

Transformation

Quantum leaps and bounds

23 October 2025

Key takeaways

- Quantum computing is set to revolutionize problem-solving, enabling calculations in seconds that would take classical computers billions of years. While early demonstrations of quantum supremacy have shown promise, achieving quantum advantage - i.e. solving real-world problems faster than classical systems - remains a work in progress.
- Yet, even as we work toward that breakthrough, quantum computing may already be finding its first foothold in energy efficiency. Hybrid quantum-classical systems are showing promise in reducing energy consumption by up to 12.5%, a timely benefit as global electricity demand continues to surge.
- At the same time, quantum computing is forming a transformative alliance with AI. This "power couple" has the potential to supercharge AI model training while using AI to accelerate quantum development. Together, they could unlock groundbreaking applications across industries bringing us closer to a future where quantum advantage isn't just theoretical, but tangible.
- Complex concepts don't have to stay complex - refer to the quantum dictionary at the end of the piece for clear, concise definitions that make the abstract a bit more accessible.

Quantum computing 101

Quantum computing could be one of the biggest revolutions yet. By leveraging sub-atomic particles to store information and using superpositions for complex calculations, a quantum computer can solve problems near instantaneously that would take a classical computer billions of years.

The evolution of quantum

The idea of quantum computation originated from the recognition that classical computers cannot efficiently simulate quantum systems. In the 1980s, physicist Richard Feynman and mathematician Yuri Manin each suggested that a quantum mechanical machine could simulate quantum physics efficiently compared to conventional computers. This foundational insight led to theoretical explorations of quantum logic gates and computational complexity.

By the mid-1990s, major breakthroughs occurred. Peter Shor introduced an algorithm, known as Shor's Algorithm, for factoring large numbers exponentially faster than the best-known classical methods. Around the same time, Lov Grover devised an algorithm, known as Grover's Algorithm, that raised promising potential for quantum computers to search unsorted databases faster than any classical approach.

Despite the theoretical promise, building actual quantum hardware proved daunting. It was not until the 2010s when quantum processors began to materialize, initially with a few working qubits (quantum bits). The race to scale up reliable quantum hardware, while solving the persistent challenges of decoherence, control precision, and error correction, has driven global investment across academia, industry, and government.

How it works: Bizarre and mysterious lesson 101

Although quantum computers and classical computers both use circuits, chips, and logic gates to process information and both are operated by algorithms, the fundamental difference lies in how information is processed. Unlike its counterpart, which operates using bits that represent either 0 or 1 (think light switches), quantum computers use qubits (quantum bits) as the basic unit of information. Quantum computers operate using quantum mechanics such as superposition and entanglement.

- **Superposition:** If a classical computer can work on two possibilities only (0 or 1, electricity is either on (i.e., 1) or off (i.e., 0)), the superposition phenomenon theoretically translates into endless possibilities and, as a result, endless calculations. Unlike classical physics, superposition posits that a particle can be in more than one state at any given time: two states, more than two or even none. For example, a photon could be up, down, up and down, in no state, or anything in between, all at the same time.

But here is where it gets even weirder. Superposition has one condition – it requires uncertainty. Once we observe and measure the position (i.e., add certainty to the equation) the superposition states collapse into one. Meaning that in order to stay in a superposition and make endless calculations, we need uncertainty.

Superposition paradox: Schrödinger's cat. To demonstrate superposition anomaly, in 1935, Erwin Schrödinger suggested a paradox, according to which a cat, a radioactive substance that decays very slowly, and a Geiger counter are put together in a sealed box. According to quantum mechanics physics after a while the cat could be in a superposition of being both alive and dead, as long as we do not open the box. Once we open the box, the uncertainty that triggers the superposition will collapse.

Another way of thinking about superposition is by imagining a sphere with the north pole as zero and the south pole as one. Anything else on or within the sphere represents infinite possibilities of other positions. This allows us to: 1) represent complex forms of information; and 2) simulate atoms in a computer.

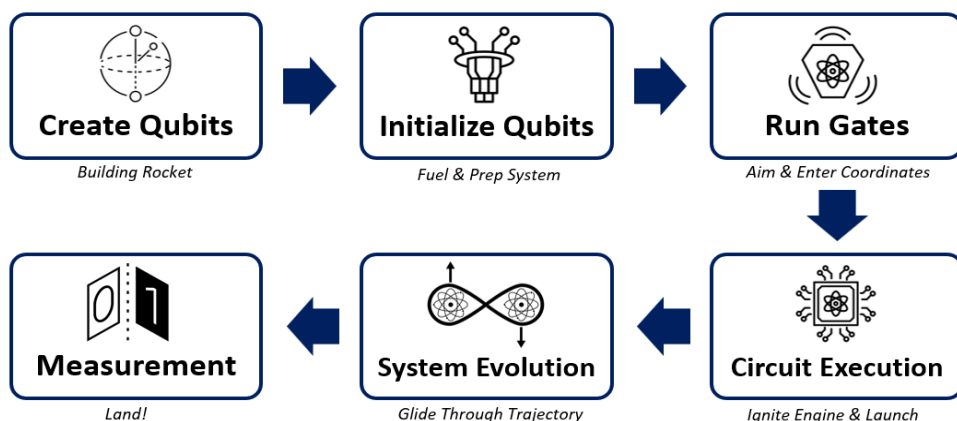
- **Entanglement:** This refers to two or more quantum systems being linked in an unseparated bond, even if far apart – meaning this status cannot be described independently, even if the distance between them is vast. Any effect on one particle will instantly impact the other, faster than the speed of light, no matter the distance between them. If superposition offers endless states and therefore calculations, entanglement provides parallel processing of the system and allows it to scale up and work as one and other properties like error correction or control interference.
- **Qubits:** In other words – quantum bits – a quantum computer's basic unit of information. Superposition of a particle can exist in a qubit and multiple qubits can be entangled – meaning one qubit can affect another. In short, these units contain the quantum mechanics properties of superpositions and entanglements. Without qubits, those properties could not be harnessed to create a quantum computer. To complicate matters yet further, qubits can act like waves, or particles and can tunnel through energy barriers – which is impossible according to classical physics – and just “turn up on the other side.” However, to achieve these qualities, qubits need to be fully isolated, and if not, they “collapse” and become “normal bits.”

The process

On a high-level basis, a quantum computing process can be broken down into six steps (Exhibit 1).

Exhibit 1: On a high level, quantum computing can be broken into six steps that go from creating qubits to measurement

Overview of quantum computing process, rocket analogy included for illustrative purposes



Source: BofA Global Research, Noun Project

BANK OF AMERICA INSTITUTE

First, is engineering the physical qubits, which serve as the hardware foundation for a quantum computer. Qubits are capable of exhibiting quantum behavior like superposition and entanglement.

Next is initialization, which means qubits are reset to a starting point (clean slate) where there is no superposition or entanglement. Initialization ensures consistent, noise-free quantum computation. A common starting state is a computational basis state $|0\rangle$, or “ket zero.”

Then, quantum gates are applied to put qubits into superposition and entangled states, effectively encoding input data (a problem) into a quantum system.

The core of the quantum algorithm is executed through the quantum circuit, where gates are applied in a structured sequence to process the encoded quantum state and solve a problem. As gates perform designated quantum logic through constructive and/or destructive interference patterns, the quantum system continues to evolve.

Upon the conclusion of all operations and entanglements, the algorithm is complete. Qubit states are expected to contain a solution and are ready to be measured.

Once measured, qubits collapse from their quantum states. Upon collapsing, qubits become classical bits which can then be used for further analysis or decision-making. It is important to note that this does not mean qubits are no longer useful in quantum computing or become “bits” permanently. Qubits can be reinitialized to ground state and be “reused” in future computations.

Solving useful real-world problems by 2033?

We've seen examples of quantum supremacy

Massive progress has been achieved in recent years in terms of examples of quantum supremacy – solving a problem that traditional computers could not solve in any feasible amount of time. For example, in 2023, Google announced that its 70-qubit Sycamore quantum processor had completed a six-second calculation that would have taken the most powerful supercomputer 47 years. And, in December 2024, Google announced a new quantum chip, Willow, which is reported to be able to solve a complex benchmark problem in under five minutes. It would have taken the world's fastest supercomputer roughly 10 septillion years (10^{25}) to complete, far exceeding the current estimated age of the universe.

But not quantum advantage yet because quantum computers are too noisy

Whilst quantum computers (QCs) may be able to solve certain problems better than a classical computer, the challenge is *demonstrating quantum advantage* – that a quantum computer can solve a useful real-world problem faster than a classical computer.

We have not yet been able to achieve this because quantum computers are too “noisy” where the qubit quality is not high enough yet to see quantum advantage. Quantum qubit “noise” refers to disturbances or inaccuracies that affect the qubits (the fundamental units of quantum information), which lead to errors in the quantum computation and cause them to lose their quantum state, known as decoherence.¹

Three barriers to adopting QCs: infrastructure, performance, learning²

- **Infrastructure:** There is a challenge in terms of integrating quantum computers into existing infrastructure like data centers and workflows or applications. Most companies in quantum computing have done an integration with the private cloud but colocating in a data center creates data security and latency benefits.
- **Performance:** Quantum computers are currently too error prone. A measure of performance is fidelity, where a higher figure represents a lower degree of error. The tablet computers we use today have a fidelity of ‘17x 9s’, i.e., 99.99999...% (17x 9s after the decimal point) and currently quantum computers are at the 99.9% level. To reach some form of advantage from quantum (“quantum advantage”), we would need to have three additional 9s.
- **Learning:** It requires a specialized skillset to program a QC. And according to OQC, we need a layer of abstraction so that a non-expert user can use a QC. This could involve integrating the QC into an existing platform or software application. There can also be a ‘quantum inspiration’ learning effect. Since QCs are still error prone, customers can identify the problem a QC might be aiming to optimize and use a classical computer instead to solve a similar problem.

First advantage of quantum may not be compute, but energy efficiency gains

Energy demand is surging – and will continue to do so for an extended period, which will require significant additions to power generation capacity and higher capex to grow the grid. In fact, BofA Global Research estimates that US electrical demand will increase at a 2.5% compound annual growth rate (CAGR) through 2035E (Exhibit 2). That compares to just a 0.5% CAGR from 2014-2024. For more on this, read: [Power check: Watt's going on with the grid?](#)

¹ QuEra. (n.d.). *Quantum Noise*.

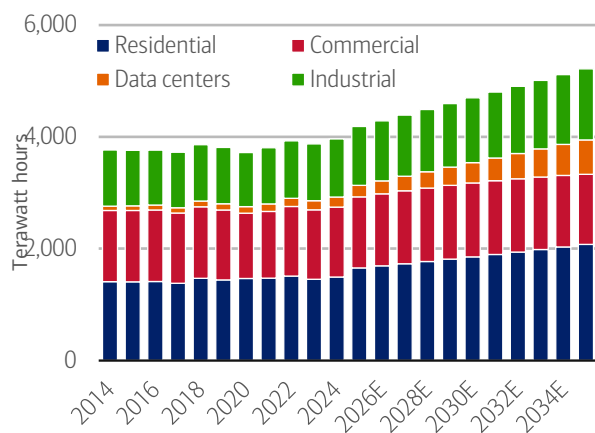
² Oxford Quantum Circuits (OQC)

With the electrification of industry, transport and buildings, potentially adding around 7,000 terawatt-hours (TWh) of electricity demand globally by 2030³ – and within that, data centers adding around 400TWh by 2030 in the US alone⁴ – greater technology use requires more energy (Exhibit 3).

So, it's with this in mind that the first advantage of quantum may not be computational. Instead, it could be the energy efficiency gains where the combination of classical and quantum computing would use less energy than leveraging purely classical computing. When combined with classical compute, QCs could reduce energy consumption by up to 12.5%.⁵ And for a given problem, QCs might use the same energy as nine household kettles versus that of 15,000 homes for a supercomputer.⁶

Exhibit 2: BofA Global Research expects US electrical demand to grow at a 2.5% CAGR over 2024-35E

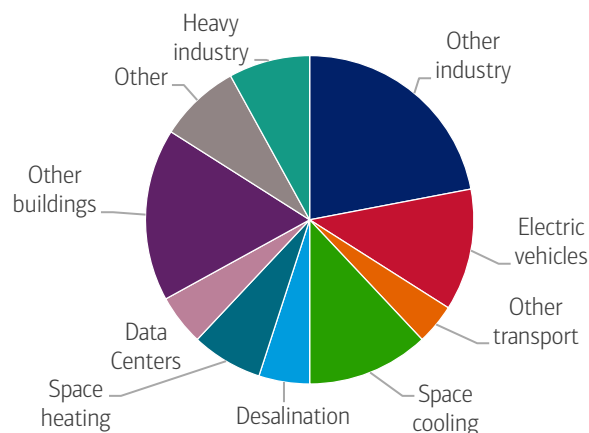
US electrical demand (TWh per year) 2014–2035E



Source: BofA Global Research estimates, US Energy Information Administration
BANK OF AMERICA INSTITUTE

Exhibit 3: Electrification of transport, industry, heating and technology set to require c.7,000 TWh additional electricity, more than annual electricity demand of the US/EU combined

Global electricity demand growth 2023-2030 (6,760TWh)



Source: IEA 2024; World Energy Outlook, CC BY 4.0

BANK OF AMERICA INSTITUTE

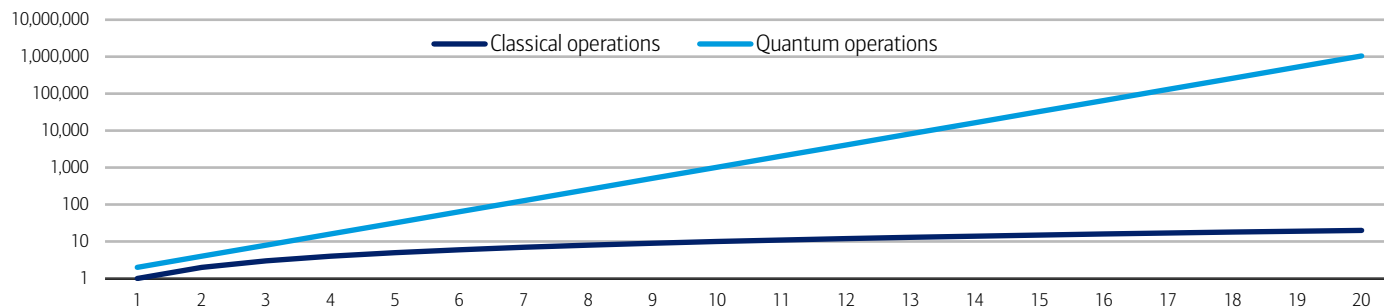
How can we broaden quantum adoption?

QCs scale exponentially, and so more qubits should bring more capabilities

Quantum computers scale exponentially where every additional qubit doubles the number of operations the system can perform. A QC with just 10 qubits could perform more than 100 times the operations that a classical computer can perform (Exhibit 4). And a QC with more qubits should be able to perform more operations and unlock more in economic value for the industries in which it can be implemented.

Exhibit 4: A quantum computer with just 10 qubits could perform more than 100x the operations that a classical computer can perform

Number of classical vs quantum operations for a given (qu)bit number (log scale)



Source: BofA Global Research

BANK OF AMERICA INSTITUTE

³ IEA. (2024, October 16). *World Energy Outlook 2024*.

⁴ McKinsey

⁵ Ajagekar, A., You, F. (2024, July). *Variational quantum circuit learning-enabled robust optimization for AI data center energy control and decarbonization*. *Advances in Applied Energy*. Vol.14.

⁶ OQC

However, scaling qubits requires us to solve many issues (e.g. error, cost, speed)

For a QC to scale, we must be able to solve problems related to readout control (measuring the quantum state of qubits), real-time error correction, cost, energy efficiency, high speed/low latency, multiplexing (dividing a communication channel into a number of “logical” channels) and GPU (graphics processing unit) integration.

For example, some quantum computing architectures involve complex architecture, e.g., cabling. As the qubit number increases, certain aspects of the physical infrastructure will need to increase too, e.g., more cables and control lines (which carry signals to drive the qubits) and these can lead to qubit interference. The result would be more errors as qubits are added to the system.

Various types of qubit and path to achieve qubit scaling

There are different ways of creating the qubits for quantum computing: superconducting circuits (based on superconducting materials cooled to near absolute zero); trapped ions (involve electromagnetic fields which confine and manipulate charged atoms and are controlled via laser pulses); and neutral atoms (involve trapping and isolating individual atoms, also controlled by lasers).

Different companies are pursuing different modalities: some big-tech companies are exploring superconducting circuits, the most mature modality, while others are using ion trap and Pasqal and QuEra on neutral atoms.

Companies are pursuing different technologies to scale up quantum computers. These include a 3D chip architecture based on superconducting qubits, which puts the control lines in a different plane to the qubits – while others are leveraging logical qubits.

A matter of unlimited possibilities

Quantum computing has a wide range of use cases

A future QC can process more calculations than there are atoms in the universe (10^{80}).⁷ The possibilities of a computer that can theoretically make endless calculations simultaneously are huge. This could range from a new unbreakable encryption to calculations that now require huge resources and time, such as simulation, deep learning and real usage of big data analysis. Quantum computing can be used for problems relating to optimization, machine learning, simulation and factorization across many sectors, such as automotive and logistics, financial services, energy and climate, health and life sciences and national security.

\$2 trillion in economic value by 2035 with a market size of up to \$72 billion

Per McKinsey, the potential economic value from quantum computing in 2035 could range from around \$0.9-2 trillion across four industries – chemicals, life sciences, finance and mobility – which may realize this value earlier than others. And the market size for quantum computing is expected to reach \$28-72 billion in 2035.⁸

The convergence between AI and quantum

The “power couple” that will change the world

One of the most exciting applications is the marriage of the two most powerful technologies: AI and quantum computers. The convergence of AI and quantum (AQ) technologies can enable fundamental improvements in the physical world as well as the digital one. While QCs will provide endless calculations when available, the increased capability of AI technologies can unlock several transformational use cases in the meantime.

Large language models (LLMs) complemented with simulation, knowledge graphs, computer vision and predictive analytics are “the new AI toolbox” that companies can deploy. Iterative research tasks that would have taken years can now be achieved in weeks. Chemicals, life sciences, materials, and finance/logistics are all in scope to benefit. To ground yourself in all-things AI, read our [AI Dictionary series](#).

A complementary relationship

AI and quantum computing could converge to complement each other unlocking more transformative use cases. For example, quantum computing can help provide compute power needed for generative AI training, and generative AI (genAI) can help speed up the development and testing time of quantum systems. To illustrate, as genAI models become larger, the memory in classical GPUs may be insufficient to store the models, or loading data from memory may become slower. But quantum computing can mitigate this. Additionally, the required compute power to train the largest genAI models is likely to grow exponentially – classical compute may be unable to match this growth, but quantum can, given that its computing power scales exponentially.

⁷ Classiq, N.M. (2022, May 2). *Quantum computing promises to solve data center energy drain*.

⁸ Soller, H. (2025, June 23). *The Year of Quantum: From concept to reality in 2025*. McKinsey & Company.

AI tools like machine learning (ML) could improve the efficiency and scalability of quantum error correction.⁹ ML models trained on simulated datasets can identify and correct errors faster than traditional methods while needing fewer computational resources. ML models can also improve the accuracy of error prediction and offer predictive capabilities.¹⁰

Per McKinsey, genAI could unlock \$2.6-4.4 trillion annually across 63 new use cases when applied across industries. When combined, AI and quantum computing can complement each other, having a larger impact than the sum of the two.

A double-edged sword

Theoretically, quantum computers could break traditional cryptography

While quantum has its many benefits, the relationship between quantum computing and cybersecurity is a double-edged sword. Quantum tech can provide advancements in quantum communication (a method of exchanging information by encoding it into the quantum states of individual particles) but may pose threats to current encryption standards. Because quantum computers can break traditional cryptography, there is urgency for quantum security innovations. Currently, this issue remains theoretical, as existing quantum computers do not have the ability to undermine the encryption techniques commonly deployed.

Number of qubits to achieve this? 1 million

Shor's algorithm is a quantum algorithm for finding the prime factors of an integer, something which is computationally infeasible for classical computers. Widely used encryption schemes include RSA (Rivest-Shamir-Adleman; which relies on the difficulty of factoring large numbers) and elliptic curve cryptography (which relies on the elliptic curve discrete logarithmic problem for its security).

When implemented on a sufficiently powerful QC, Shor's algorithm could break these forms of encryption by exponentially reducing the time to find prime factors and expose vulnerabilities in typical encryption methods.¹¹ Shor's algorithm could be used to crack RSA keys of a commonly used size (2048 bits) in less than one week with around 1 million noisy qubits.¹²

Pursuing quantum-resistant algorithms now as a precautionary measure

This rationale behind starting to use quantum-resistant algorithms now is because it could take five to ten years to implement a new encryption standard.¹³ Additionally, once a powerful quantum computer becomes available, it might not be publicly known, which could enable malicious actors to decipher encrypted data, posing a risk to future security. And so precautionary measures may be required now to be prepared for these potential future scenarios.

"Tech wars" and sovereign quantum

A nascent technology in which many stakeholders have an interest

Quantum is the first new platform technology for computers since digital technology and many stakeholders have an interest in it for economic competitiveness, security, supply chain resilience or defense. Because of this, they may want to achieve "sovereign quantum" (where quantum capabilities are owned and operated by a particular nation) by investing in quantum, building out of their expertise or even exporting controls to hinder other stakeholders from developing sovereign quantum. Government quantum investment has reached at least ~\$42 billion to date.

The geopolitical race is on

At least nine countries implemented export controls on quantum technology in 2024.¹⁴ In terms of cumulative government investment in quantum tech (up to 2023), Europe is second behind China (at \$13.9 billion vs \$15.3 billion).

However, looking at private investment, over the past 20 years, most of the investment in quantum tech startups has been in companies based in the US, followed by the United Kingdom (UK), Canada and the European Union (EU). In 2024, US quantum companies raised 10 times the private investments collected by their European counterparts.

Additionally, over the past 20 years, China and the US have been the leaders in patent requests filed, but Europe has been in the lead in the number of patents granted. China may have trained the largest proportion (~25%) of the top quantum researchers at the undergraduate level but, in terms of employment, the largest proportion (one-third) of the top talent is now based in the US.

⁹ Tang, H., Wang, Z. (2024, December 29). *Artificial Intelligence for Quantum Error Correction: A Comprehensive Review*. Cornell University

¹⁰ Swayne, M. (2025, January 6). *AI For Quantum Error Correction: A Comprehensive Guide to Using Artificial Intelligence to Improve Quantum Error Correction*. Quantum Insider.

¹¹ Fortinet. (n.d.). *Understanding Shor's and Grover's Algorithms and Their Impact on Cybersecurity*.

¹² Gidney, C. (2025, May 21). *How to factor 2048 bit RSA integers with less than a million noisy qubits*. Cornell University.

¹³ Dargan, J. (2024, April 11) *Quantum Cybersecurity Explained: Comprehensive Guide*. Quantum Insider.

¹⁴ Groenewegen-Lau, J., Hmaid, A. (2024, December 12). *China's long view on quantum tech has the US and EU playing catch up*. Merics.

Quantum dictionary

- **Quantum computing:** A type of computing that uses qualities of quantum mechanics to solve certain problems faster than classical computers by leveraging quantum mechanical effects like superposition and entanglement.¹⁵ It uses sub-atomic particles to store information and superpositions for complex calculations. Because of this, a quantum computer can solve problems near instantaneously that would take a classical computer billions of years.
- **Qubits:** In other words – quantum bits – a quantum computer’s basic unit of information. In short, these units contain the quantum mechanical properties of superposition and entanglement. Without qubits, those properties could not be harnessed to create a quantum computer.
- **Decoherence:** Coherence is the ability of a quantum system to maintain a relationship between different states in a superposition. This property allows qubits to exist in a combination of states enabling the system to perform quantum operations.¹⁶ But this feature can be lost due to noise – ‘decoherence’ – where the system behaves more classically and loses its superposition and entanglement properties.¹⁷
- **Entanglement:** This refers to two or more quantum systems being linked in an unseparated bond, even if far apart. Any effect on one particle will instantly impact the other, faster than the speed of light, no matter the distance between them.
- **Modality:** The type of physical implementation or architecture used to create and manipulate quantum systems e.g., qubits. These modalities include superconducting qubits, silicon quantum dots, trapped ions, neutral atoms, photonic qubits and nitrogen vacancy centers.
- **Neutral atoms:** A quantum modality where atoms with a net electrical charge of zero are the foundation for qubits. This method uses lasers to trap atoms and manipulate the qubit states.¹⁸
- **Nitrogen vacancy center:** A quantum modality based on defects in diamond structures. In the process, a nitrogen atom and a vacancy (missing carbon atoms in the lattice structure) add an electron to a diamond lattice. Its quantum spin state and nearby carbon nuclei can be controlled with light.¹⁹
- **Noise:** Unwanted disturbances that affect quantum systems, leading to errors in quantum computations. Noise can arise from various sources such as interactions with the environment, electromagnetic interference and thermal fluctuations. Even small amounts of noise can lead to decoherence – when qubits lose their quantum properties. Quantum noise poses a barrier to developing large-scale, fault-tolerant quantum computers.²⁰
- **Photonic:** A quantum modality relying on the quantum properties of light. It uses photons as qubits to perform quantum calculations.²¹ This machine uses beam splitters (optical device that splits a beam of light into a transmitted and reflected beam) and phase shifters (device that alters the phase angle of a signal without changing its amplitude) to implement the qubit gates.
- **Physical vs logical qubits:** All present-day qubits are physical qubits – they are “noisy,” i.e., error-prone. Every possible solution has the same probability of being right as having no answers at all. Physical qubits would need to be connected and structured in a way that will provide enough error correction to each other to be considered “fault-tolerant” collectively. At this point, these qubits are called logical qubits.²²
- **Quantum advantage:** Quantum supremacy is where a quantum computer can perform a trivial calculation within a certain set of parameters, which is often not useful in the real world. Quantum advantage, on the other hand, is defined as a quantum computer solving a useful real-world problem faster than a classical computer. The challenge today is that quantum computers are too noisy where the qubit quality is not high enough yet to see quantum advantage.

¹⁵ Schneider, J., Smalley, I. (n.d.). *What is quantum computing?* IBM.

¹⁶ QuEra. (n.d.) *Coherence*.

¹⁷ Quandela. (n.d.). *Quantum Decoherence*.

¹⁸ Moore, J. (2025, March 28). *The 6 different types of quantum computing technology*. TechTarget.

¹⁹ Benjamin, S., Smith, J. (2011, October 3). *Driving a Hard Bargain with Diamond Qubits*. Physics Magazine.

²⁰ QuEra. (n.d.). *Quantum Noise*.

²¹ Moore, J. (2025, March 28). *The 6 different types of quantum computing technology*. TechTarget.

²² Classiq. (2022, July 19). *Quantum Cryptography – Shor’s Algorithm Explained*.

- **Quantum supremacy:** The point that quantum computer has a computational advantage by solving a problem that traditional computers could not solve in any feasible amount of time. There is no quantitative barrier, or calculation number to achieve quantum supremacy – it just refers to complex calculations that classical computers cannot do. In other words, proving that quantum computers have an embedded advantage over classical computers that cannot be gapped.
- **Scaling:** The scaling up of quantum computing hardware to build larger and more powerful quantum computers. To do this would involve overcoming the challenges of increasing the number and quality of qubits. Currently, we are in the noisy intermediate scale quantum era, meaning that quantum computers have several tens to a few hundred qubits and perform quantum operations with significant noise and errors that limit their capabilities.²³
- **Shor's algorithm** A quantum algorithm for finding the prime factors of an integer, something which is computationally infeasible for classical computers. When implemented on a sufficiently powerful quantum computer, Shor's algorithm could theoretically break widely used forms of encryption like RSA (Rivest-Shamir-Adleman; which relies on the difficulty of factoring large numbers) by exponentially reducing the time to e.g. find prime factors²⁴ and expose vulnerabilities in typical encryption methods.
- **Silicon quantum dots:** A quantum modality where 'artificial atoms' are made by adding an electron to a small piece of pure silicon and microwaves control the electron's quantum state.²⁵
- **Superconducting circuits:** A quantum modality in which electronic circuits create qubits. Microwave pulses manipulate the qubits' quantum states to run computations.²⁶ Specifically, a resistance-free current oscillates back and forth around a quantum loop. An injected microwave signal excites the current into superposition states.²⁷ The process involves having superconducting materials cooled to near absolute zero. It is the most mature modality with some of the largest quantum players in this field. This modality represents 35.7% of the quantum tech market.²⁸
- **Superposition:** Unlike classical computer, that only works on two possibilities (0 or 1, electricity is either on i.e., 1 or off, i.e., 0), superposition posits that a particle can be in more than one state at any given time: two states, more than two or even none. Superposition theoretically translates into endless possibilities and, as a result, endless calculations.
- **Trapped ions:** A quantum modality where quantum computers hold charged particles in an electromagnetic field. The confined particles are the qubits, which the system controls using lasers.²⁹

²³ Quandela. (n.d.). NISQ.

²⁴ Fortinet. (n.d.). *Understanding Shor's and Grover's Algorithms and Their Impact on Cybersecurity*.

²⁵ Simon Benjamin

²⁶ Moore, J. (2025, March 28). *The 6 different types of quantum computing technology*. TechTarget.

²⁷ Simon Benjamin

²⁸ OQC

²⁹ Moore, J. (2025, March 28). *The 6 different types of quantum computing technology*. TechTarget.

Contributors

Vanessa Cook

Content Strategist, Bank of America Institute

Lynelle Huskey

Analyst, Bank of America Institute

Sources

Haim Israel

Strategist, BofA Global Research

Lauren-Nicole Kung

Strategist, BofA Global Research

Felix Tran

Strategist, BofA Global Research

Martyn Briggs

Strategist, BofA Global Research

Wamsi Mohan

Analyst, BofA Global Research

Ruplu Bhattacharya

Analyst, BofA Global Research

Aisling Grueninger

Analyst, BofA Global Research

Joseph Leeman

Analyst, BofA Global Research

Ryan Choi

Analyst, BofA Global Research

Disclosures

These materials have been prepared by Bank of America Institute and are provided to you for general information purposes only. To the extent these materials reference Bank of America data, such materials are not intended to be reflective or indicative of, and should not be relied upon as, the results of operations, financial conditions or performance of Bank of America. Bank of America Institute is a think tank dedicated to uncovering powerful insights that move business and society forward. Drawing on data and resources from across the bank and the world, the Institute delivers important, original perspectives on the economy, sustainability and global transformation. Unless otherwise specifically stated, any views or opinions expressed herein are solely those of Bank of America Institute and any individual authors listed, and are not the product of the BofA Global Research department or any other department of Bank of America Corporation or its affiliates and/or subsidiaries (collectively Bank of America). The views in these materials may differ from the views and opinions expressed by the BofA Global Research department or other departments or divisions of Bank of America. Information has been obtained from sources believed to be reliable, but Bank of America does not warrant its completeness or accuracy. These materials do not make any claim regarding the sustainability of any product or service. Any discussion of sustainability is limited as set out herein. Views and estimates constitute our judgment as of the date of these materials and are subject to change without notice. The views expressed herein should not be construed as individual investment advice for any particular person and are not intended as recommendations of particular securities, financial instruments, strategies or banking services for a particular person. This material does not constitute an offer or an invitation by or on behalf of Bank of America to any person to buy or sell any security or financial instrument or engage in any banking service. Nothing in these materials constitutes investment, legal, accounting or tax advice. Copyright 2025 Bank of America Corporation. All rights reserved.