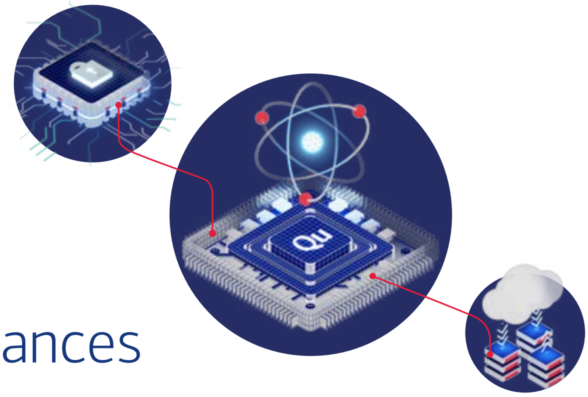
BANK OF AMERICA



BREAKTHROUGH TECHNOLOGY DIALOGUE ASIA PACIFIC 2025

Quantum technology: On the cusp of world-changing advances

The promise of quantum technology is a paradigm shift in computing power, communications and cryptography. We are not there yet — but scientists and investors alike are increasingly positive about a quantum future.

Key takeaways:

- Quantum technology uses the principles of subatomic science. It has the potential to make great strides forward in computing, communication, cryptography and drug discovery, among other things.
- Quantum computing uses principles different to those in classical computing. By using qubits, which can hold numerous states simultaneously, multiple calculations become possible, increasing processing power and enhancing the speed and efficiency of AI algorithms.
- Quantum has great potential in communications, too, because of the level of encryption it can achieve.
- But this power brings a threat when — on a date known as Q-Day — quantum computers will be able to crack all existing encryption. So as the technology advances, so, too, do preemptive measures to protect against it.

Quantum technology seeks to harness the principles of quantum mechanics: the way that nature behaves at the very smallest, subatomic scale. In doing so, it marks a key shift in the way we interact with the world. It has the potential to be a game-changing technology across computing, communications, cryptography and even drug discovery.

Quantum can be the rocket fuel that propels artificial general intelligence beyond its existing ceilings, because it should bring advances in processing power that are beyond that of classical computing. And in 2025, the United Nations' International Year of Quantum Science and Technology,[1] it is front of mind among breakthrough technology investors.

"I believe we are making tremendous progress in quantum hardware," says one such investor, Tony Fadell, principal, Build Collective, speaking at Bank of America's Breakthrough Technology Dialogue in Singapore in February 2025.

> *"The makers of these machines are asking people to come up with applications to run on them because they're going to be so powerful our brains have not yet figured out how to utilize all this computational power.*

Tony Fadell, Build Collective, joined virtually.

Quantum computing is the focus, though not the entirety, of quantum technology advancement today. It operates on principles fundamentally different from those in classical computing, which use bits — 0s and 1s — to process information. Quantum computers instead use qubits, which can exist in a state of superposition, meaning they hold numerous states simultaneously.

The outcome of this is that they can perform multiple calculations at once, exponentially increasing their processing power. That, in turn, can enhance the speed and efficiency of AI algorithms, with implications from self-driving cars to advanced robotics, healthcare to finance.

Timelines and milestones

The timeline for achieving a commercially viable and practically useful quantum computer is a topic of intense debate. Projections vary from the end of the decade to 20 years from now, though some developers have made significant breakthroughs in the number of qubits that can be assembled in a system.[2]

Quantum technology: On the cusp of world-changing advances

Today, the largest such successful assembly stands at just over 1,000 qubits.[3] While that sounds good, it is still relatively nascent, not yet a level that creates widespread commercial use cases that a classical computer could not achieve.

“As capability grows, we should watch for three milestones,” says Gerald Mullally, CEO of quantum technology developer Oxford Quantum Circuits (OQC).[4] These milestones are measured by the number of quantum operations that can take place in a system before errors dominate.

At a rate of one million quantum operations, Mullally says, “We’ll be able to have small-scale, narrow-based advantage in certain use cases for quantum over classical compute.”

That might, for example, include cases in the financial services sector, which suffers around a trillion dollars of fraud per year. Mullally says quantum algorithms have already been devised that give a 15% increase in the ability to detect fraud above the best of classical computing.

> *Now what we need is a computer system that is powerful enough to run that algorithm.*

Gerald Mullally, OQC, sees three quantum milestones.

This capacity, he thinks, is three to five years away.

At the second stage, a billion quantum operations, one of the areas with the clearest practical utility is drug discovery. Pharma companies spend a lot of time and money testing potential drugs and would be greatly assisted by being able to simulate the interaction of molecules with sharper precision.

Classical computers are limited in their capacity to do this, whereas quantum computers, with their ability to perform multiple calculations simultaneously, will offer an edge. In doing so, they will make it more likely that pharma companies focus on breakthrough medications that have a greater chance of success.

Dr. Simone Fishburn, VP and editor in chief at BioCentury Inc., explains:

> *Quantum matters because it takes 10 to 13 years to make a drug and costs about $2 billion, and built into that is a tremendous amount of failure: Most drug candidates don’t work.*

And she adds: “So the point is to increase the number of shots on goal, so you’re spending less time on all those molecules that don’t work.”

Dr. Alexander Zhavoronkov, founder and CEO of Insilico Medicine, has begun using quantum technology already to test hypotheses around molecule interaction.[5]
He states:

> *Now we need to be able to scale the number of qubits for us to go from proof of concepts to actual clinical trials. Doing so will enhance the possibility of success and reduce the cost in achieving it.*

Dr. Alexander Zhavoronkov, Insilico Medicine, explains his use of quantum technology.

Communication, coding — and a threat

The third phase, at a trillion quantum operations, ought to bring us close to what is known as Q-Day:[6] the point at which quantum computers can break all existing encryption algorithms.

At this point, it is useful to take a step back and consider quantum’s potential in secure communications. This builds upon a property called entanglement, which means that there are correlations between two quantum particles no matter how far apart they are.

Quantum technology: On the cusp of world-changing advances

This technology is called Quantum Key Distribution (QKD). Prof. Alexander Ling, principal investigator, Centre for Quantum Technologies at the National University of Singapore, says:

> “
> *We can use this for encryption purposes to build a more secure communications network.*

Prof. Alexander Ling, National University of Singapore, explains QKD.

Much of the work in this field takes place in space, using satellites. If an entangled photon source on a satellite is linked to two photons on the Earth's surface, an unbreakable level of encryption can be affected, andany attempt to hack it instantly detected.

China leads the world in this satellite communication endeavor, first achieving quantum communication with its Micius satellite launched in 2016.[7] Today, the Deep Space Quantum Link, developed by the NASA Jet Propulsion Laboratory, is developing the use of QKD at deep space distances.[8] Ling's center in Singapore is working on achieving similar outcomes to Micius on shoebox-sized satellites.[9]

The ability to develop secure cryptography on this scale has a regrettable flip side: the ability to crack codes, which brings us back to Q-Day — which may be close at hand (the Global Risk Institute, consulting leading experts in a 2023 study, calculated a 31% chance that Q-Day would arrive within a decade: by 2033).[10]

The Shor algorithm[11] tells us that if you have a really powerful, fault-tolerant computer, you can break the codes that we use today," Ling says. This brings us into the realm of national security, and the need to protect against the misuse of a technology even before that technology is fully developed.

In Singapore, even as quantum research develops, work is underway in parallel on a National Quantum-Safe Network,[12] which seeks to preserve the security and integrity of systems in a quantum age.

> “
> *In Singapore, we have the ambition to be quantum-safe in 10 years.*

says Dr. Ong Chen Hui, assistant CEO of Singapore's Infocomm and Media Development Authority (IMDA) Biztech Group. Ling already speaks of developing "post-quantum cryptography."

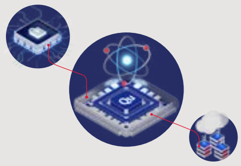
Dr. Ong Chen Hui, IMDA, Biztech Group, outlines Singapore's quantum-safe future.

A quantum future

While quantum technology will be so powerful that it brings security and even geopolitical questions to bear, it is important to consider the many potential positives. Beyond drug discovery and communications, quantum computers can help banks with credit scoring and derivative pricing, energy companies with battery technology, the automotive and logistics industries with efficiency.

"Imagine a motorsport team trying to improve the performance of their car in a wind tunnel," says Mullally. "They've got 50,000 data points on that car, and changing any one impacts many more. That's too complex for a classical computer, but a quantum computer will be able to assimilate the information and model it."

Chris Wright, Resonate Global, **Prof. Alexander Ling,** National University of Singapore, and **Gerald Mullally,** OQC, untangle quantum technology.



There is also an important energy perspective. Quantum computers use relatively little power compared to a classical supercomputer, which has implications for data centers, for example.

Quantum brings many logistical challenges: Some methods of building these computers require temperatures colder than space, while all of them battle with overcoming the inherent instability of asking qubits to work collectively.

But no matter how mind-bending the science behind it all, at heart, a quantum system is a replication of nature. “Richard Feynman, the Nobel laureate physicist, famously said about synthetic biology: Why would you want to use a classical computer to simulate a quantum system?” says Tony Fadell. “He also said: What I cannot create, I cannot understand.”

1. 2025 International Year of Quantum Science and Technology – see official site: https://quantum2025.org

2. For example: *Microsoft’s Majorana 1 chip carves new path for quantum computing*, Catherine Bolgar, Microsoft News, February 19 2025. https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/#:~:text=Microsoft%20today%20introduced%20Majorana%201,and%20societal%20problems%2C%20Microsoft%20said

3. *Record-breaking quantum computer has more than 1,000 quibits, Alex Wilkins, NewScientist, 24 October 2023*: https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/ and *IBM Releases First-ever 1,000-Qubit Quantum Chip*, Davide Castelvecchi & Nature Magazine, Scientific American, December 5 2023: https://www.scientificamerican.com/article/ibm-releases-first-ever-1-000-qubit-quantum-chip/

4. OQC was the first company in the world to deploy a quantum computer to a commercial data centre including the integration with high performance compute. See company website: https://oqc.tech/company/

5. *Quantum-computing-enhanced algorithm unveils potential KRAS inhibitors*, multiple authors including Alex Zhavoronkov, Nature.com, 22 January 2025: https://www.nature.com/articles/s41587-024-02526-3

6. Wired’s analysis of Q-Day explores some complex issues. *The Quantum Apocalypse Is Coming. Be Very Afraid.* Amit Katwala, Wired, March 24 2025: https://www.wired.com/story/q-day-apocalypse-quantum-computers-encryption/

7. *China Reaches New Milestone in Space-Based Quantum Communications*, Karen Kwon, Scientific American, June 25 2020: https://www.scientificamerican.com/article/china-reaches-new-milestone-in-space-based-quantum-communications/

8. *The deep space quantum link: prospective fundamental physics experiments using long-baseline quantum optics*, multiple authors, EPJ Quantum Technology, 8 October 2022: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-022-00143-0

9. *Quantum satellite device tests technology for global quantum network*, NUS News press release, June 3 2016: https://news.nus.edu.sg/quantum-satellite-device-tests-technology-for-global-quantum-network/

10. *2023 Quantum Threat Timeline Report, Global Risk Institute*, December 22 2023: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

11. *Toward a code-breaking quantum computer*, Adam Zewe, MIT News, August 23 2024: https://news.mit.edu/2024/toward-code-breaking-quantum-computer-0823#:~:text=Quantum%20computers%2C%20on%20the%20other,feasible%20to%20implement%20in%20practice

12. National Quantum-Safe Network Singapore – official site: https://www.nqsn.sg