Transformation

Quantum dictionary, part 2: From potential to progress

02 November 2026

Key takeaways

- In the second and final part of our quantum dictionary series, we move beyond the basics to explore where quantum could go next. Today's quantum computers remain limited by noise and errors, but their potential grows rapidly as they scale. Emerging applications like quantum AI and sensing could eventually unlock new capabilities and significant economic value.
- Quantum communication could change both how we connect quantum computers and how we protect information. A quantum internet could use entanglement to link quantum systems, creating additional computing power, while quantum networks could make eavesdropping detectable and offer new ways to securely transmit information.
- Meanwhile, the race for quantum leadership is already underway. Governments are pursuing greater quantum sovereignty as the technology's potential implications for competitiveness, security and defense grow.

Assessing quantum's performance and progress

Quantum advantage versus supremacy

Quantum advantage is reached when a quantum computer can solve a useful, real-world problem faster than a classical computer. The problem is, today's quantum computers are still too noisy, as we discussed in part one of this series, and qubit quality isn't yet high enough to demonstrate quantum advantage.

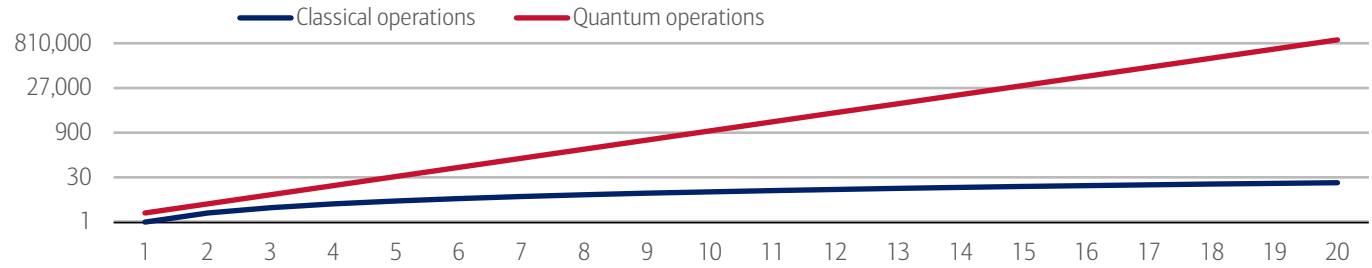
Quantum supremacy takes this one step further. It refers to the point when a quantum computer has computational advantage, meaning it can solve a problem that a traditional computer couldn't in any feasible amount of time.

Quantum scaling

Quantum scaling is about building bigger, more powerful quantum computers. It involves overcoming the challenges of increasing both the number and the quality of qubits. Today, we're in the noisy intermediate-scale quantum era. Quantum computers have tens to a few hundred qubits, but noise and errors still limit what they can do.[1]

However, when quantum computers do scale, they do so exponentially. Every additional qubit doubles the number of operations the system can perform. A quantum computer with just 10 qubits could perform more than 100 times the operations of a classical computer (Exhibit 1). More qubits could therefore mean more operations and, ultimately, more economic value in the industries where quantum computing can be put to work, according to BofA Global Research.

Exhibit 1: A quantum computer with just 10 qubits could perform more than 100 times the operations than classical
Number of classical versus quantum operations for a given (qu)bit number (log scale)



Source: BofA Global Research

BANK OF AMERICA INSTITUTE

[1] Quandela. (n.d.). *NISQ*.

Quantum Benchmarking Initiative

The Defense Advanced Research Projects Agency's (DARPA's) Quantum Benchmarking Initiative (QBI) aims to answer a big question: Is it possible to build a commercially relevant quantum computer by 2033? To be clear, QBI is not a competition between companies. DARPA evaluates all viable approaches for which funding is available.

QBI has three stages:

- Stage A: Start with a concept. At this stage, there is a utility-scale quantum computer concept that has a plausible path to realization in the near term.
- Stage B: Put a plan behind it. This stage involves developing a research and development plan, identifying the associated risks and introducing prototypes to overcome them.
- Stage C: Put it to the test. In the final stage, companies work with the government to verify and validate that the utility-scale quantum computer concept can be built as intended.

Exploring emerging quantum applications

Quantum AI

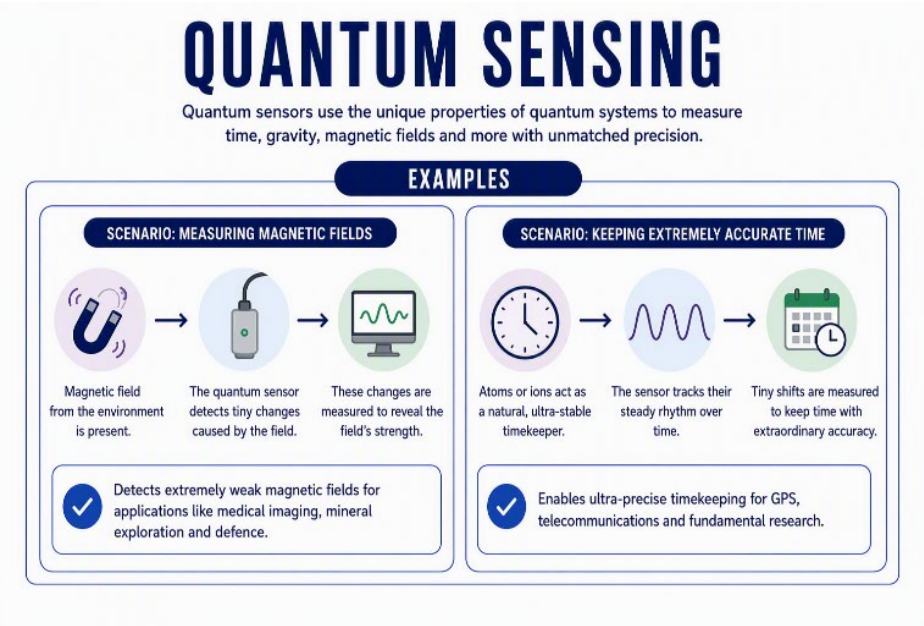
According to BofA Global Research, quantum AI brings together two powerful technologies: AI and quantum computing, with the potential to improve both the physical and the digital worlds. And the relationship could work both ways. Quantum computing could provide some of the compute power needed to train generative AI, while generative AI could help speed up the development and testing time of quantum systems.

AI tools like machine learning (ML) could also make quantum error correction (QEC) more efficient and scalable.[2] ML models trained on simulated datasets can identify and correct errors faster than traditional methods while using fewer computing resources. They can also more accurately predict errors before they happen.[3]

Quantum sensing

Quantum sensing uses the properties of quantum mechanics to measure things like magnetic fields, gravitational forces, time and rotation with greater precision than classical instruments (Exhibit 2).[4]

Exhibit 2: Quantum sensors use quantum properties to measure physical quantities with unmatched precision
An infographic of quantum sensing



Source: BofA Global Research

BANK OF AMERICA INSTITUTE

[2] Wang, Z. & Tang, H. (2024, December 29). *Artificial Intelligence for Quantum Error Correction: A Comprehensive Review*. arXiv.
[3] Swayne, M. (2025, January 6). *AI for Quantum Error Correction: A Comprehensive Guide to Using Artificial Intelligence to Improve Quantum Error Correction.* Quantum Insider.
[4] Rehman, M.U. (2026, March 2). *Understanding Quantum Sensing and Its Industrial Potential.* Quantum Insider.

So, how does it work? In simple terms, there are three steps. First, a quantum system is prepared in a well-defined initial state, for example, by cooling an atom to near absolute zero. Next, the sensor is exposed to whatever is being measured, causing a subtle shift in its quantum state. In an atomic magnetometer, for example, a magnetic field changes the energy levels of an atom's electrons, which changes how the atom absorbs or emits light. Finally, the sensor measures how much the quantum state has shifted, revealing the strength of the external force.[5]

Benefits and challenges

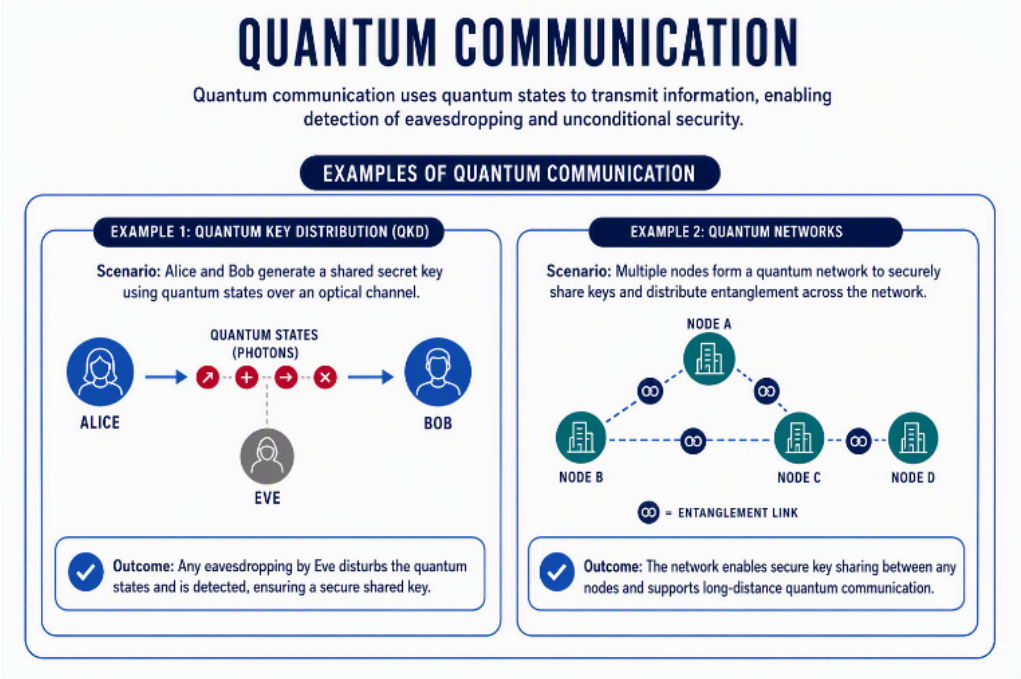
Compared with quantum computers, quantum sensors face some lower technical barriers. They don't need nearly as many qubits to be useful, entanglement can help but isn't required for every application, and even short coherence times can produce useful measurements.[6] The catch? They often require large vacuum chambers, laser systems and magnetic shielding to maintain coherence.

The quantum internet and communications

Quantum communication

Quantum communication is the study of how information can be encoded and transmitted between quantum systems over a distance (Exhibit 3). It uses properties like superposition and entanglement to enable the secure transmission of information. Why does that matter? One of the main goals is to keep information secure from potential eavesdroppers, particularly as more powerful quantum computers could pose new challenges for traditional communication methods. The ultimate goal is what some call the quantum internet, where quantum signals can move seamlessly across many quantum networks.[7]

Exhibit 3: Quantum communication uses quantum states to encode and transmit information
An infographic of quantum communication



Source: BofA Global Research

BANK OF AMERICA INSTITUTE

Quantum internet

Think of the quantum internet as a scalable network that allows two or more quantum devices to exchange information (Exhibit 4). These connections could span vastly different distances, from within a silicon chip all the way to satellite links.[8]

But the quantum internet isn't meant to replace the internet we use today, nor is it simply a faster version of it. According to Cisco, the classical internet can move information between computers, but it is ultimately limited by what those computers can compute. Some problems become so complex so quickly that no classical machine can solve them in a useful amount of time.

[5] Ibid.
[6] Ibid.
[7] Quantinuum. (2024, July 30). *Coming Over the Horizon: Quantum Communication Enters the Mainstream.*
[8] Imperial. (n.d.). *Quantum Internet.*

When connection becomes computation

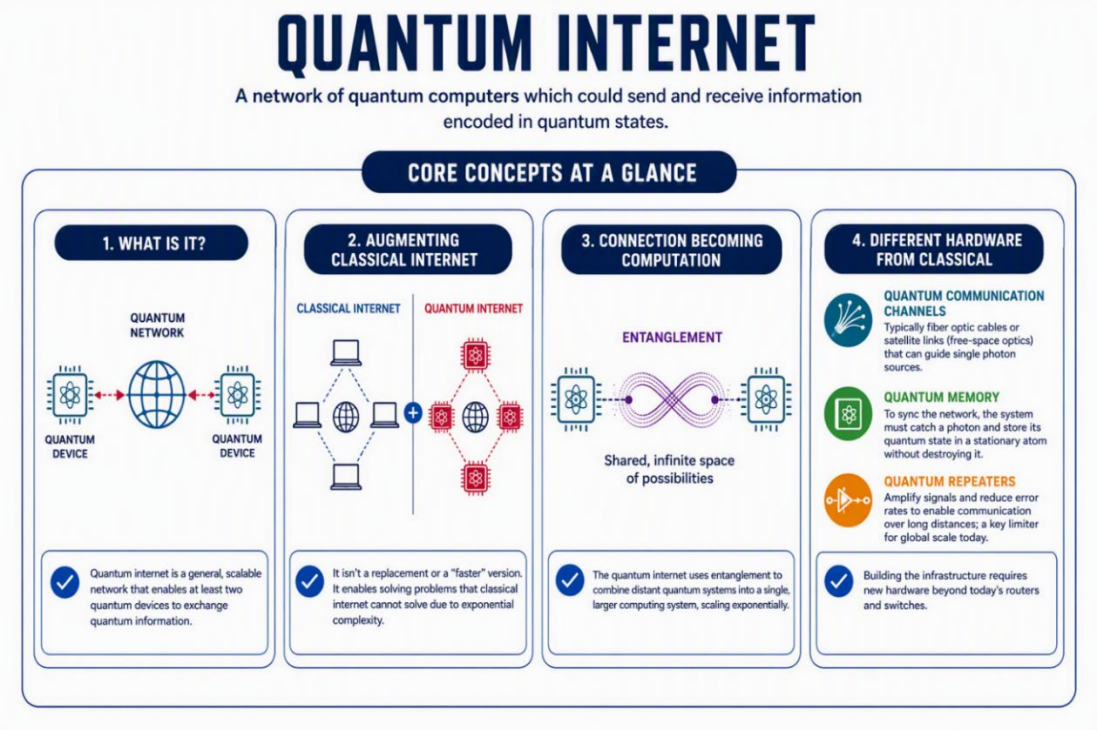
Here's what makes the quantum internet different: the connection itself can create new computing power. Using entanglement, a quantum network can connect quantum systems into a single, larger computing system that scales exponentially.[9] That's fundamentally different from classical computers, which communicate by passing copies of information back and forth. Quantum computers connected through a quantum network can instead create a feedback loop of entanglement and a shared space of possibilities that neither could produce on its own.

Different hardware from classical

Building a quantum internet requires a different set of hardware than the routers and switches that power today's internet. Key pieces include:[10]

- Quantum communication channels: These carry quantum signals, typically through fiber-optic cables or satellite links using free-space optics.
- Quantum memory: To keep the network in sync, the system must catch a photon and store its quantum state in a stationary atom without destroying it.
- Quantum repeaters: These help quantum signals travel longer distances by amplifying signals and reducing error rates. According to QuEra, the lack of viable quantum repeaters is currently a key limitation to building a global quantum network.

Exhibit 4: A network of quantum computers which could send and receive information encoded in quantum states
An infographic explaining the quantum internet



Source: BofA Global Research

BANK OF AMERICA INSTITUTE

Quantum networking

Quantum networking is a way of sending information using quantum states. It generally includes three network types: quantum key distribution (QKD) for secure communications (more on this below), the quantum internet for distributed quantum computing, and quantum sensing networks that use entanglement to improve measurements.

Classical networks turn information into electrical or optical signals that can be copied or intercepted without the sender or receiver knowing. Quantum networks work differently. Because information is transmitted using quantum states, it cannot be

[9] Chan, M. (2026, June 1). *Quantum internet 101: What it is, and why it matters.* Cisco.
[10] QuEra. (n.d.) *Quantum Internet.*

intercepted and copied without disturbing the original information. That disturbance makes an eavesdropping attempt detectable.

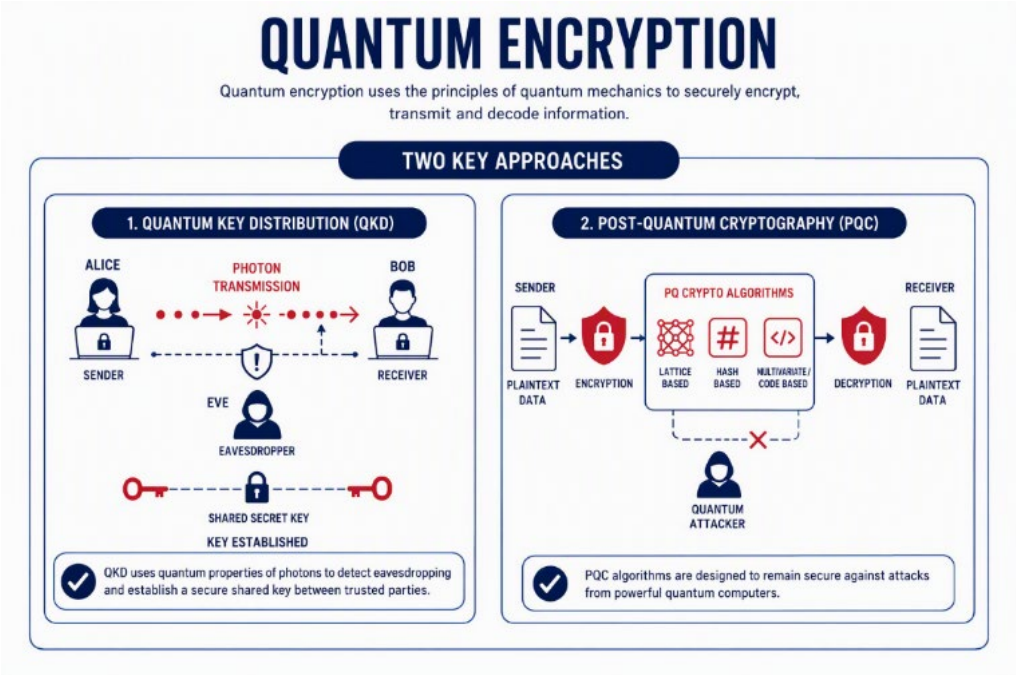
Evaluating security & strategic risks

Quantum encryption

Quantum encryption uses the principles of quantum mechanics, including superposition and entanglement, to encrypt and securely transmit data (Exhibit 5).

One potential risk of quantum computing is that it could eventually break widely used forms of encryption. And while large-scale quantum computers are still being developed, organizations may need to start preparing for that possibility today.

Exhibit 5: Examples include quantum key distribution and post-quantum cryptography
An infographic illustrating quantum encryption



Source: BofA Global Research

BANK OF AMERICA INSTITUTE

Quantum key distribution

Quantum key distribution (QKD), a type of quantum encryption, uses the laws of quantum physics to create and distribute secure keys which prevent data decryption.[11] Think of a key as something that locks and unlocks a digital message. Two parties share a key to encrypt and decrypt information sent between them. If an eavesdropper tries to obtain the key, the attempt disturbs the quantum states, alerting the parties that the key may have been compromised and shouldn't be used.[12]

According to Quantum Insider, QKD generally involves three steps:[13]

- Create entangled photons: First, a quantum source, such as a laser and nonlinear crystal or a quantum dot, generates pairs of entangled photons. The photons are correlated in ways that classical light cannot replicate, so measurements of one reveal information about its partner.

- Send the photons: The photons travel to different locations through fiber-optic cables or free-space optical channels, such as satellite-to-ground or satellite-to-satellite links, while maintaining their quantum correlations. But those connections can be lost over long distances, with current systems reaching roughly 100 kilometers, according to Quantum Insider.[14] Classical networks get around distance limitations with repeaters that receive, amplify and retransmit signals.

[11] Toshiba. (n.d.). *Quantum Key Distribution (QKD).*
[12] QuEra. (n.d.). *Quantum Key Distribution.*
[13] Rehman, M.U. (2026, March 9). *Understanding Quantum Networking and Its Industrial Potential.* Quantum Insider.
[14] Ibid.

Quantum signals can't simply be amplified without destroying their quantum properties, so quantum repeaters take a different approach. They use entanglement swapping and quantum memory to extend the range of quantum networks.

- Measure the photons: Finally, the photons are measured at each location. This confirms whether the entanglement survived the journey and can reveal whether someone tried to intercept the photons along the way. The results can then be used to generate a shared secret key for encrypting classical messages.

Quantum sovereignty

Quantum sovereignty is an economic actor's ability to develop, produce and operate its own quantum technology.

Quantum is the first new computing platform technology since the arrival of digital computing. And the stakes are high. Stakeholders are interested in quantum because of its potential implications for economic competitiveness, security, supply chain resilience and defense. As a result, some may pursue "sovereign quantum," meaning quantum capabilities are owned and operated by a particular nation. That could involve investing in quantum technology, building domestic expertise or even export controls to limit other stakeholders' ability to develop their own sovereign capabilities.

The geopolitical race is on

Government quantum investment has reached at least about $58 billion cumulatively as of 2025, led by Europe at $15.4 billion and China at $15.3 billion.

The competition extends beyond investment. At least nine countries implemented export controls on quantum technology in 2024. Over the past 20 years, China and the US have led in patent requests filed, but Europe and China have led in the number of patents granted. The race for talent is global, too. China has trained the largest share of top quantum researchers at the undergraduate level, at roughly one-fourth, while the US is home to the largest share of top talent by employment, at one-third.

Quantum supply chain

Building quantum technology requires much more than qubits. A broader supply chain provides the equipment, components and materials needed to make quantum systems work, including:

- Cryogenics: Most types of qubits require some level of extreme cooling, with superconducting qubits among the most demanding at roughly 5–10 millikelvin. Keeping qubits this cold helps shield them from environmental noise that can cause decoherence.

- Qubit control electronics: Quantum gates direct qubits by sending them photons. That requires supporting electronics, including wiring, room-temperature electronics and amplifiers. For example, analog microwave signals used to read qubits must be amplified through several stages before they can be converted into digital signals and analyzed.

- Photonics: Lasers use light and atoms to help power quantum technology, while other devices can modify properties of photons, such as their path and polarization.

- Foundries: Quantum development also relies on several types of fabrication facilities, including research fabs at national research organizations and universities, pre-industry research fabs, independent foundries that manufacture semiconductors for third parties, and in-house fabs operated by quantum technology vendors.

- Raw materials: Quantum systems also depend on materials used in qubits themselves and in supporting components such as cables and cryostats. Helium-3 and helium-4 are used in cryostats to maintain very low temperatures, while rare earth metals used in quantum technology include yttrium, neodymium, europium, erbium and ytterbium.[15]

AI singularity

AI singularity refers to a hypothetical point when AI evolves to become self-improving and autonomous, surpassing human cognitive abilities.[16]

A complementary relationship between quantum and AI

Rather than developing in isolation, AI and quantum computing could ultimately help advance each other. Quantum computing may eventually provide some of the compute power needed to train generative AI, while generative AI could help speed up the development and testing of quantum systems.

[15] Swayne, M. (2025, October 15). *Rare-Earth Minerals And Quantum Computing: How Secure Are The Supply Chains?* Quantum Insider.
[16] ISB. (2025, March). *What is AI Singularity? Explore Its Future Impact.*

That relationship could become increasingly important as the computing power needed to train the largest generative AI models continues to grow exponentially. Classical computing may eventually struggle to keep pace, while quantum computing could help meet some of that demand because its computing power also scales exponentially.

By 2045? 2029? Now?

AI is becoming increasingly powerful and capable, raising a big question: when could it reach or even surpass human intelligence? Futurologist Ray Kurzweil expects AI to reach human levels of intelligence by 2029 and technological singularity by 2045. His view extends Moore's Law beyond processing power to other forms of technological progress.

Under that framework, computing power would continue growing exponentially. By 2045, Kurzweil projects that $1,000 worth of computing could perform as many calculations in one second as all human brains combined.

Contributors

Lynelle Huskey

Analyst, Bank of America Institute

Vanessa Cook

Content Strategist, Bank of America Institute

Sources

Haim Israel

Equity Strategist, BofA Global Research

Lauren-Nicole Kung

Equity Strategist, BofA Global Research

Martyn Briggs

Equity Strategist, BofA Global Research

Felix Tran

Equity Strategist, 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 2026 Bank of America Corporation. All rights reserved.