Leaders' Guide to Quantum Computing

10 April 2025 - ID G00817816 - 27 min read

By: Mark Horvath, Chirag Dekate, Matthew Brisse

Initiatives:Security of Applications and Data

Quantum computing is playing an increasingly visible role in research and development and in cybersecurity, but there are uncertainties about its function, capabilities and evolution. IT leaders can use this research to establish how and when to respond to and utilize this technology.

Overview

Key Findings

- Quantum computers are not high-performance computers that can faster run problems solved by Turing complete systems, but are a specialty computing platform that does some specific kinds of computing that classical systems are not capable of addressing. Typically, the current generation of quantum computers work on various kinds of optimization and physical science R&D problems.

- Unlike existing classical computers, quantum computers can be made out of a fairly wide variety of physics; each quantum computer platform has its own strengths, weaknesses and timelines. All quantum computers at this point are custom-made one-off platforms, with no common ground among them except for some language support.

- One of the concerns about the rise of quantum computers is their ability to enable key breaking for the asymmetric cryptography in use today. This is prompting the need for postquantum cryptography (PQC), or cryptography that a quantum computer cannot break, as a replacement. Quantum computers are not necessary for using PQC

- Similar to the early days of AI, there are not many specialists in quantum computing programming compared with classical programmers, but demand is rising as claims of quantum advantages increase.

Recommendations

IT leaders looking to effectively respond to and utilize the quantum computing technology should:

- Evaluate whether a quantum computer can potentially offer an advantage in priority use cases over a combination of best of latest classical technologies and leading algorithmic and heuristic techniques before investing in any quantum computing solution.
- Favor quantum computing as a service (QCaaS). Because of the wide variety of physical systems, upkeep and maintenance of quantum computers are unlike those of most traditional computers.
- Prepare your overall security posture for quantum computing by moving encrypted systems and data to industry-approved PQC in a way to protect your valuable data assets. Set a deadline and make sure you will complete this work by 2030.
- Form a small team to identify, evaluate and manage threats and opportunities presented by quantum computing.

Introduction

An integral part of the job of any IT leader is dealing with new and emerging technologies, and evaluating the risks and advantages they bring. In other words, IT leaders must ensure software is running smoothly on traditional computers either on-premises, in the cloud or with legacy systems. Quantum computers, however, are something completely different. It's a mistake to think of them as just faster, higher-performance systems similar to those already existing in a typical portfolio.

The following is a quick list of points that you should keep in mind when talking with quantum-computer-eager teams and evaluating the kinds of tasks for which they can show advantage:

- **You, as an IT leader, don't need to understand the detailed physics of quantum computers.** While a physics background can be very helpful, especially for understanding some of the early concepts and some of the product offerings, it's not the most important thing. As we will see, a quantum computer spans eight different physics systems. Though it's possible to build a working quantum computer based on any of these very different physics, the results are what matters, especially in the long run. While it's helpful to know what a qubit is and how it works, you can engage with quantum computers at a systematic level without a detailed understanding of quantum physics.

- **You do not need a quantum computer to run PQC.** One common myth about PQC is that you need a quantum computer to run it. Fortunately, that's not true. PQC was designed to run on something with relatively minimal computing resources, even a mobile phone, that is, a classical computing system. While you would need a quantum computer to break traditional encryption, you don't need one to use PQC and enhance your encryption today. Similarly, quantum key distribution (QKD) and quantum random number generators (QRNGs), while offering some advantages in security, are not quantum computing technologies.

- **Business advantages are still rare and limited.** The quantum advantage, the ability of a quantum computer to outperform a classical system, is still the exception rather than the rule, and is only available for limited classes of problems. Most problems typically encountered by a chief information security officer (CISO) would not benefit from quantum computers.

- **Access to a quantum computer is always managed through a classical computer.** Quantum computers are not able to handle all the networking, security, translation, staging and OS tasks common to classical computers. They are so different that they are almost never programmed directly. Lacking all these subsystems, their security and programming interfaces are handled through a classical system that does the staging, communication and security tasks. These have all the normal security issues that every classical system has and will also need conventional security protection.

The above are the four most common misunderstandings Gartner sees about quantum computing practices. While it is important to point them out upfront, this does not mean quantum computers do not offer advantages when used in a proper context and with proper expectations set for both teams and management.

Analysis

Evaluate Whether a Quantum Computer Can Offer an Advantage in Priority Use Cases

Focus: CIOs, IT R&D leaders

It’s popular to think of quantum computing as a kind of supercomputer or high-performance computing (HPC) technology, but that’s not really an accurate view. It’s more akin to a math co-processor that supports a classical computer or existing HPC system.

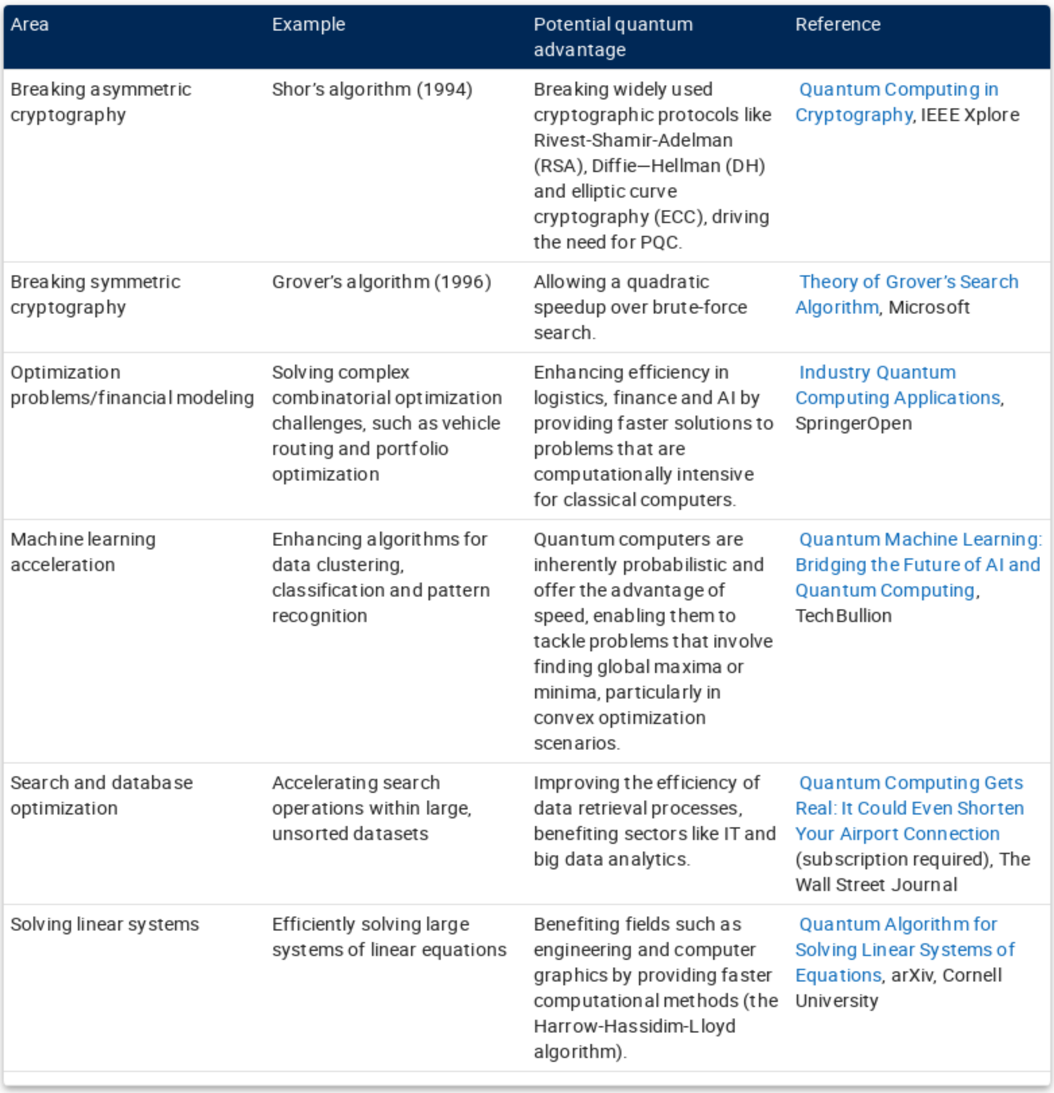
It’s also important to keep in mind that while classical computers are deterministic, quantum computers are probabilistic in nature. For example, if I ask my calculator, “What is 2 plus 2?” it will say “4” (unless it’s broken). If I ask a quantum computer, it will give a range of answers between 0 and 10 with 4 being the most probable answer. Probability scores are built up by running the program many times; the more times you run it, the more accurate the score. Quantum computers are not designed for spreadsheets or other typical office uses, but highly useful for finding “optimal” answers to certain kinds of unconstrained or optimization problems.

For these reasons, quantum computers will not soon replace existing classical systems. Their advantages over classical computers (quantum advantages) only exist for a narrow range of specialty applications. In the current market, quantum computers are primarily applied to optimization challenges prevalent in logistics, financial services and a few other related domains. There are also hard science use cases, mostly in chemistry and statistical analysis, and a very limited use in optimizing small parts of AI models.

Table 1 lists the common areas where quantum computing can potentially be used for business or security advantages.

Table 1: Areas Where Potential Quantum Advantages Can Be Realized

(Enlarged table in Appendix)



Area	Example	Potential quantum advantage	Reference
Breaking asymmetric cryptography	Shor’s algorithm (1994)	Breaking widely used cryptographic protocols like Rivest-Shamir-Adelman (RSA), Diffie—Hellman (DH) and elliptic curve cryptography (ECC), driving the need for PQC.	Quantum Computing in Cryptography, IEEE Xplore
Breaking symmetric cryptography	Grover’s algorithm (1996)	Allowing a quadratic speedup over brute-force search.	Theory of Grover’s Search Algorithm, Microsoft
Optimization problems/financial modeling	Solving complex combinatorial optimization challenges, such as vehicle routing and portfolio optimization	Enhancing efficiency in logistics, finance and AI by providing faster solutions to problems that are computationally intensive for classical computers.	Industry Quantum Computing Applications, SpringerOpen
Machine learning acceleration	Enhancing algorithms for data clustering, classification and pattern recognition	Quantum computers are inherently probabilistic and offer the advantage of speed, enabling them to tackle problems that involve finding global maxima or minima, particularly in convex optimization scenarios.	Quantum Machine Learning: Bridging the Future of AI and Quantum Computing, TechBullion
Search and database optimization	Accelerating search operations within large, unsorted datasets	Improving the efficiency of data retrieval processes, benefiting sectors like IT and big data analytics.	Quantum Computing Gets Real: It Could Even Shorten Your Airport Connection (subscription required), The Wall Street Journal
Solving linear systems	Efficiently solving large systems of linear equations	Benefiting fields such as engineering and computer graphics by providing faster computational methods (the Harrow-Hassidim-Lloyd algorithm).	Quantum Algorithm for Solving Linear Systems of Equations, arXiv, Cornell University

Source: Gartner (April 2025)

Recommendations

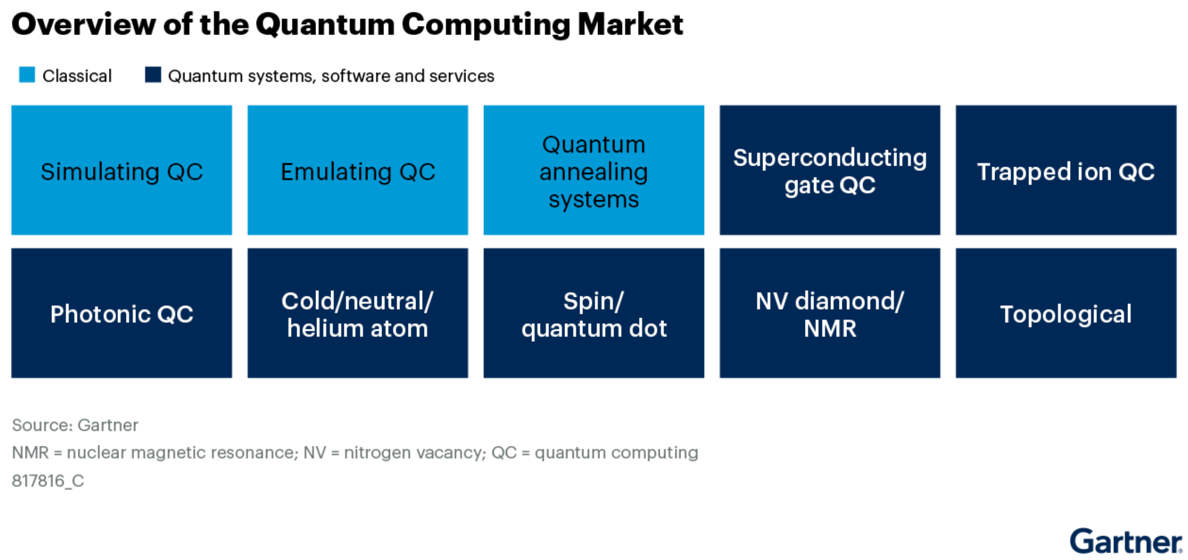
Evaluate the types of problems your organization’s business units are looking to solve before looking at quantum computers. With few exceptions, classical systems are usually a better answer.

Favor Quantum Computing as a Service

Focus: CIOs, IT R&D leaders

Classical computing platforms are predominantly built using silicon-based semiconductor technology and have a set of well-established chip architectures. Quantum computers differ from them significantly in terms of physics, computational power, support and the ability to solve problems. Figure 1 offers an overview of the types of quantum computers in the market, as of the fourth quarter of 2024.

Figure 1: Overview of the Quantum Computing Market



Overview of the Quantum Computing Market

🟦 Classical ■ Quantum systems, software and services

Simulating QC	Emulating QC	Quantum annealing systems	Superconducting gate QC	Trapped ion QC
Photonic QC	Cold/neutral/ helium atom	Spin/ quantum dot	NV diamond/ NMR	Topological

Source: Gartner

NMR = nuclear magnetic resonance; NV = nitrogen vacancy; QC = quantum computing

817816_C

Quantum Computing Landscape

How to choose a quantum computing system for a certain type of problem is beyond the scope of this research. However, it is worthwhile to note the following trends:

- Many quantum computing systems, across multiple physics platforms, are available as a service.
- All of the hyperscalars have quantum computing as a service (QCaaS) offerings, as well as extensive training in common quantum programming languages like Qiskit (IBM), Cirq (Google), Q# (Microsoft), pyQuil (Rigetti) and Strawberry Fields (Xanadu). Most of these languages enjoy support across many platforms, even from those they, themselves, did not sponsor.
- There is a significant diversity of base physics for quantum computing platforms. Trapped ions, for example, use multiple, identical atoms, pinned down by lasers to do computations, while superconducting qubits don't use atoms at all, but microscopic electrical circuits that exhibit quantum properties in a variety of different superconductors.

The choices of a platform, a vendor and a language are all free parameters. However, different vendors will have different subspecialities and areas of focus.

Because of the diversity of platforms, it's more important to match the problem you have to a quantum computing platform that can address it natively.

> **The problem should determine your choice of quantum computing platform, not the other way around.**

There are no agreed-upon figures of merit for quantum computers; each has its own trade-offs. See the table of glossary terms used in evaluating quantum computers and Note 1 for a high-level overview of quantum computers and some of their characteristics.

Common to nearly all platforms is the need for error correction. Because of factors like the environment, noise, coherence times and the layout of particular circuits, extra qubits are often necessary to correct errors at the gate level. In effect, this means that the number of logical qubits, that is, the qubits that are needed to form the gates that will run your programs, is often much smaller than the number of physical qubits on the machine, because many of the physical qubits are being used to correct errors. This has the net effect of limiting the number of logical gates that can be run at once. Improving the number of available logical qubits is the challenge for this generation of quantum computers. See Quantum Error Correction for Dummies for an overview of this problem.

For these reasons, Gartner recommends favoring QCaaS.

Recommendations

Because there are so many different systems, each with their own advantages and disadvantages, and because the field is advancing nonlinearly, Gartner recommends avoiding the purchase of a quantum computer for on-premises use. Some quantum computers require very special care and upkeep, which can be expensive, especially if there isn't a quantifiable advantage. And often these systems are replaced with newer models in fairly short periods of time. Instead, favor QCaaS to avoid vendor lock-in, and ask your teams to code in one of the quantum computing languages that can be ported between vendors.

Prepare Your Security Posture for Quantum Computing

Focus: CIOs, CISOs, data protection officers (DPOs)

Get Prepared for PQC by 2030

For a full analysis of PQC, the market and recommended actions, see Postquantum Cryptography: The Time to Prepare Is Now! In brief, Gartner notes:

- Quantum computers pose an existential threat to most current cryptographic methods.
- Asymmetric cryptography is under the most pressure, and Gartner predicts that the RSA and ECC algorithms will be unsafe to use by 2030. Please note that they probably won't be completely broken, but will be well on the way to full breakage by then, similar to the way that Secure Hash Algorithm 1 (SHA-1) became unsafe and was broken.
- The U.S. National Institute of Standards and Technology (NIST) announced the first of the new quantum-resistant (aka PQC) algorithms based on ring learning with errors (RLWE) in August 2024. [1] Another, independent set, HQC, based on structured codes is due in early 2027. [2] The new algorithms are based on entirely different math and will complete the initial goal of having two mathematically independent systems, similar to the independence of RSA and ECC.
- RSA, ECC and their associated signature algorithms will need to be replaced before they are broken. Gartner observes that:
  - Adoption of those alternative algorithms has already begun in some products.
  - Hybrid certificates with both classical and PQC signatures are currently being used to test systems.
- Symmetric algorithms are under substantially less pressure because the current algorithm to break them, that is, Grover's algorithm, is much less efficient, so doubling symmetric key sizes should be sufficient in protection for the near future. Grover's algorithm is very difficult to implement and requires an unrealistic number of qubits at the present time.
- Standards like Transport Layer Security (TLS), Public Key Cryptography Standard (PKCS) and other public-key infrastructure (PKI) will need to be upgraded, which could mean patching, equipment upgrades or system replacement depending on the affected system and its current security posture.

Cybersecurity Threat Actors and Quantum

While Gartner doesn't track threat actors in specific ways, it's very clear that state actors (SAs) will have access to large-scale quantum computing before anyone else. This poses a couple of threats and, potentially, will involve other actors.

Gartner does not believe that SAs currently have cryptographically relevant quantum computers (CRQCs) as of the time of the publication of this research, based on the state of quantum physics as reflected by published research in peer-reviewed journals. While states will undoubtedly be ahead of commercial providers, the overall level of the market does not yet support anything near the level of logical qubits that would be needed to execute Shor's or Grover's algorithm by a few orders of magnitude. You should also consider one high likelihood that other quantum algorithms for breaking keys could have been developed, using fewer logical qubits than known algorithms. Given that these algorithms could be developed without a review or input from the wider community, it seems likely that they constitute a more relevant attack vector than a large-scale machine exploiting existing or new physics.

> The most likely attack is the "harvest now, decrypt later" attack where data is exfiltrated through various means like the advanced persistent threat, and stored until it can be decrypted and read.

Most data at rest is secured by symmetric algorithms like Advanced Encryption Standard (AES), which are much more resistant to quantum attacks than to asymmetric attacks, and there are known methods like increasing key sizes, which will blunt or significantly reduce the likelihood of decryption. However, most knowledge management systems (KMSs) and identity and access management (IAM) systems do use asymmetric keys to secure keystores that are a possible vector. Attackers could launch an IAM attack on a keystore, grab the keys and then decrypt the documents. There are many standard ways, such as data security platforms and IAM systems, to detect or blunt such attacks.

> Because quantum computers don’t have an advantage over classical computers for running standard attacks and they are still fairly modest, they are not generally useful as direct vectors for cybercrimes.

For state actors aimed at developing more standard methods of attacks, quantum computers as optimizers could make attacks more efficient, smaller or harder to detect. These attacks are often released to a hacker community anonymously, used by attackers, and monitored by the SAs to determine effectiveness and avenues of further optimization. Although we do not have direct evidence, we know that this is a pattern that SAs followed to achieve their goals in the past. To protect against such attacks, you should have effective standard cybersecurity measures in place.

Risks Posed by AI Running on Quantum Computers

As of spring 2025, commercially available quantum computers are incapable of working with the large datasets required by even the simplest AI. We don’t expect them to become relevant for quite some time, except for very specific and limited cases.

That said, if ways can be found to involve them, AI and quantum computers, both of which are probabilistic in nature, should work well together. Theoretically, a quantum computer could allow the creation of an optimized AI for a given training set a few orders of magnitude faster than existing classical machines. “Quantum-inspired” machine learning (ML) algorithms, developed on quantum computers, could perhaps be transferred to classical systems and, in theory, can be more efficient or effective.

Recommendations

Prepare for PQC by recognizing that classical cryptography should be deprecated by 2030 and following the guidance provided by Postquantum Cryptography: The Time to Prepare Is Now!

Enhance protection from advanced persistent threats and other classical mechanisms for data exfiltration.

Quantum computers should have no influence on AI in the near future, so favor standard AI security precautions.

Form a Small Team to Manage Threats and Opportunities Presented by Quantum Computing

Focus: CIOs, CISOs, DPOs, heads of software development

Though not an immediate threat or opportunity, quantum computing signifies a shift in CISO priorities that will increasingly gain importance as 2030 approaches. As quantum computers mature and the threat posed by SAs escalates, this shift will become more pronounced.

Similar to AI, which came onto the market so suddenly that there were not enough data scientists to meet the demand, quantum computing presents a challenge that programming and cybersecurity skills gaps will make it hard to effectively manage.

Recommendations

Gartner recommends putting together a small, but well-trained team that:

- Can understand the threat landscape posed by advancing quantum computers and deal with threats posed by state-level actors.
- Can interface with the cryptographic center of excellence that leads the PQC response to new algorithms.
- Includes programmers and project managers who are trained in quantum computing, and can quickly evaluate opportunities presented by quantum computers and respond in an informed manner to determine what benefits, if any, quantum computers will bring to the organization.
- Can separate real opportunities and threats from hyperbole around quantum computers and evaluate these opportunities and threats.

Although small in size, the team can keep up with advances in technology and help you determine whether, when and how to capitalize on the advances in quantum computing. The next five to seven years will see advances, as well as claims and even hyperbole, related to quantum computing. This team will keep your organization grounded and help it develop a sound strategy on quantum computing.

Evidence

[1] NIST Releases First 3 Finalized Post-Quantum Encryption Standards

[2] NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

This research is based in part on interactions with clients from 2023 through March 2025 on quantum computing, as well as dozens of briefings from the quantum computing research and vendor community as part of our twice monthly quantum research group.

Acronym Key and Glossary Terms

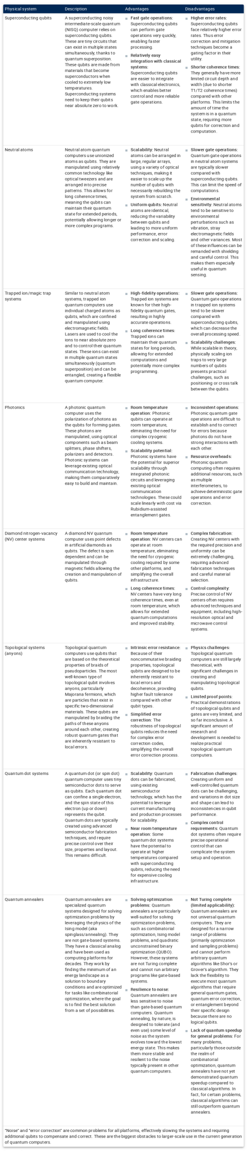
Entanglement	This is also known as“quantum magic,” which means putting qubits into a state where they share information in probabilistic ways that can't be done in a classical channel. It's the key to quantum advantages and is essentially a nonclassical computational route also known as quantum parallelism. The state is very fragile, can be "measured" by almost anything and will eventually collapse on its own.
Coherence time	This means how long a qubit can remain in a quantum state. There are two typical parameters: T1 (relaxation time) which represents how long a qubit can remain in an excited state before naturally decaying into the ground state (decoherence) and T2 (dephasing time) which represents how long a qubit can remain "in phase" or in a superposition of |0> and |1>.
Quantum gate	Quantum gates are the building blocks of quantum circuits, which manipulate qubits by changing their states (like logic gates in classical computing). Gates enable quantum algorithms to perform complex operations. Qubits need to be in phase and in coherence in order to form a computational logic gate (e.g., AND, NOR, XOR).
Quantum error rate	This is the frequency at which errors occur during the execution of quantum operations. These occur for a wide variety of reasons, but the net effect is to blunt the effectiveness of the quantum advantage. There are a wide variety of ways around this depending on the physics of the machine.
Quantum gate error	A quantum gate error occurs when, usually due to noise, a qubit in an entangled group collapses into a random state and causes the system to compute the wrong gate. Such errors can be mitigated through techniques such as tensor stabilizer codes and error correction codes.
Noise	Because entanglement is very fragile in quantum computers, noise from the environment (or dephasing, measurement errors, cross talk or decoherence) acts like a measurement of the quantum state, causing it to collapse into a single value |0> or |1>. This property can be valuable in quantum sensing if it comes from the environment.
Quantum volume	It's very difficult to compare the "power" or abilities of one quantum computer against another, especially when they are made from different physical strata. IBM published research on dozen or so different parameters that characterize quantum computers (including gate configurations, circuit depth and

	length, T1/T2 times and others) to try to form a stable basis of comparison. It's very complicated, and the same quantum computer can have different quantum volumes depending on the problem being solved. Because of this complexity, it's rarely cited by vendors outside of peer-reviewed science.

Note 1: A Brief Guide to the Physics of Quantum Computers

Table 2: Physics of Quantum Computers

(Enlarged table in Appendix)



Physical system	Description	Advantages	Disadvantages
Superconducting qubits	A superconducting noisy intermediate-scale quantum (NISQ) computer relies on superconducting qubits. These are tiny circuits that can exist in multiple states simultaneously, thanks to quantum superposition. These qubits are made from materials that become superconductors when cooled to extremely low temperatures. Superconducting systems need to keep their qubits near absolute zero to work.	▪ **Fast gate operations:** Superconducting qubits can perform gate operations very quickly, enabling faster processing. ▪ **Relatively easy integration with classical systems:** Superconducting qubits are easier to integrate with classical electronics, which enables better control and more reliable gate operations.	▪ **Higher error rates:** Superconducting qubits face relatively higher error rates. Thus error correction and mitigation techniques become a gating factor in their utility. ▪ **Shorter coherence times:** They generally have more limited circuit depth and width (due to shorter T1/T2 coherence times) compared with other platforms. This limits the amount of time the system is in a quantum state, requiring more qubits for correction and computation.
Neutral atoms	Neutral atom quantum computers use unionized atoms as qubits. They are manipulated using relatively common technology like optical tweezers and are arranged into precise patterns. This allows for long coherence times, meaning the qubits can maintain their quantum state for extended periods, potentially allowing longer or more complex programs.	▪ **Scalability:** Neutral atoms can be arranged in large, regular arrays, using a variety of optical techniques, making it easier to scale up the number of qubits with necessarily rebuilding the system from scratch. ▪ **Uniform qubits:** Neutral atoms are identical, reducing the variability between qubits and leading to more uniform performance, error correction and scaling.	▪ **Slower gate operations:** Quantum gate operations in neutral atom systems are typically slower compared with superconducting qubits. This can limit the speed of computations. ▪ **Environmental sensitivity:** Neutral atoms tend to be sensitive to environmental perturbations such as vibration, stray electromagnetic fields and other variances. Most of these influences can be remanded with shielding and careful control. This makes them especially useful in quantum sensing.
Trapped ion/magic trap systems	Similar to neutral atom systems, trapped ion quantum computers use individual charged atoms as qubits, which are confined and manipulated using electromagnetic fields. Lasers are used to cool the ions to near absolute zero and to control their quantum states. These ions can exist in multiple quantum states simultaneously (quantum superposition) and can be entangled, creating a flexible quantum computer.	▪ **High-fidelity operations:** Trapped ion systems are known for their high-fidelity quantum gates, resulting in highly accurate operations. ▪ **Long coherence times:** Trapped ions can maintain their quantum states for long periods, allowing for extended computations and potentially more complex programming.	▪ **Slower gate operations:** Quantum gate operations in trapped ion systems tend to be slower compared with superconducting qubits, which can decrease the overall processing speed. ▪ **Scalability challenges:** While scalable in theory, physically scaling ion traps to very large numbers of qubits presents practical challenges, such as positioning or cross talk between the qubits.
Photonics	A photonic quantum computer uses the polarization of photons as the qubits for forming gates. These photons are manipulated, using optical components such as beam splitters, phase shifters, polarizers and detectors. Photonic systems can leverage existing optical communication technology, making them comparatively easy to build and maintain.	▪ **Room temperature operation:** Photonic qubits can operate at room temperature, eliminating the need for complex cryogenic cooling systems. ▪ **Scalability potential:** Photonic systems have the potential for superior scalability through integrated photonic circuits and leveraging existing optical communication technologies. These could scale linearly with cost via Rubidium-assisted entanglement gates.	▪ **Inconsistent operations:** Photonic quantum gate operations are difficult to establish and to correct for errors because photons do not have strong interactions with each other. ▪ **Resource overheads:** Photonic quantum computing often requires additional resources, such as multiple interferometers, to achieve deterministic gate operations and error correction.
Diamond nitrogen-vacancy (NV) center systems	A diamond NV quantum computer uses point defects in artificial diamonds as qubits. The defect is spin dependent and can be manipulated through magnetic fields allowing the creation and manipulation of qubits.	▪ **Room temperature operation:** NV centers can operate at room temperature, eliminating the need for cryogenic cooling required by some other platforms, and simplifying the overall infrastructure. ▪ **Long coherence times:** NV centers have very long coherence times, even at room temperature, which allows for extended quantum computations and improved stability.	▪ **Complex fabrication:** Creating NV centers with the required precision and uniformity can be extremely challenging, requiring advanced fabrication techniques and careful material selection. ▪ **Control complexity:** Precise control of NV centers often requires advanced techniques and equipment, including high-resolution optical and microwave control systems.
Topological systems (anyons)	Topological quantum computers use qubits that are based on the theoretical properties of braids of pseudoparticles. The most well-known type of topological qubit involves anyons, particularly Majorana fermions, which are particles that exist in specific two-dimensional materials. These qubits are manipulated by braiding the paths of these anyons around each other, creating robust quantum gates that are inherently resistant to local errors.	▪ **Intrinsic error resistance:** Because of their noncommutative braiding properties, topological qubits are designed to be inherently resistant to local errors and decoherence, providing higher fault tolerance compared with other qubit types. ▪ **Simplified error correction:** The robustness of topological qubits reduces the need for complex error correction codes, simplifying the overall error correction process.	▪ **Physics challenges:** Topological quantum computers are still largely theoretical, with significant challenges in creating and manipulating topological qubits. ▪ **Limited proof points:** Practical demonstrations of topological qubits and gates are very limited, and so far inconclusive. A significant amount of research and development is needed to realize practical topological quantum computers.
Quantum dot systems	A quantum dot (or spin dot) quantum computer uses tiny semiconductor dots to serve as qubits. Each quantum dot can confine a single electron, and the spin state of this electron (up or down) represents the qubit. Quantum dots are typically created using advanced semiconductor fabrication techniques, and require precise control over their size, properties and layout. This remains difficult.	▪ **Scalability:** Quantum dots can be fabricated, using existing semiconductor technology, which has the potential to leverage current manufacturing and production processes for scalability. ▪ **Near room temperature operation:** Some quantum dot systems have the potential to operate at higher temperatures compared with superconducting qubits, reducing the need for expensive cooling infrastructure.	▪ **Fabrication challenges:** Creating uniform and well-controlled quantum dots can be challenging, and variations in dot size and shape can lead to inconsistencies in qubit performance. ▪ **Complex control requirements:** Quantum dot systems often require precise operational control that can complicate the system setup and operation.
Quantum annealers	Quantum annealers are specialized quantum systems designed for solving optimization problems by leveraging the physics of the Ising model (aka spinglass/annealing). They are not gate-based systems. They have a classical analog and have been used as computing platforms for decades. They work by finding the minimum of an energy landscape as a solution to boundary conditions and are optimized for tasks like combinatorial optimization, where the goal is to find the best solution from a set of possibilities.	▪ **Solving optimization problems:** Quantum annealers are particularly well-suited for solving optimization problems, such as combinatorial optimization, Ising model problems, and quadratic unconstrained binary optimization (QUBO). However, these systems are not Turing complete and cannot run arbitrary programs like gate-based systems. ▪ **Resilience to noise:** Quantum annealers are less sensitive to noise than gate-based quantum computers. Quantum annealing, by nature, is designed to tolerate (and even use) some level of noise as the system evolves toward the lowest energy state. This makes them more stable and resilient to the noise typically present in other quantum computers.	▪ **Not Turing complete (limited applicability):** Quantum annealers are not universal quantum computers. They are designed for a narrow range of problems (primarily optimization and sampling problems) and cannot perform arbitrary quantum algorithms like Shor's or Grover's algorithm. They lack the flexibility to execute most quantum algorithms that require general quantum gates, quantum error correction, or entanglement beyond their specific design because there are no logical qubits. ▪ **Lack of quantum speedup for general problems:** For many problems, particularly those outside the realm of combinatorial optimization, quantum annealers have not yet demonstrated quantum speedup compared to classical algorithms. In fact, for certain problems, classical algorithms can still outperform quantum annealers.

"Noise" and "error correction" are common problems for all platforms, effectively slowing the systems and requiring additional qubits to compensate and correct. These are the biggest obstacles to larger-scale use in the current generation of quantum computers.

Source: Gartner

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Justify, Build and Launch a Postquantum Response

Top Strategic Technology Trends for 2025: Postquantum Cryptography

Postquantum Cryptography: The Time to Prepare Is Now!

Table 1: Areas Where Potential Quantum Advantages Can Be Realized

Area	Example	Potential quantum advantage	Reference
Breaking asymmetric cryptography	Shor's algorithm (1994)	Breaking widely used cryptographic protocols like Rivest-Shamir-Adelman (RSA), Diffie—Hellman (DH) and elliptic curve cryptography (ECC), driving the need for PQC.	Quantum Computing in Cryptography, IEEE Xplore
Breaking symmetric cryptography	Grover's algorithm (1996)	Allowing a quadratic speedup over brute-force search.	Theory of Grover's Search Algorithm, Microsoft
Optimization problems/financial modeling	Solving complex combinatorial optimization challenges, such as vehicle routing and portfolio optimization	Enhancing efficiency in logistics, finance and AI by providing faster solutions to problems that are computationally intensive for classical computers.	Industry Quantum Computing Applications, SpringerOpen
Machine learning acceleration	Enhancing algorithms for data clustering, classification and pattern recognition	Quantum computers are inherently probabilistic and offer the advantage of speed, enabling them to tackle problems that involve finding global maxima or minima, particularly in convex optimization scenarios.	Quantum Machine Learning: Bridging the Future of AI and Quantum Computing, TechBullion
Search and database optimization	Accelerating search operations within large, unsorted datasets	Improving the efficiency of data retrieval processes, benefiting sectors like IT and big data analytics.	Quantum Computing Gets Real: It Could Even Shorten Your Airport

			Connection (subscription required), The Wall Street Journal
Solving linear systems	Efficiently solving large systems of linear equations	Benefiting fields such as engineering and computer graphics by providing faster computational methods (the Harrow-Hassidim-Lloyd algorithm).	Quantum Algorithm for Solving Linear Systems of Equations, arXiv, Cornell University

Source: Gartner (April 2025)

Table 2: Physics of Quantum Computers

Physical system	Description	Advantages	Disadvantages
Superconducting qubits	A superconducting noisy intermediate-scale quantum (NISQ) computer relies on superconducting qubits. These are tiny circuits that can exist in multiple states simultaneously, thanks to quantum superposition. These qubits are made from materials that become superconductors when cooled to extremely low temperatures. Superconducting systems need to keep their qubits near absolute zero to work.	■ **Fast gate operations:** Superconducting qubits can perform gate operations very quickly, enabling faster processing. ■ **Relatively easy integration with classical systems:** Superconducting qubits are easier to integrate with classical electronics, which enables better control and more reliable gate operations.	■ **Higher error rates:** Superconducting qubits face relatively higher error rates. Thus error correction and mitigation techniques become a gating factor in their utility. ■ **Shorter coherence times**: They generally have more limited circuit depth and width (due to shorter T1/T2 coherence times) compared with other platforms. This limits the amount of time the system is in a quantum state, requiring more qubits for correction and computation.
Neutral atoms	Neutral atom quantum computers use unionized atoms as qubits. They are manipulated using relatively common technology like optical tweezers and are arranged into precise patterns. This allows for long	■ **Scalability:** Neutral atoms can be arranged in large, regular arrays, using a variety of optical techniques, making it easier to scale up the number of qubits with	■ **Slower gate operations:** Quantum gate operations in neutral atom systems are typically slower compared with superconducting qubits. This can limit the speed of computations.

	coherence times, meaning the qubits can maintain their quantum state for extended periods, potentially allowing longer or more complex programs.	necessarily rebuilding the system from scratch. ■ **Uniform qubits:** Neutral atoms are identical, reducing the variability between qubits and leading to more uniform performance, error correction and scaling.	■ **Environmental sensitivity:** Neutral atoms tend to be sensitive to environmental perturbations such as vibration, stray electromagnetic fields and other variances. Most of these influences can be remanded with shielding and careful control. This makes them especially useful in quantum sensing.
Trapped ion/magic trap systems	Similar to neutral atom systems, trapped ion quantum computers use individual charged atoms as qubits, which are confined and manipulated using electromagnetic fields. Lasers are used to cool the ions to near absolute zero and to control their quantum states. These ions can exist in multiple quantum states simultaneously (quantum superposition) and can be entangled, creating a flexible quantum computer.	■ **High-fidelity operations:** Trapped ion systems are known for their high-fidelity quantum gates, resulting in highly accurate operations. ■ **Long coherence times:** Trapped ions can maintain their quantum states for long periods, allowing for extended computations and potentially more complex programming.	■ **Slower gate operations:** Quantum gate operations in trapped ion systems tend to be slower compared with superconducting qubits, which can decrease the overall processing speed. ■ **Scalability challenges:** While scalable in theory, physically scaling ion traps to very large numbers of qubits presents practical challenges, such as positioning or cross talk between the qubits.
Photonics	A photonic quantum computer uses	■ **Room temperature operation:**	■ **Inconsistent operations:** Photonic

	the polarization of photons as the qubits for forming gates. These photons are manipulated, using optical components such as beam splitters, phase shifters, polarizers and detectors. Photonic systems can leverage existing optical communication technology, making them comparatively easy to build and maintain.	Photonic qubits can operate at room temperature, eliminating the need for complex cryogenic cooling systems. - **Scalability potential:** Photonic systems have the potential for superior scalability through integrated photonic circuits and leveraging existing optical communication technologies. These could scale linearly with cost via Rubidium-assisted entanglement gates.	quantum gate operations are difficult to establish and to correct for errors because photons do not have strong interactions with each other. - **Resource overheads:** Photonic quantum computing often requires additional resources, such as multiple interferometers, to achieve deterministic gate operations and error correction.
Diamond nitrogen-vacancy (NV) center systems	A diamond NV quantum computer uses point defects in artificial diamonds as qubits. The defect is spin dependent and can be manipulated through magnetic fields allowing the creation and manipulation of qubits.	- **Room temperature operation:** NV centers can operate at room temperature, eliminating the need for cryogenic cooling required by some other platforms, and simplifying the overall infrastructure. - **Long coherence times:** NV centers have very long coherence times, even at room temperature, which allows for extended quantum	- **Complex fabrication:** Creating NV centers with the required precision and uniformity can be extremely challenging, requiring advanced fabrication techniques and careful material selection. - **Control complexity:** Precise control of NV centers often requires advanced techniques and equipment, including high-resolution optical and microwave control systems.

		computations and improved stability.	
Topological systems (anyons)	Topological quantum computers use qubits that are based on the theoretical properties of braids of pseudoparticles. The most well-known type of topological qubit involves anyons, particularly Majorana fermions, which are particles that exist in specific two-dimensional materials. These qubits are manipulated by braiding the paths of these anyons around each other, creating robust quantum gates that are inherently resistant to local errors.	▪ **Intrinsic error resistance:** Because of their noncommutative braiding properties, topological qubits are designed to be inherently resistant to local errors and decoherence, providing higher fault tolerance compared with other qubit types. ▪ **Simplified error correction:** The robustness of topological qubits reduces the need for complex error correction codes, simplifying the overall error correction process.	▪ **Physics challenges:** Topological quantum computers are still largely theoretical, with significant challenges in creating and manipulating topological qubits. ▪ **Limited proof points:** Practical demonstrations of topological qubits and gates are very limited, and so far inconclusive. A significant amount of research and development is needed to realize practical topological quantum computers.
Quantum dot systems	A quantum dot (or spin dot) quantum computer uses tiny semiconductor dots to serve as qubits. Each quantum dot can confine a single electron, and the spin state of this electron (up or down) represents the qubit. Quantum dots are typically created using advanced	▪ **Scalability:** Quantum dots can be fabricated, using existing semiconductor technology, which has the potential to leverage current manufacturing and production processes for scalability.	▪ **Fabrication challenges:** Creating uniform and well-controlled quantum dots can be challenging, and variations in dot size and shape can lead to inconsistencies in qubit performance. ▪ **Complex control requirements:** Quantum dot systems often

	semiconductor fabrication techniques, and require precise control over their size, properties and layout. This remains difficult.	- **Near room temperature operation:** Some quantum dot systems have the potential to operate at higher temperatures compared with superconducting qubits, reducing the need for expensive cooling infrastructure.	require precise operational control that can complicate the system setup and operation.
Quantum annealers	Quantum annealers are specialized quantum systems designed for solving optimization problems by leveraging the physics of the Ising model (aka spinglass/annealing). They are not gate-based systems. They have a classical analog and have been used as computing platforms for decades. They work by finding the minimum of an energy landscape as a solution to boundary conditions and are optimized for tasks like combinatorial optimization, where the goal is to find the best solution from a set of possibilities.	- **Solving optimization problems:** Quantum annealers are particularly well-suited for solving optimization problems, such as combinatorial optimization, Ising model problems, and quadratic unconstrained binary optimization (QUBO). However, these systems are not Turing complete and cannot run arbitrary programs like gate-based systems. - **Resilience to noise:** Quantum annealers are less sensitive to noise than gate-based quantum computers. Quantum annealing, by nature, is designed to tolerate (and even use) some level of noise as the system evolves toward the	- **Not Turing complete (limited applicability):** Quantum annealers are not universal quantum computers. They are designed for a narrow range of problems (primarily optimization and sampling problems) and cannot perform arbitrary quantum algorithms like Shor's or Grover's algorithm. They lack the flexibility to execute most quantum algorithms that require general quantum gates, quantum error correction, or entanglement beyond their specific design because there are no logical qubits.

	lowest energy state. This makes them more stable and resilient to the noise typically present in other quantum computers.	■ **Lack of quantum speedup for general problems:** For many problems, particularly those outside the realm of combinatorial optimization, quantum annealers have not yet demonstrated quantum speedup compared to classical algorithms. In fact, for certain problems, classical algorithms can still outperform quantum annealers.
"Noise" and "error correction" are common problems for all platforms, effectively slowing the systems and requiring additional qubits to compensate and correct. These are the biggest obstacles to larger-scale use in the current generation of quantum computers.		

Source: Gartner