking design could require the qubits to remain in an ultra-low-temperature cryogenic environment. Such an environment would ensure that they maintain their quantum form and would minimize the risk of losses caused by noise, even very small vibrations or changes in temperature. This could be accomplished by housing the communicating computers within a single large cryogenic system or in a network of cryogenic environments connected by superconducting coaxial cables.

A second approach is transduction, which is the process of converting quantum information from one physical quantum system to another without losing its quantum properties.[23] Quantum transduction to optical photons (typically in fibers) is essential for networking quantum processors over long distances.[24]

It is also essential whenever quantum information must be transmitted through room-temperature, non-vacuum environments.

Typical examples of transduction include converting quantum information from states of an atom or superconducting qubit to states of a photon for transmission over an optical fiber network. In these cases, the quantum transducer converts quantum signals encoded as atomic spins or microwave photons into optical photons and vice versa while preserving their quantum state.

For long-distance quantum communication (many kilometers and above), quantum repeaters may be needed. A quantum signal traveling long distances degrades because information-carrying photons are eventually lost during transmission due to absorption by the glass comprising the optical fiber.

To deal with this loss, quantum repeaters—essentially small quantum computers dedicated to a single function—must first build up entanglement between adjacent nodes of the network. They then use that entanglement along with classical communication to generate longer and longer range entanglement. Preserving the qubits and their entanglement in quantum memory at each node (i.e., at each repeater) as the chain grows, this process continues until the entanglement spans the entire network. At that point, the network can be employed—again in conjunction with classical communication—to teleport quantum information without errors or loss across its full extent.

Quantum networking entails many technical challenges, all focused on how to transfer quantum information between quantum computers or other quantum devices without loss.

Such repeaters, which are the subject of intense research activity, would make it possible to move quantum information from one place to another without making a copy of the original quantum state (which would otherwise violate the no-cloning theorem) in the presence of loss.

## Key Developments

Some important technology developments in quantum communication in recent years include the following:

- **Interconnects**  Researchers in China have built low-loss superconducting interconnects that enable high-fidelity quantum information transfer between modular quantum processor units.[25] A quantum interconnect is a device or system that links different quantum components—such as quantum processors, sensors, or memories—so they can exchange and process quantum information coherently.

- **Repeaters**  A prototype quantum repeater that successfully distributes entanglement between two trapped-ion nodes separated by 50 kilometers (km) of optical fiber has been demonstrated.[26] This system integrates telecom-wavelength photon conversion to minimize transmission loss with quantum memories for storing entangled states and entanglement-swapping protocols, marking a critical advance toward scalable quantum networks.

- **Approaches to transduction**  Some of the leading approaches to transduction include the following:

  - **Atomic decay–based transduction**  This uses atoms or ions that absorb and emit light, helping transfer quantum information from one form (like microwave signals) to another (like optical light) without losing it.[27]

  - **Integrated microwave-to-optical transduction**  Tiny optical circuits on chips convert quantum signals between microwave and optical light.[28] These devices can use either optomechanical or electro-optical interactions as the base physical process (see below). Integrated transducers can achieve high-rate transduction with reduced heat production.[29]

  - **Optomechanical transduction**  Mechanical vibrations act as an intermediary between light and microwaves. These approaches have successfully demonstrated efficient bidirectional conversion[30] and microwave-optical entanglement.[31]

  - **Electro-optical transduction**  The electric fields of the microwave photons modify the optical properties of a material to affect the microwave-to-optical conversion.[32]

Despite significant progress, even the approaches that have succeeded in demonstrating microwave-optical entanglement currently do so at a quantum information transmission rate and fidelity significantly below what is needed to perform networked quantum computation. Importantly, current microwave-optical conversion rates are roughly six orders of magnitude smaller than the rate at which qubits in the same cryogenic environment can natively communicate with each other.

- **Transducer efficiency**  New architectures have been developed that significantly increase the efficiency and speed of atom-to-photon quantum transducers.[33] Based on arrays of optical cavities, which are structures formed by pairs of highly reflective mirrors that can confine photons, the new architecture enables simultaneous transduction from many atoms. This advance is a step in the direction of higher-rate transmission in quantum networks.

- **Operational tests**  Quantum-enabled data security affordances have been tested in operational scenarios by financial institutions such as HSBC,[34] JPMorgan Chase,[35] and Shinhan Bank in South Korea.[36] Other demonstrations have shown

that QKD can operate over hundreds of kilometers[37] and even in space via the use of satellites and ground stations.[38]

## Over the Horizon

Quantum communication is expensive and technologically difficult to put into place on a large scale. For it to be effective at such scale, it must solve problems less expensively than other approaches. As discussed in chapter 3, on cryptography and computer security, a variety of efforts are underway to deploy post-quantum encryption algorithms to resist quantum computing approaches to crack them. The security afforded by quantum communication will be valuable and important only if these efforts fail.

Even as the technology for quantum communication matures, classical networking will continue to handle most data traffic.[39] The vast majority of data in the world is classical, and classical networks are far more efficient and far faster for high-bandwidth communications. Quantum networks are inherently prone to loss and noise, limiting distance and speed, and their reliance on complex hardware like quantum repeaters restricts scalability. In short, quantum networks will at best complement, but not supersede, their classical counterparts in secure communication applications.

Nonetheless, it is expected that future networking between quantum data centers will enable joint, distributed quantum computations that surpass the capabilities of isolated quantum processors. This scaling approach is critical because of the physical and technical challenges in building large monolithic quantum computers. In this context, a "quantum internet" is likely to emerge.[40] This will likely involve localized quantum data centers performing the heavy lifting and more modest quantum devices securely querying them and communicating with one another. Networking between these quantum data centers will enable even larger calculations.

Finally, large-scale quantum networks may enable novel applications beyond secure communication and sensing. Speculatively, these include the following:

- **Quantum-assisted location verification and encryption** A protocol called quantum geo-encryption could allow data to be decrypted only at a specific geographic location or time, enhancing security against unauthorized or improper access.[41]

- **Entanglement-enhanced clock comparisons** Networks of optical clocks can surpass classical precision limits in frequency and time measurement, enabling applications in fundamental physics tests, navigation, and geodesy.[42]

- **Spoofing-proof timing synchronization** Using quantum entanglement properties for time synchronization could make timing systems much more resistant to spoofing or jamming attacks. This would improve the reliability of global navigation satellite systems, such as GPS, Russia's GLONASS, and the European Union's Galileo.[43]

# Quantum Sensing

## Essential Points

- Quantum sensing is the most mature of quantum technologies and is uniquely well suited for applications that involve small signals or that are delicate. These include astronomy (which requires capture of dim images), bioimaging (which requires that the light source not damage delicate specimens), and ultra-low-power platforms. Quantum sensing demonstrably excels in areas where classical probes are impractical, invasive, or inadequate, including gravitational-wave detection, precision timekeeping, and nanoscale field sensing.

- Quantum sensors increase their sensitivity by first suppressing classical sources of noise (e.g.,

technical or engineering noise). They then use quantum techniques for controlling quantum noise resulting from quantum effects such as the uncertainty principle. Quantum sensors do not eliminate all noise issues.

- True quantum advantage is not demonstrated by individual devices that show exceptional sensitivity only under idealized, highly controlled conditions. Rather it is demonstrated by a full system that outperforms a well-optimized classical baseline under equal resource constraints (size, weight, power, integration time). The system's sensitivity must reach and be maintained at the quantum noise limit in a robust, practically engineered package that doesn't require complex calibration and is rugged enough to use under changing environmental conditions.

- The advancement of practical quantum sensing is dominated by engineering challenges. These include the effective integration of system components, minimization of signal loss, and the development of compact, reliable photonic devices. Additionally, if sensors are networked, the challenges also include the establishment of precise timing and phase coordination, the reduction of losses in interconnections, and reliable synchronization across the network. Classical networking of quantum-enhanced nodes is likely to mature before fully entangled networks are fieldable.

- Networked and coordinated quantum sensing offer a number of benefits in principle, such as better ways to minimize the impact of noise and more accurate estimation of certain quantum wave properties important for sensing. However, realizing them in practice is a significant challenge separate from single-node engineering.

### *About Quantum Sensing*

Sensing gathers information about the world, from telling time to detecting faint signals, such as light or gravitational fields. Many sensor improvements over the years have been driven by advances in materials, electronics, and data processing. However, as sensors are made more sensitive, they eventually hit the limits of classical measurement precision. These limits can sometimes be overcome by devoting more energy or time to the sensing process. Quantum sensing exploits quantum mechanics to achieve greater sensitivity per photon, per atom, per second, or per joule of energy. It does this through techniques such as entanglement, squeezed states of light, and quantum feedback.

- **Entanglement** refers to linking particles so their states become correlated, enhancing measurement precision.

- **Squeezed light** refers to light prepared in a way that reduces the noise due to random photon arrival times, thereby improving sensitivity beyond what is possible with classical instruments.

- **Quantum feedback** involves controlling quantum systems in real time to correct errors and boost measurement accuracy.

Quantum sensors measure diverse phenomena including time, magnetic and electric fields, mass, and forces such as gravity. To achieve their advanced sensitivity, these devices must protect the fragile quantum properties of their probes from the external environment through to the final measurement.

- For sensors based on matter—such as neutral atoms, ions, or nitrogen-vacancy (NV) centers in diamonds—this typically means shielding them to extend their coherence time (i.e., the time over which their probes retain their quantum state information).

- For photonic sensors, the dominant challenge is different: Optical loss must be minimized as light travels and interacts with the sample because lost photons irrevocably degrade the quantum advantage of the sensor. Furthermore, the final measurement itself must be nearly perfect; this often

requires specialized hardware like high-quantum-efficiency photodetectors to ensure the delicate quantum information is read out without being destroyed.

Quantum sensing repurposes a fundamental challenge from quantum computing: While a quantum computer must be shielded from environmental noise, a sensor uses its quantum components as sensitive probes that intentionally interact with specific parts or properties of the environment to obtain information about it.

This distinction shows how the same quantum systems can be used differently by leveraging their unique properties for either computation or sensing. Similar observations apply for supporting technologies shared with quantum computing, such as lasers, photonics, and cryogenics. Overall, the field benefits from the fact that progress in one quantum area drives advances in others.

## Key Developments

The applications in which quantum sensors are used today include scientific instrumentation, navigation, energy prospecting, biological imaging, and defense, among others. To support these and other applications, a number of underlying quantum sensing technologies have been developed. These include technologies for sensing magnetic and gravitational fields, quantum networking for sensors, and technologies related to operational integration. We address each in turn.

### APPLICATION DOMAINS

**Scientific instrumentation**   An example is the Laser Interferometer Gravitational-Wave Observatory (LIGO), a large-scale physics experiment designed to detect gravitational waves produced by cosmic events such as black holes and neutron star collisions. LIGO uses laser interferometry enhanced by squeezed light to measure changes that are far smaller than the width of a proton in the 4 km length of

its arms,[44] which would not be possible with classical instruments. This quantum upgrade has nearly doubled the volume of the universe LIGO can observe. This means it can detect far more events, pushing the boundaries of our cosmic understanding.

**Navigation**   Quantum sensors can facilitate GPS-independent navigation in two ways. First, they can provide superior inertial navigation through more accurate measurements of acceleration, rotation, and reduced sensor drift.[45] (Sensor drift is the gradual and undesirable change in a sensor's output over time, even when the input being measured remains constant. This results in a discrepancy between the sensor's readings and the true physical value of what is being measured.)

Second, quantum sensors can also support navigation through map matching. This involves sensors measuring subtle variations in the local electric or magnetic field as a function of position and aligning those measurements with a previously constructed map of the area to pinpoint their location.[46] The accuracy of this method depends on the availability of detailed field maps. In one demonstration, a quantum magnetic-anomaly navigation system was tested on aircraft and ground vehicles, achieving positioning accuracies on par with, or exceeding, GPS in some scenarios. This includes one case where the position accuracy was better than twenty-two meters, outperforming traditional inertial navigation systems by up to forty-six-fold.[47]

**Energy and natural mineral prospecting**   In energy exploration,[48] quantum gravimeters can detect minute variations in Earth's gravitational field that provide information on the density and spatial structure of aquifers and hydrocarbon or minerals reserves. Quantum magnetometers can detect buried infrastructure, unexploded ordnance, and mineral deposits in real time, supporting safer and more efficient resource extraction.

**Defense and national security**   Quantum sensing promises to support a wide range of battlefield

applications, though none of those cited below have yet been matured fully into operational systems suitable for routine use. Navigation in GPS-denied environments is a critical need for mobile platforms and precision weapons, for which quantum accelerometers and gyroscopes are helpful (see figure 7.4). Quantum sensors for electromagnetic radiation detection and accurate timekeeping improve radar and electronic warfare systems by enhancing detection or improving resistance to jamming. Quantum-enhanced imaging methods can improve intelligence, surveillance, and reconnaissance capabilities, especially in low-visibility or degraded visual environments such as camouflage or dense foliage.

Quantum gravitometers may be able to assist in the more precise and certain locations of tunnels and underground bunkers.

**Biological imaging and sensing**   Quantum sensors enable high-resolution optical imaging at ultra-low-light levels, minimizing light damage to sensitive samples. This allows researchers to observe living cells and tissues in their native states and supports noninvasive, high-precision, low-light imaging for biomedical research.[49] Quantum techniques can also extend these benefits to electron microscopy, enabling minimally destructive, nanoscale imaging of fragile specimens.

**FIGURE 7.4**   A quantum accelerometer from Imperial College London uses ultracold atoms to make highly accurate measurements
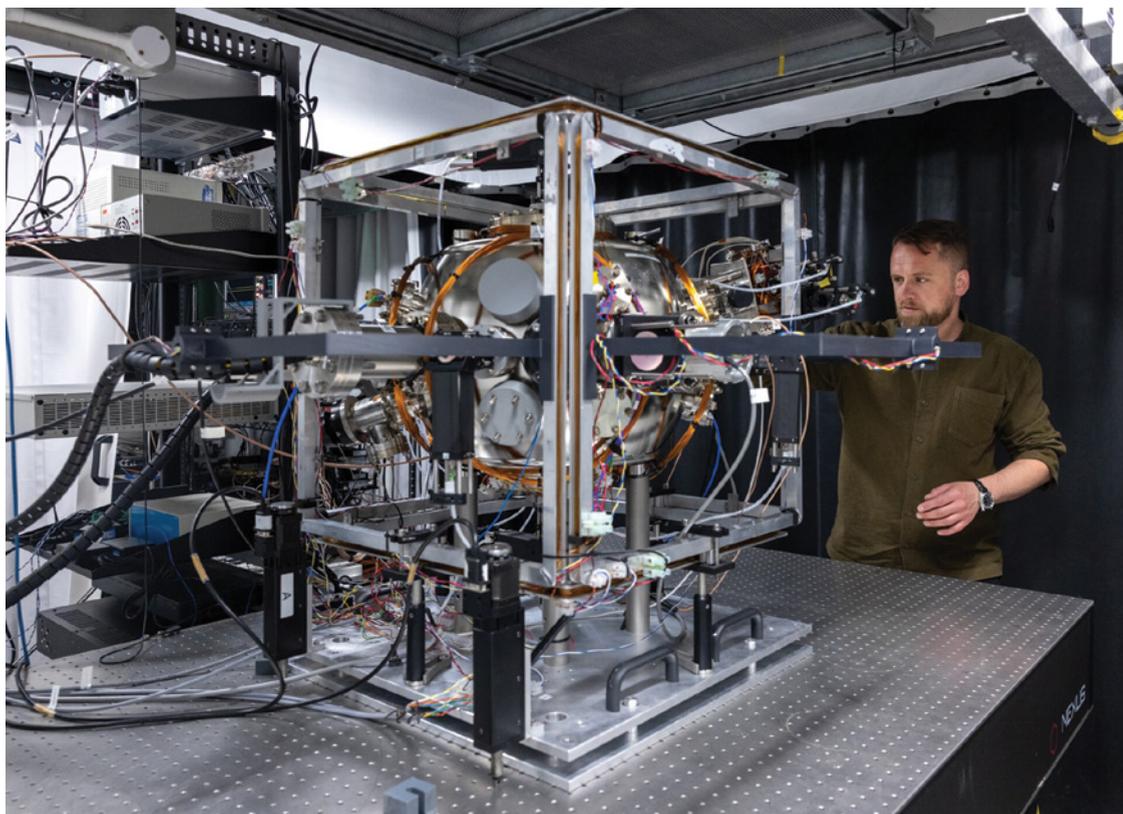


Source: Royal Navy

Quantum sensors can detect extremely small signals previously inaccessible to classical methods. For example, sensors based on NV centers in diamonds have measured microscopic magnetic and electric fields in single molecules and neurons and have also mapped heat production within cells.[50] Unlike traditional electrodes, quantum sensors probe living systems noninvasively, offering high spatial resolution and sensitivity. This enables precise study of brain function, neural communication, and neurological diseases.

A novel development is the use of an enhanced yellow fluorescent protein as a qubit.[51] This protein-based quantum sensor can be placed inside living systems to measure magnetic and electric fields, chemical changes, and protein interactions at the nanoscale. Because fluorescent proteins are naturally biocompatible, this approach allows quantum sensing within complex cellular environments. In essence, the biological qubit is like a temperature probe for the quantum age. However, instead of being sensitive to heat, it is sensitive to a suite of biologically relevant signals inside living systems.

## SENSOR DEVELOPMENTS

The following are a sampling of some important developments in quantum sensors:

**Cold-atom interferometers** These use clouds of atoms cooled to near absolute zero to measure acceleration, rotation, and gravity with extraordinary precision. For example, cold-atom inertial sensors based on light-pulse atom interferometry have achieved sensitivity and accuracy levels that compete with—and sometimes surpass—traditional inertial sensors. Laboratory experiments have demonstrated high-precision measurements of acceleration and rotation, with technique improvements such as interleaved atom interferometry enabling measurements of rotation rate with high resolution and accuracy.[52] Chinese researchers successfully demonstrated that a cold-atom gyroscope has lower drift compared to traditional fiber-optic gyroscopes.[53]

**NV center diamond sensors** These are particularly useful for sensing magnetic fields.[54] They take advantage of a nitrogen atom next to a vacant site in a diamond's crystal structure in ways that enable detection of magnetic fields at sensitivities and resolutions far better than classical magnetic sensors. These sensors are thus well suited for the detection of weak, localized, or rapidly varying magnetic fields in domains such as biomedical imaging, scientific instrumentation more broadly, materials science, navigation, and defense.

**Quantum radar** Classical radar detects objects by sending microwave signals to a target and measuring what is reflected back. Quantum radar does the same using pairs of entangled photons, more often at optical frequencies rather than at microwave ones.[55] On theoretical grounds, this approach potentially offers modestly higher sensitivity in very noisy environments by leveraging quantum correlations rather than raw signal power. However, the increased complexity of the transmitters and receivers, and the modest enhancements promised, means that, in practice, a true quantum advantage in radar will remain elusive until significant photonic hardware challenges are overcome.

**Networking for coordinated sensing** Though networking for coordinated sensing has not been deployed in the field, even on an experimental basis, there is every reason to believe that quantum communication can enhance quantum sensors through coordinating their operation. This would improve sensitivity and precision beyond classical sensor arrays or individual quantum sensors. Applications span fields such as navigation, timing, environmental monitoring, geophysics, and medical imaging. As one example of recent theoretical work, researchers have shown how networking quantum sensors together can enable the highly selective detection of electromagnetic waves.[56] These networks can be tuned to ignore unwanted waves from specific directions while remaining sensitive to the desired signal.

In the coming decade, quantum sensing is expected to significantly impact fields such as biology, medicine, navigation, and geoscience.

**Operational integration** Once the foundational science of a particular sensor is validated in the laboratory, its transition to field deployment introduces substantial engineering challenges. This is because performance that is robust under controlled lab conditions often declines under real-world stressors. Recognizing these issues, the Defense Advanced Research Projects Agency (DARPA) has initiated programs that tackle this operational challenge from different angles. Its Robust Quantum Sensors program, for example, focuses on system-level ruggedization. It aims to make entire complex sensor systems (like cold-atom interferometers) resilient enough to maintain high performance while mounted on moving military platforms.

A complementary, component-level approach is taken by DARPA's Intensity-Squeezed Photonic Integration for Revolutionary Detectors program.[57] This effort focuses on miniaturization and integration. It seeks to take the sophisticated squeezed-light technology used in massive experiments like LIGO and shrink it to a compact photonic chip.[58] When it happens in any given use case, the shift from large, stationary experimental setups to compact, rugged field sensors is a significant milestone, enabling systems that are valuable to military end users.

Although not funded by DARPA, one example of such work is the demonstration of the integration and miniaturization of accelerometers based on cold-atom interferometry. This is done by combining traditionally separate components into a compact unit suitable for field deployment on operational platforms. This innovation reduces the size and complexity from large optical-table systems to a rugged package roughly the size of a shoebox.[59]

### *Over the Horizon*

Especially exciting now is the development of new applications of quantum sensing technologies. These include portable brain scanners that use atomic magnetometers; quantum-enhanced microscopes that can look inside living cells without damaging them; and gravimeters that can detect underground cavities without digging.

In the coming decade, quantum sensing is expected to significantly impact fields such as biology, medicine, navigation, and geoscience. In the life sciences, emerging protein-based sensors may eventually enable measurements of signals inside living cells, opening new opportunities in neuroscience and bioanalytics. For example, quantum sensors may enable in-vivo imaging through enhanced microspectroscopy.[60] Theoretical work also suggests that entangled photon imaging could further improve the imaging of tissues and biological organisms, although this remains largely conceptual.[61]

In navigation and geoscience, quantum gravimeters, gyroscopes, and portable clocks could strengthen navigation where GPS is unavailable while improving climate monitoring and resource mapping. Progress in integrated quantum photonics is also anticipated to deliver substantial gains in power efficiency, bringing new sensing capabilities to power-constrained platforms.

At the same time, a new frontier lies in algorithmic sensing: Rather than treating sensors as passive data collectors, quantum algorithms could directly use quantum sensors to gather and process data. Early theoretical work points to the possibility of extracting extremely weak signals from noise or scanning large, uncertain parameter spaces far more efficiently than classical approaches. If realized, such algorithmic strategies would link quantum sensors and quantum computers in real-time feedback loops, expanding capabilities in areas from spectrum monitoring to distributed sensor networks.

Next-generation quantum sensors promise to extend the march toward lower drift, lower power consumption, and higher precision. Therefore, it seems reasonable to expect that these techniques, combined with large-scale classical data-fusion techniques, will continue to progress in such detection tasks. In short, we anticipate continued incremental gains in sensor capabilities as the result of continued progress in quantum sensing, rather than a large, discrete jump in overall performance.

## Policy Issues

### *The American Advantage*

America currently leads the world in many of the most advanced quantum computing technologies, including superconducting circuits, neutral atoms, and trapped ions. This leadership is the result of the following:

- A stable pipeline of experimentally demonstrated approaches, techniques, and materials emerging from basic research labs on university campuses

- A healthy ecosystem of start-ups and large companies exploring commercialization opportunities

- A forward-looking, entrepreneurial mindset that has been willing to support the pursuit of new opportunities before their payoff is clear

The United States doesn't necessarily lead in developing enabling technologies, such as electronics, optics, and cryogenics. Nor is it the fastest at commercializing or scaling up quantum devices; furthermore, its skilled and unskilled labor is relatively expensive. Nevertheless, the national quantum ecosystem that's been built since World War II to nurture and develop novel creative ideas and support their commercialization has given America a significant competitive advantage.

Other countries are now investing significant amounts of public capital into quantum technologies—in particular, China, which has made the domain one of the main technology priorities in its five-year plans.[62] To sustain America's advantage in quantum technologies, several areas of policy are important.

The national quantum ecosystem that's been built since World War II . . . has given America a significant competitive advantage.

### Support for Basic Science Research

In the past five years, both start-ups and tech giants have increasingly taken on the task of building large-scale, commercial quantum computing. Industrial efforts that focus on a wide variety of qubit technologies and their associated architectures now exist. These efforts typically focus on building toward the million-physical-qubit systems necessary for useful error-corrected computation. Thus, they emphasize the scaling of existing technologies, with relatively small tweaks to hardware and algorithms.

By contrast, academic efforts tend to focus on discovery of entirely new qubit platforms, improving qubit properties in existing platforms, creating new routes to scaling, and developing new quantum algorithms. Unlike many fields where academic efforts are disconnected from industrial realities, this high-risk basic academic science remains crucial to the continued progress of private-sector efforts. Ideas from academia are regularly adopted by both large companies and start-ups.

### The Quantum Workforce

On university campuses—where the basic science powering quantum innovations occurs—it is critically important to ensure access to doctoral students from abroad and particularly from China. There is an insufficient supply of adequately skilled US-trained undergraduates. Therefore, cutting the flow of international students actively hinders American competitiveness in quantum technology. In almost every university research laboratory, graduate students, as part of their training, provide much of the day-to-day labor necessary for advancing the state-of-the-art science.[63] Furthermore, after these international students have graduated, they disproportionately move into the quantum workforce in America; ensuring that this trend remains possible is essential to the current and future dynamism of America's quantum creativity engine.

### Supply Chain

Quantum hardware requires an increasingly diverse array of support technologies. On the materials side, this includes electro-optic and acousto-optic crystals, high purity aluminum, and rare earth metals. Among assembled technologies, it includes lasers, optical modulators, single photon detectors, and cryogenic refrigerators. Many of these technologies are produced abroad, typically at a cost many times lower than that of US manufacturers. In some cases, no US alternatives are available. Because quantum technology remains largely in a research and development phase, tariffs on these support technologies cannot be passed on to consumers, stifling the ability of quantum scientists and engineers to lead the way in developing them.

### Competition with China

There is currently an active competition between the United States and China in quantum technologies. China is leading in overall investment, at around $15 billion,[64] while the United States lags behind at around $8 billion ($4 billion of private investment plus $4 billion of public funding).[65]

As of August 2025, the largest controlled system of neutral atoms was produced in China,[66] as was the largest system of trapped ions.[67] Similarly, Chinese demonstrations of ground-to-satellite quantum networking via the Micius satellite and a 700-fiber ground-based communications network exceed (at least in terms of scale) anything yet attempted in the United States.[68] In all of these cases, the techniques have been pushed to their limits, leveraging impressive integration of technologies beyond the traditional quantum ecosystem. Regardless of whether these technologies ultimately prove commercially useful, efforts to develop them have unquestionably contributed to further growth of the Chinese talent base in quantum science and technology.

By contrast, the first demonstrations of quantum logic in neutral atom arrays, superconducting circuits, and ion traps all originated from the United States. Most new approaches and technologies continue to emerge from the US academic ecosystem. DARPA programs in quantum computing, networking, and

sensing sharpen and focus these efforts, and a broad ecosystem of basic science funded through the National Science Foundation, US Department of Energy, and US Department of Defense support this innovation engine. Examples of US government funding for basic research in quantum science and technology include the National Quantum Initiative, which was signed into law in early 2019,[69] and the Quantum Benchmarking Initiative, launched in 2024 by DARPA.[70]

Assuming that there is sustained support for basic research in quantum technologies, it seems likely that US innovation will continue to drive progress and that China will follow in ideas but lead in scaling. The gap, however, is closing, as China recruits more talent and grows its basic science portfolio.

## NOTES

1. "Nobel Prize in Physics 2025," NobelPrize.org, Nobel Prize Outreach 2025, October 20, 2025, https://www.nobelprize.org/prizes/physics/2025/summary/.

2. Zack Savitsky, "Debate Erupts Around Microsoft's Blockbuster Quantum Computing Claims," *Science* 387(6741): 1338–39, March 28, 2025, https://www.science.org/content/article/debate-erupts-around-microsoft-s-blockbuster-quantum-computing-claims.

3. David S. Wang, Austin G. Fowler, and Lloyd C. L. Hollenberg, "Surface Code Quantum Computing with Error Rates over 1%," *Physical Review A* 83, no. 2 (2011): 020302, https://doi.org/10.1103/PhysRevA.83.020302.

4. An analogy to classical computing would be that it is possible to build digital computers out of transistors and of vacuum tubes. For a variety of reasons (e.g., cost, energy consumption), transistor technology proved decisively superior as the fundamental hardware building block of classical computers.

5. Alkim Bozkurt, Han Zhao, Chaitali Joshi, Henry G. LeDuc, Peter K. Day, and Mohammad Mirhosseini, "A Quantum Electromechanical Interface for Long-Lived Phonons," *Nature Physics* 19, no. 9 (2023): 1326–32, https://doi.org/10.1038/s41567-023-02080-w.

6. Dolev Bluvstein, Simon J. Evered, Alexandra A. Geim, et al., "Logical Quantum Processor Based on Reconfigurable Atom Arrays," *Nature* 626 (2024): 58–65, https://doi.org/10.1038/s41586-023-06927-3.

7. Craig Gidney, "How to Factor 2048 Bit RSA Integers with Less than a Million Noisy Qubits," arXiv:2505.15917, version 1, preprint, arXiv, May 21, 2025, https://doi.org/10.48550/arXiv.2505.15917.

8. Michael E. Beverland, Prakash Murali, Matthias Troyer, et al., "Assessing Requirements to Scale to Practical Quantum Advantage," arXiv:2211.07629, preprint, arXiv, November 14, 2022, https://doi.org/10.48550/arXiv.2211.07629.

9. Matt Swayne, "Quantum Computing Roadmaps and Predictions of Leading Players," *The Quantum Insider*, May 16, 2025, https://thequantuminsider.com/2025/05/16/quantum-computing-roadmaps-a-look-at-the-maps-and-predictions-of-major-quantum-players/.

10. Hari P. Paudel, Madhava Syamlal, Scott E. Crawford, et al., "Quantum Computing and Simulations for Energy Applications: Review and Perspective," *ACS Engineering Au* 2, no. 3 (2022): 151–96, https://doi.org/10.1021/acsengineeringau.1c00033.

11. Mauro D'Arcangelo et al., "Leveraging Analog Quantum Computing with Neutral Atoms for Solvent Configuration Prediction in Drug Discovery," *Physical Review Research* 6, no. 4 (2024), https://doi.org/10.1103/PhysRevResearch.6.043020.

12. Ehud Altman et al., "Quantum Simulators: Architectures and Opportunities," *PRX Quantum* 2, no. 1 (2021): 017003; A. J. Daley, I. Bloch, C. Kokail, et al., "Practical Quantum Advantage in Quantum Simulation," *Nature* 607 (2022): 667–76.

13. Craig Gidney, "How to Factor 2048 Bit RSA Integers with Less than a Million Noisy Qubits." arXiv:2505.15917, version 1, preprint, arXiv, May 21, 2025, https://doi.org/10.48550/arXiv.2505.15917. The five-to-fifteen-year time frame comes from "DARPA Eyes Companies Targeting Industrially Useful Quantum Computers," DARPA, April 3, 2025, https://www.darpa.mil/news/2025/companies-targeting-quantum-computers.

14. Oskar Leimkuhler and K. Birgitta Whaley, "Exponential Quantum Speedups in Quantum Chemistry with Linear Depth," arXiv:2503.21041, preprint, arXiv, May 16, 2025, https://doi.org/10.48550/arXiv.2503.21041.

15. Benedikt Fauseweh, "Quantum Many-Body Simulations on Digital Quantum Computers: State-of-the-Art and Future Challenges," *Nature Communications* 15, no. 1 (2024): 2123, https://doi.org/10.1038/s41467-024-46402-9.

16. Hsin-Yuan Huang et al., "Power of Data in Quantum Machine Learning," *Nature Communications* 12, no. 1 (2021): 2631.

17. In general, a polynomial speedup is useful for turning a problem that is already doable in a plausible amount of time into one that is doable in a meaningfully shorter amount of time. Instead of a billion years turning into a few minutes, polynomial speedups turn days or weeks of computation into minutes and can be fairly regarded as highly useful but not transformational.

18. See, for example, Seunghoon Lee, Joonho Lee, Huanchen Zhai, et al., "Evaluating the Evidence for Exponential Quantum Advantage in Ground-State Quantum Chemistry," *Nature Communications* 14, no. 1 (2023): 1952, https://doi.org/10.1038/s41467-023-37587-6.

19. Yulin Wu et al., "Strong Quantum Computational Advantage Using a Superconducting Quantum Processor," *Physical Review Letters* 127, no. 18 (2021), https://doi.org/10.1103/PhysRevLett.127.180501.

20. William K. Wootters and Wojciech H. Zurek, "A Single Quantum Cannot Be Cloned," *Nature* 299 (1982): 802–3.

21. "Quantum Safe Cryptography and Security," ETSI White Paper #8, European Telecommunications Standards Institute, June 2015, https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

22. Sunil K. Singh, Sudhakar Kumar, Anureet Chhabra, et al., "Advancements in Secure Quantum Communication and Robust Key Distribution Techniques for Cybersecurity Applications," *Cyber Security and Applications* 3 (December 2025): 100089, https://doi.org/10.1016/j.csa.2025.100089.

23. David Awschalom et al., "Development of Quantum Interconnects (Quics) for Next-Generation Information Technologies," *Prx Quantum* 2 (2021): 017002.

24. Marcello Caleffi, Laura d'Avossa, Xu Han, and Angela Sara Cacciapuoti, "Quantum Transduction: Enabling Quantum Networking," arXiv:2505.02057, preprint, arXiv, May 4, 2025, https://doi.org/10.48550/arXiv.2505.02057.

25. Simon Storz, Josua Schär, Anatoly Kulikov, et al., "Loophole-Free Bell Inequality Violation with Superconducting Circuits," *Nature* 617, no. 7960 (2023): 265–70, https://doi.org/10.1038/s41586-023-05885-0.

26. V. Krutyanskiy, M. Canteri, M. Meraner, et al., "Telecom-Wavelength Quantum Repeater Node Based on a Trapped-Ion Processor," *Physical Review Letters* 130, no. 21 (2023): 213601, https://doi.org/10.1103/PhysRevLett.130.213601.

27. Aishwarya Kumar, Aziza Suleymanzade, Mark Stone, et al., "Quantum-Enabled Millimetre Wave to Optical Transduction Using Neutral Atoms," *Nature* 615, no. 7953 (2023): 614–19, https://doi.org/10.1038/s41586-023-05740-2.

28. Nikolai Lauk, Neil Sinclair, Shabir Barzanjeh, et al., "Perspectives on Quantum Transduction," *Quantum Science and Technology* 5, no. 2 (2020): 020501, https://doi.org/10.1088/2058-9565/ab788a.

29. Galan Moody, Volker J. Sorger, Daniel J Blumenthal, et al., "2022 Roadmap on Integrated Quantum Photonics," *Journal of Physics: Photonics* 4, no. 1 (2022): 012501, https://doi.org/10.1088/2515-7647/ac1ef4.

30. R. W. Andrews, R. W. Peterson, T. P. Purdy, et al., "Bidirectional and Efficient Conversion Between Microwave and Optical Light," *Nature Physics* 10, no. 4 (2014): 321–26, https://doi.org/10.1038/nphys2911.

31. Srujan Meesala, David Lake, Steven Wood, et al., "Quantum Entanglement Between Optical and Microwave Photonic Qubits," *Physical Review X* 14, no. 3 (2024), https://doi.org/10.1103/PhysRevX.14.031055.

32. Charles Möhl, Annina Riedhauser, Max Glantschnig, et al., "Bidirectional Microwave-Optical Conversion with an Integrated Soft-Ferroelectric Barium Titanate Transducer," preprint, January 26, 2025, https://doi.org/10.1103/1gvf-w6lx.

33. For theoretical work on the superiority of cavity arrays to lenses, see Josiah Sinclair, Joshua Ramette, Brandon Grinkemeyer, Dolev Bluvstein, Mikhail Lukin, and Vladan Vuletić, "Fault-Tolerant Optical Interconnects for Neutral-Atom Arrays," arXiv:2408.08955, preprint, arXiv, August 16, 2024, https://doi.org/10.48550/arXiv.2408.08955. For experimental work implementing cavity arrays, see Adam L. Shaw, Anna Soper, Danial Shadmany, et al., "A Cavity Array Microscope for Parallel Single-Atom Interfacing," arXiv:2506.10919, preprint, arXiv, June 12, 2025, https://doi.org/10.48550/arXiv.2506.10919.

34. "HSBC Pioneers Quantum Protection for AI-Powered FX Trading," news release, HSBC, December 23, 2023, https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-pioneers-quantum-protection-for-ai-powered-fx-trading.

35. "JPMorgan Chase to Implement a Quantum-Secured Network," *Quantum Herald*, n.d., accessed September 27, 2025, https://www.quantumsecuritydefence.com/news/jpmorgan-chase-to-implement-a-quantum-secured-network.

36. "Toshiba Digital Solutions and KT Demonstrate Hybrid Quantum Secure Communications with South Korea's Shinhan Bank," Toshiba.com, April 19, 2024, https://www.global.toshiba/ww/news/digitalsolution/2024/04/news-20240419-01.html.

37. Shi-Chang Zhuang, Bo Li, Ming-Yang Zheng, et al., "Ultrabright-Entanglement-Based Quantum Key Distribution over a 404-Km-Long Optical," arXiv:2408.04361, version 1, preprint, arXiv, August 8, 2024, https://doi.org/10.48550/arXiv.2408.04361.

38. Juan Yin, Yu-Huai Li, Sheng-Kai Liao, et al., "Entanglement-Based Secure Quantum Cryptography over 1,120 Kilometres," *Nature* 582, no. 7813 (2020): 501–5, https://doi.org/10.1038/s41586-020-2401-y.

39. Joseph M. Lukens, Nicholas A. Peters, and Bing Qi, "Hybrid Classical-Quantum Communication Networks," arXiv:2502.07298, preprint, arXiv, July 24, 2025, https://doi.org/10.48550/arXiv.2502.07298.

40. H. Jeff Kimble, "The Quantum Internet," *Nature* 453.7198 (2008): 1023–30.

41. Robert Malaney, "Quantum Geo-Encryption," 2016 IEEE Global Communications Conference (IEEE Press, 2016), 1–6, https://doi.org/10.1109/GLOCOM.2016.7842191.

42. "An Elementary Network of Entangled Optical Atomic Clocks?," University of Oregon, June 2, 2023, https://omq.uoregon.edu/events/elementary-network-entangled-optical-atomic-clocks.

43. Abyad Enan, Mashrur Chowdhury, Sagar Dasgupta, and Mizanur Rahman, "Quantum-Classical Hybrid Framework for Zero-Day Time-Push GNSS Spoofing Detection," arXiv:2508.18085, preprint, arXiv, August 25, 2025, https://doi.org/10.48550/arXiv.2508.18085.

44. M. Tse et al., "Quantum-Enhanced Advanced LIGO Detectors in the Era of Gravitational-Wave Astronomy," *Physical Review Letters* 123, no. 23 (2019), https://doi.org/10.1103/PhysRevLett.123.231107.

45. Mary Burkey, *How Quantum Sensing Will Solve GPS Denial in Warfare*, Lawrence Livermore National Laboratory Center for Global Security Research Fellows Publication, June 2025, https://cgsr.llnl.gov/sites/cgsr/files/2025-06/Burkey_QS_final.pdf.

46. Samuel Lellouch and Michael Holynski, "Integration of a High-Fidelity Model of Quantum Sensors with a Map-Matching Filter for Quantum-Enhanced Navigation," *Quantum Science and Technology* 10, no. 4 (2025): 045007, https://doi.org/10.1088/2058-9565/adf2d9.

47. Murat Muradoglu, Mattias T. Johnsson, Nathanial M. Wilson et al., "Quantum-Assured Magnetic Navigation Achieves Positioning Accuracy Better than a Strategic-Grade INS in Airborne and Ground-Based Field Trials," arXiv:2504.08167, preprint, arXiv, April 10, 2025, https://doi.org/10.48550/arXiv.2504.08167.

48. Scott E. Crawford, Roman A. Shugayev, Hari P. Paudel, et al., "Quantum Sensing for Energy Applications: Review and Perspective," *Advanced Quantum Technologies* 4, no. 8 (2021), https://doi.org/10.1002/qute.202100049.

49. Hoda Lotfipour, Hassan Sobhani, Mohamad Taghi Dejpasand, and Morteza Sasani Ghamsari, "Application of Quantum Imaging in Biology," *Biomedical Optics Express* 16, no. 8 (2025): 3349–77, https://doi.org/10.1364/BOE.566801.

50. Nikolaj Hansen et al., "Microscopic-Scale Magnetic Recording of Brain Neuronal Electrical Activity Using a Diamond Quantum Sensor," *Sci. Rep* 13, no. 1 (2023); Nabeel Aslam et al., "Quantum Sensors for Biomedical Applications," *Nature Review Physics* 5, no. 3 (2023).

51. Jacob S. Feder, Benjamin S. Soloway, Shreya Verma, et al., "A Fluorescent-Protein Spin Qubit," *Nature* 645, no. 8079 (2025): 73–9, https://doi.org/10.1038/s41586-025-09417-w.

52. Remi Geiger, Arnaud Landragin, Sébastien Merlet, and Franck Pereira Dos Santos, "High-Accuracy Inertial Measurements with Cold-Atom Sensors," *AVS Quantum Science* 2, no. 2 (2020): 024702, https://doi.org/10.1116/5.0009093.

53. Jinting Li, Xi Chen, Danfang Zhang, et al., "Realization of a Cold Atom Gyroscope in Space," *National Science Review* 12, no. 4 (2025): nwaf012, https://doi.org/10.1093/nsr/nwaf012.

54. Ning Wang and Jianming Cai, "Hybrid Quantum Sensing in Diamond," *Frontiers in Physics* 12 (February 2024), https://doi.org/10.3389/fphy.2024.1320108.

55. Athena Karsa, Alasdair Fletcher, Gaetana Spedalieri, and Stefano Pirandola, "Quantum Illumination and Quantum Radar: A Brief Overview," *Reports on Progress in Physics* 87, no. 9 (2024): 094001, https://doi.org/10.1088/1361-6633/ad6279.

56. Arne Hamann, Paul Aigner, Pavel Sekatski, and Wolfgang Dür, "Selective and Noise-Resilient Wave Estimation with Quantum Sensor Networks," *Quantum Science and Technology* 10, no. 3 (2025): 035028, https://doi.org/10.1088/2058-9565/add61b.

57. US Defense Advanced Research Projects Agency, "Intensity-Squeezed Photonic Integration for Revolutionary Detectors (INSPIRED)," accessed October 20, 2025, https://www.darpa.mil/research/programs/intensity-squeezed-photonic.

58. Jon Harper, "DARPA Eyeing New Quantum Sensing Program," *DefenseScoop*, December 30, 2024, https://defensescoop.com/2024/12/30/darpa-eyeing-new-quantum-sensing-program-robust-quantum-sensors-roqs/.

59. Jongmin Lee, Roger Ding, Justin Christensen, et al., "A Compact Cold-Atom Interferometer with a High Data-Rate Grating Magneto-Optical Trap and a Photonic-Integrated-Circuit-Compatible Laser System," *Nature Communications* 13, no. 1 (2022): 5131, https://doi.org/10.1038/s41467-022-31410-4.

60. Tian Li, Vsevolod Chevurkanov, Vladislav Yakovlev, "Harnessing Quantum Light for Microscopic Biomechanical Imaging of Cells and Tissues," *PNAS* 121, no. 45 (2024).

61. Yide Zhang, Zhe He, Xin Tong, David Garrett, et. al., "Quantum Imaging of Biological Organisms Through Spatial and Polarization Entanglement," *Science Advances* 10, no. 10 (2024).

62. State Council, People's Republic of China, "China to Include Quantum Technology in Its 14th Five-Year Plan," CGTN News Service, October 22, 2020, https://english.www.gov.cn/news/videos/202010/22/content_WS5f90e700c6d0f7257693e3fe.html.

63. National Science Board, "Science & Engineering Indicators: Human Resources and Academic R&D" (NSB2023-26), accessed October 20, 2025, https://ncses.nsf.gov/pubs/nsb202326/human-resources-and-academic-r-d.

64. Brad Smith, "Investing in American Leadership in Quantum Technology," *Microsoft on the Issues*, April 28, 2025, https://blogs.microsoft.com/on-the-issues/2025/04/28/investing-in-american-leadership-quantum/.

65. "Special Gaps Analysis-Quantum," Special Competitive Studies Project, 2025, https://www.scsp.ai/reports/2025-gaps-analysis/gaps-analysis/quantum/.

66. Lin Rui et al., "AI-Enabled Parallel Assembly of Thousands of Defect-Free Neutral Atom Arrays," *Physical Review Letters* 135, no. 6 (2025): 060602.

67. Guo S-A. et al., "A Site-Resolved Two-Dimensional Quantum Simulator with Hundreds of Trapped Ions," *Nature* 630, no. 8017 (2024): 613–18.

68. Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, et al., "An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres," *Nature* 589, no. 7841 (2021): 214–19, https://doi.org/10.1038/s41586-020-03093-8.

69. Martin Giles, "President Trump Has Signed a $1.2 Billion Law to Boost US Quantum Tech," *MIT Technology Review*, December 22, 2018, https://www.technologyreview.com/2018/12/22/138149/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/.

70. US Defense Advanced Research Projects Agency, "Quantum Benchmarking Initiative (QBI)," accessed October 20, 2025, https://www.darpa.mil/research/programs/quantum-benchmarking-initiative.

## STANFORD EXPERT CONTRIBUTORS

**Dr. Jon Simon**
SETR Faculty Council, Joan Reinhart Professor of Physics, and Professor of Applied Physics

**Dr. Amir Safavi Naeini**
Associate Professor of Applied Physics and, by courtesy, of Electrical Engineering

**Dr. David Schuster**
Professor of Applied Physics

**Ms. Junna Gui**
SETR Fellow and Q-Farm Program Manager