



Quantum computing will not replace classical financial calculation, it will rather complement it in very specific applications



Access to this technology will be highly concentrated amongst a few players and conditioned by the industrial policies of the major geopolitical blocs



The standardization and opacity of models, coupled with a direct threat to banking cryptography, will require a regulatory and infrastructure response that cannot wait for the technology to mature

QUANTUM FINANCE: A RACE FOR CONTROL OF QUANTUM COMPUTING

Manuel AYALA LÓPEZ
Jaime CABOTÁ JIMÉNEZ
Raúl VIÑAS ABADÍA

Afi

The competitive advantage of quantum computing will depend not only on technological progress, but also on who has access to it and their ability to harness its potential

The future of quantum computing in banking and financial markets will be determined less by technological development than by the conditions governing access to computing capacity. Quantum computing will be incorporated into financial calculations in specific applications (derivatives valuation, portfolio optimization, payment settlement), but access to this technology will be highly concentrated amongst a small number of players with sufficient resources to conduct experiments over many years. This concentration (rather than the technology itself) will determine who benefits from the market advantages and who bears the risks: standardization of models, opacity and a direct threat to banking cryptography. In the coming years, a "quantum moment" that revolutionizes technology is not expected, but rather gradual advances in post-quantum infrastructure and regulation. The decisive factor lies in which organizations start preparing to manage its distribution and associated risks.

Concentrate before transforming

Logic suggests that a revolutionary technology replaces existing processes. In the short to medium term, however, quantum computing will operate in symbiosis with traditional procedures, wherever highly complex problems need to be solved.

The leap to quantum technology currently faces a physical limit. Quantum computers are extremely sensitive to their environment, which causes a loss of information

known as decoherence; the resulting errors accumulate to the point of limiting the size of the problems that can be reliably solved.

Access to this technology is not expected to be uniform due to the significant entry barriers it presents. High hardware costs and a shortage of specialized talent capable of combining financial and computational expertise will concentrate the advantage in the hands of a small number of players, many of whom are major technology firms and financial institutions with sufficient resources to experiment without an immediate return. It is this disparity in access rather than the pace at which *hardware* advances that will determine which players capture the market advantages and which are exposed to its risks.

It could be argued that worrying today about the allocation of a capacity that does not yet exist is getting ahead of ourselves. This may be true for modelling, but not for cryptography, where what is encrypted today is already at risk, nor for dependence on suppliers, which develops over years of experimentation.

What quantum computing brings to finance

The potential of quantum computing lies in analyzing a very large number of alternatives and finding the most efficient combinations amongst them, such as valuing complex derivatives more quickly, or optimizing portfolios with a number of constraints that is currently unmanageable.

In a paper published in 2022, researchers from the Bank of Canada, in collaboration with D-Wave, applied a hybrid quantum annealing algorithm to thirty days' worth of non-urgent payments within the Canadian system. [By reordering the payments into batches of seventy, the average daily liquidity saving was 240 million Canadian dollars, out of a daily allocation by the system of between 15 and 20 billion, and exceeded 1 billion on some days in the sample.](#)¹ The cost of this improvement was an average delay of 90 seconds in settlement, attributable almost entirely to the time required to aggregate each batch, as the algorithm took five seconds to solve the problem.

Extrapolated to the sector, this could translate into a more efficient allocation of capital and liquidity and near real-time risk measurement. The implementation will consist, at least initially, of hybrid systems, but the underlying significance is considerable, because problems that currently must be simplified due to a lack of computational capacity would be able to accommodate an unprecedented number of variables.

In the markets, the advantage lies in methods rather than power. In a traditional Monte Carlo simulation, halving the margin of error requires, approximately, quadrupling the number of simulations needed. Under ideal conditions, some quantum algorithms could achieve the same improvement by merely doubling the number of queries to the quantum system, thanks to a technique known as quantum amplitude estimation. Quantum computing would thus enable the analysis of more

scenarios using the same resources, or the attainment of a more precise estimate within the same timeframe.

The experiment announced by HSBC and IBM in September 2025 achieved this advantage through a different approach. [Rather than speeding up a calculation, the team used quantum circuits to transform the input data and feed it into conventional statistical models, to estimate the probability that a corporate bond quote would ultimately result in an executed trade.² Using real data from the European corporate fixed-income market, predictive accuracy improved by up to 34 per cent compared with the traditional techniques the bank uses as a benchmark.³](#)

That advantage, however, has an expiry date. In competitive markets, any predictive improvement is eroded as soon as several participants gain access to a similar technique, as prices adjust and the margin disappears. The real difference lies in converting that early access into proprietary models and processes that are difficult to replicate before the advantage is diluted.

Providers, banks and states: Who controls quantum capacity

Three players take part in the quantum race: technology providers, which control the infrastructure; financial institutions, which accumulate applied knowledge; and states, which set the rules for the technology.

Providers such as IBM, Google and D-Wave dominate both the hardware and the development environments upon which the first financial algorithms are built. Due to cost and specialization, most organizations will not build their own quantum computers, just as they do not develop their own AI models. They will access them via the cloud or collaboration agreements, which reduces the initial investment but transfers control of a strategic resource to a handful of suppliers capable of influencing the market and setting the pace for the sector. JPMorgan's case illustrates this. [Despite having one of the most advanced quantum teams in banking, it has had to rely on Quantinuum's computers and take a stake in the company, leading funding rounds of \\$300 million in 2024 and nearly \\$600 million in 2025, to secure a position in the supplier it depends on.⁴](#)

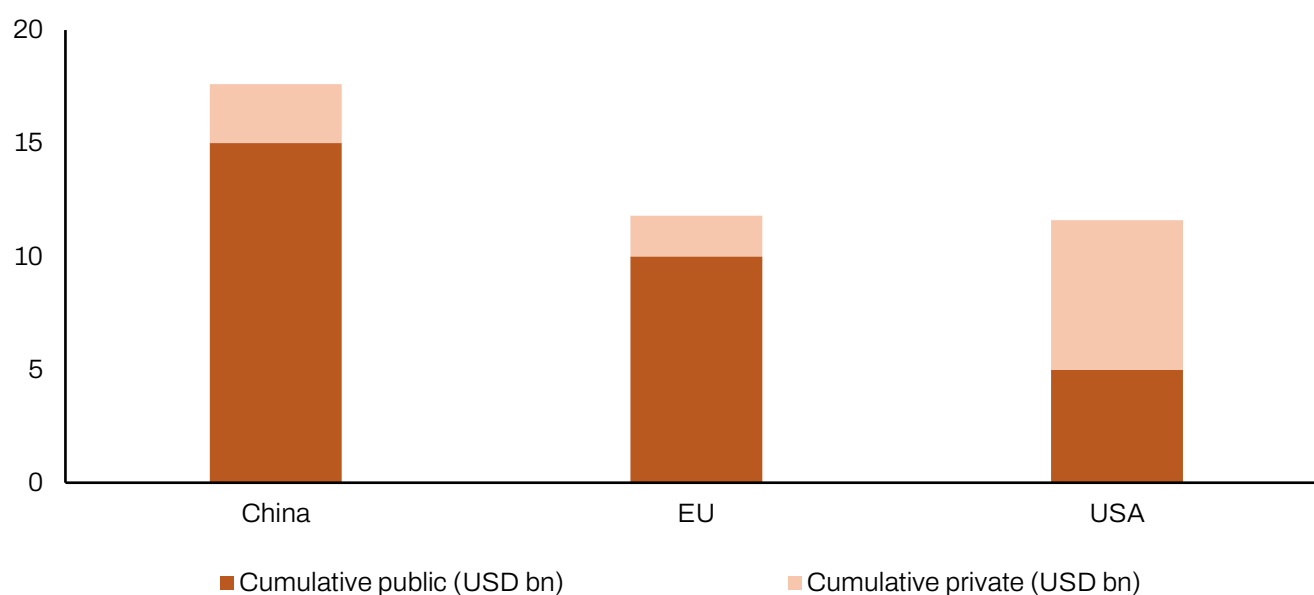
Financial institutions such as JPMorgan, Goldman Sachs and HSBC are already experimenting with this technology. Learning to translate financial problems into quantum models and to integrate them into environments subject to strict risk controls generates a body of knowledge which, regardless of access to hardware, separates early adopters from those who will adopt the technology once it has matured.

States, led by the U.S., China and the EU, have incorporated quantum technology into their industrial policies to attract investment and talent and to develop their own suppliers. That intervention is already shaping the market. Since 2024, the U.S. has required export licenses for quantum computers exceeding certain thresholds for qubit count and error rates, while the EU has applied similar controls since November

Three key actors shape the quantum race: technology providers, which control the infrastructure; financial institutions, which develop expertise in their practical applications; and governments, which establish the regulatory framework

2025. In May 2026, the U.S. government also proposed investing \$2 billion in minority stakes in nine quantum companies, likewise seeking a position in its suppliers. For a European institution accessing a U.S. computer via the cloud, the conditions of access also depend on that export remaining permitted.

Figure 1 - Public and private investment in quantum computing up to March 2025



Source: [ECIPE, Benchmarking Quantum Technology Performance \(March 2025\)](#).⁵ The private investment figures are our own calculation based on the percentages in the report.

Systemic risk: Homogenization, opacity and security

If access to algorithms and infrastructure remains concentrated amongst a few providers, banks and funds could end up using similar tools. If those models interpret a disruption in the same way, different institutions could simultaneously reduce their exposure to certain assets. This simultaneity amplifies the movement that triggered it: coordinated selling pushes prices down, seemingly confirming the signal issued by the models and reinforcing the incentive to continue selling. What begins as a model interpretation ends as a market crash.

The problem is compounded by the fact that every model relies on historical data and assumptions that may cease to be valid during a period of uncertainty. If several institutions use the same tool, an erroneous estimate can spread through the market and affect numerous institutions simultaneously. This is why validating these models will be even more important than with classical ones.

And that validation will not be easy. Quantum algorithms return probabilistic results that are not reproduced identically by two successive runs, and their internal behavior does not allow for a step-by-step inspection equivalent to that of a classical calculation. This complicates both internal auditing and supervisory review in a sector where every relevant decision must be capable of being explained and reconstructed, and where the levels of traceability required of a quantum model have not yet been defined.

The most pressing risk, however, concerns information security: a sufficiently powerful quantum computer could undermine some of the public-key cryptography used for key exchange, user authentication and the verification of digital certificates and signatures

The risks above depend on institutions adopting quantum algorithms. Security, by contrast, affects them even if they never use them, and it is the most immediate. A sufficiently advanced quantum computer could compromise some of the public-key cryptography used to exchange keys, authenticate users and validate digital certificates and signatures. In August 2024, the U.S. National Institute of Standards and Technology (NIST) approved the first three post-quantum cryptography standards, designed to gradually replace the algorithms that currently protect key exchange and digital signatures. Migration cannot wait until a computer capable of carrying out such attacks exists, not least because information encrypted today may be stored for decryption in the future, a strategy known as *harvest now, decrypt later*. The pace of this migration will depend on the timetables set by regulators in each country, which links this risk to the state-led race described earlier.

In all cases, the systemic risk stems not only from an individual failure, but also from reliance on the same tools and the spread of vulnerabilities across a closely interconnected financial system.

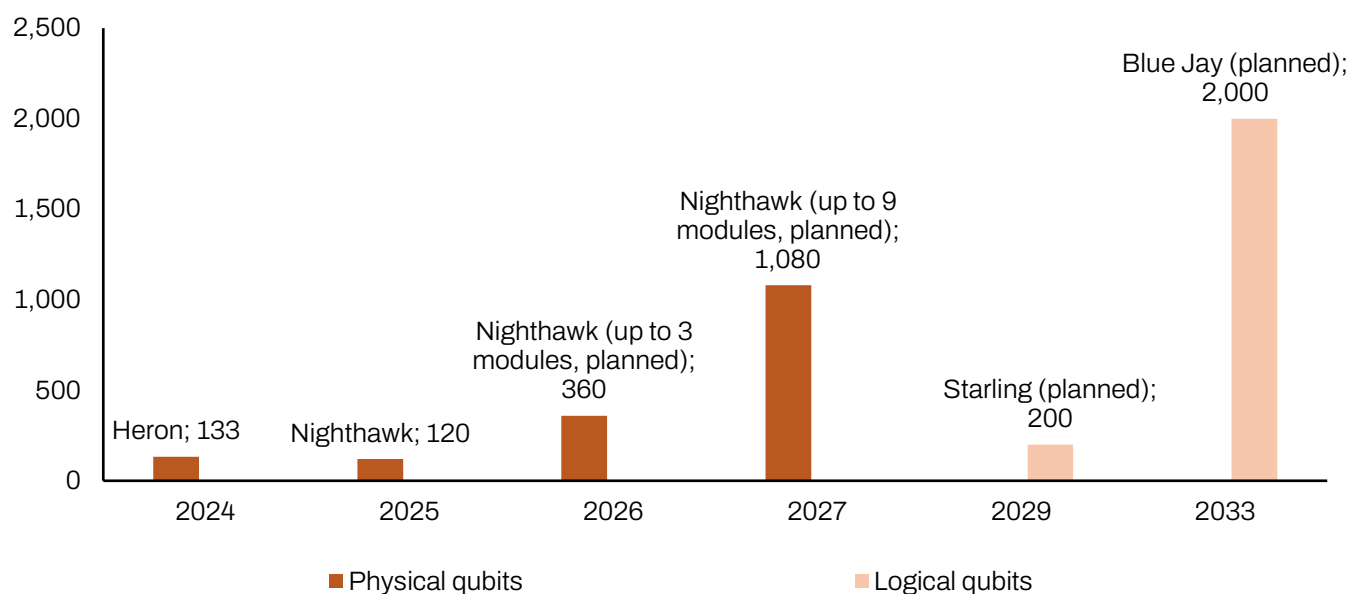
What to expect in the coming decade

[In the field of cryptography, the European Union has set the end of 2030 as the deadline for migrating critical financial systems to post-quantum standards, with a full transition expected by 2035.](#)⁶ The United States has gone further: an executive order issued in June 2026 brought forward the deadline for the establishment of keys in high-value federal systems from 2035 to 2030, and that for digital signatures to 2031, extending the requirement to its contractors.

[In terms of hardware, IBM estimates that processors with thousands of qubits and sufficient error correction to run applications currently in the proof-of-concept phase will be available between 2029-2033.](#)⁷ If this timetable is met, the key question will not be whether access will continue to be via the cloud, something that is already the case today, but under what conditions. One scenario would open this access to a wide range of organizations on competitive terms; the other would keep commercial exploitation concentrated amongst the same providers that already dominate hardware and cloud services, reserving the best terms for selected clients through closed agreements.

The timeline matters less than the position from which each organization approaches it, and that position depends on decisions that can be taken now. Classifying which information requires long-term protection, assessing the extent to which the organization relies on external suppliers before that reliance becomes structural, or establishing its own criteria for validating any quantum model that is adopted are steps that do not require waiting for the technology to mature.

That is the difference between adopting technology on someone else's terms or doing so on one's own. Quantum computing can improve risk management, but it does not eliminate its institutional dimension. **FI**

Figure 2 - Evolution of physical qubits in IBM quantum processors / (2024-2033)

Source: IBM Quantum, official roadmap.

References

1. Bank of Canada — McMahon, C., McGillivray, D., Desai, A., Rivadeneyra, F., Lam, J.-P., Lo, T., Marsden, D. and Skavysh, V. (2022). Improving the Efficiency of Payments Systems Using Quantum Computing. *Staff Working Paper 2022-53*, Bank of Canada. <https://www.bankofcanada.ca/2022/12/staff-working-paper-2022-53/>
2. HSBC and IBM — Ciceri, A., Cottrell, A., Freeland, J. et al. (2025). Enhanced fill probability estimates in institutional algorithmic bond trading using statistical learning algorithms with quantum computers. arXiv:2509.17715. <https://arxiv.org/abs/2509.17715>
3. Press release: HSBC (25 September 2025). <https://www.hsbc.com/news-and-views/news/media-releases/2025/hsbc-demonstrates-worlds-first-known-quantum-enabled-algorithmic-trading-with-ibm>
4. Quantinuum (January 2024). Honeywell Announces the Closing of \$300 Million Equity Investment Round for Quantinuum at \$5B Pre-Money Valuation. Press release. <https://www.quantinuum.com/press-releases/honeywell-announces-the-closing-of-300-million-equity-investment-round-for-quantinuum-at-5b-pre-money-valuation>
5. ECIPE (March 2025). Benchmarking Quantum Technology Performance: Governments, Industry, Academia and their Role in Shaping our Technological Future. *ECIPE Policy Brief*. <https://ecipe.org/publications/benchmarking-quantum-technology-performance/>
6. European Union — NIS Cooperation Group (June 2025). Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>
7. IBM Quantum. Development Roadmap. <https://www.ibm.com/roadmaps/quantum.pdf>
8. Quantinuum (September 2025). Honeywell Announces \$600 Million Capital Raise For Quantinuum at \$10B Pre-Money Equity Valuation to Advance Quantum Computing at Scale. Press release. <https://www.quantinuum.com/press-releases/honeywell-announces-600-million-capital-raise-for-quantinuum-at-10b-pre-money-equity-valuation-to-advance-quantum-computing-at-scale#>
9. United States — Bureau of Industry and Security (6 September 2024). Commerce Control List Additions and Revisions; Implementation of Controls on Advanced Technologies Consistent With Controls Implemented by International Partners. Interim final rule. *Federal Register*, vol. 89, no. 173. <https://govinfo.gov/content/pkg/FR-2024-09-06/pdf/2024-19633.pdf>
10. European Union — Commission Delegated Regulation (EU) 2025/2003 (14 November 2025) amending Annex I to Regulation (EU) 2021/821 on dual-use items. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg_del/2025/2003/oj/eng
11. NIST (21 May 2026). Department of Commerce Announces Letters of Intent With 9 Companies for \$2 Billion to Accelerate U.S. Leadership in Quantum Computing. Press release. <https://www.nist.gov/news-events/news/2026/05/department-commerce-announces-letters-intent-9-companies-2-billion>
12. NIST (13 August 2024). NIST Releases First 3 Finalized Post-Quantum Encryption Standards (FIPS 203, 204 and 205). <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
13. United States — Executive Order 14412, Securing the Nation Against Advanced Cryptographic Attacks (22 June 2026). *Federal Register*, vol. 91, no. 121. <https://www.federalregister.gov/documents/2026/06/25/2026-12909/securing-the-nation-against-advanced-cryptographic-attacks>