



La computación cuántica no sustituirá el cálculo financiero clásico, sino que se sumará a él en aplicaciones muy concretas



El acceso a esta tecnología estará muy concentrado en pocos actores y condicionado por las políticas industriales de los grandes bloques geopolíticos



La homogeneización y la opacidad de los modelos, junto con una amenaza directa a la criptografía bancaria, exigirán una respuesta regulatoria y de infraestructura que no puede esperar a que la tecnología madure

QUANTUM FINANCE: LA CARRERA POR EL CONTROL DE LA COMPUTACIÓN CUÁNTICA

Manuel AYALA LÓPEZ
Jaime CABOTÁ JIMÉNEZ
Raúl VIÑAS ABADÍA

Afi

La carrera cuántica en banca y mercados se decidirá menos en el desarrollo de la tecnología que en las condiciones de acceso a su capacidad de cálculo. La computación cuántica se incorporará a las finanzas en aplicaciones concretas (valoración de derivados, optimización de carteras, liquidación de pagos), pero el acceso a ella estará muy concentrado en un número reducido de actores con recursos suficientes para experimentar durante años. Esa concentración, más que la tecnología en sí, determinará quién captura las ventajas de mercado y quién asume sus riesgos: homogeneización de modelos, opacidad y una amenaza directa a la criptografía bancaria. En los próximos años no cabe esperar tanto un “momento cuántico” que revolucione las finanzas como avances graduales en infraestructura y en regulación poscuántica. La cuestión decisiva es qué entidades empiezan a prepararse para gestionar ese reparto y sus riesgos.

Concentrar antes de transformar

La intuición lleva a pensar que una tecnología revolucionaria sustituye a los procesos existentes. Sin embargo, a corto y medio plazo, la computación cuántica funcionará en simbiosis con los procedimientos tradicionales, allí donde haya que resolver problemas de elevada complejidad.

Ese papel complementario obedece, por ahora, a un límite físico. Los ordenadores cuánticos son extremadamente sensibles a su entorno, lo que provoca una pérdida de información conocida como decoherencia. Los errores que genera se acumulan y limitan el tamaño de los problemas que pueden resolverse con fiabilidad.

La ventaja competitiva de la computación cuántica no dependerá solo de su desarrollo tecnológico, sino también de quién tenga acceso a ella y de su capacidad para aprovecharla

Además, el acceso a esta tecnología no será uniforme, debido a sus elevadas barreras de entrada. El alto coste del *hardware* y la escasez de talento especializado, capaz de combinar conocimiento financiero y computacional, concentrarán la ventaja en un número reducido de actores, muchos de ellos grandes tecnológicas y entidades financieras con recursos suficientes para experimentar sin un retorno inmediato. De ese desnivel en el acceso, y no del ritmo al que avance el *hardware*, dependerá qué actores capturen las ventajas de mercado y cuáles queden expuestos a sus riesgos.

Cabe objetar que preocuparse hoy por el reparto de una capacidad que aún no existe es prematuro. La objeción vale para los modelos, pero no para la criptografía, donde lo que se cifra hoy ya está expuesto, ni para la dependencia de proveedores, que se forja durante los años de experimentación.

¿Qué aporta la computación cuántica a las finanzas?

El potencial de la computación cuántica reside en su capacidad para analizar un número muy elevado de alternativas y encontrar entre ellas las combinaciones más eficientes: valorar derivados complejos con mayor rapidez u optimizar carteras con un número de restricciones hoy inabordable.

En un trabajo publicado en 2022, investigadores del Banco de Canadá aplicaron, junto con D-Wave, un algoritmo híbrido de recocido cuántico (*quantum annealing*) a treinta días de pagos no urgentes del sistema canadiense. [Al reordenar los pagos en lotes de setenta, lograron un ahorro medio de liquidez de 240 millones de dólares canadienses al día \(superior a 1.000 millones en algunas jornadas de la muestra\), sobre una asignación diaria del sistema de entre 15.000 y 20.000 millones¹](#). El coste de esa mejora fue un retraso medio de 90 segundos en la liquidación, atribuible casi por completo al tiempo necesario para acumular cada lote, ya que el algoritmo tardaba cinco segundos en resolver el problema.

Extrapolado al conjunto del sector, este resultado podría traducirse en una asignación más eficiente del capital y la liquidez, y en una medición de riesgos casi en tiempo real. Al menos al principio, la implementación se basará en sistemas híbridos, pero su alcance no es menor: problemas que hoy deben simplificarse por falta de capacidad de cálculo admitirían un número de variables sin precedentes.

En los mercados, la ventaja es de método antes que de potencia. En una simulación de Monte Carlo tradicional, reducir el margen de error a la mitad exige multiplicar aproximadamente por cuatro el número de simulaciones. En condiciones ideales, algunos algoritmos cuánticos podrían lograr la misma mejora con solo duplicar el número de consultas al sistema cuántico, gracias a una técnica conocida como estimación cuántica de amplitudes. La computación cuántica permitiría así analizar más escenarios con los mismos recursos o alcanzar una estimación más precisa en el mismo tiempo.

El experimento que HSBC e IBM anunciaron en septiembre de 2025 obtuvo una ventaja por otra vía. [En lugar de acelerar un cálculo, el equipo empleó circuitos cuánticos](#)

[para transformar los datos de entrada y alimentar con ellos modelos estadísticos convencionales, con el fin de estimar la probabilidad de que una cotización de bonos corporativos terminara convirtiéndose en una operación ejecutada². Con datos reales del mercado europeo de renta fija corporativa, la capacidad predictiva mejoró hasta un 34 % frente a las técnicas clásicas que el banco utiliza como referencia³.](#)

Esa ventaja, sin embargo, tiene fecha de caducidad. En mercados competitivos, cualquier mejora predictiva se erosiona en cuanto varios participantes acceden a una técnica similar: los precios se ajustan y el margen desaparece. La diferencia real está en convertir ese acceso temprano en modelos propios y procesos difíciles de replicar antes de que la ventaja se diluya.

Proveedores, bancos y Estados: quién controla la capacidad cuántica

En la carrera cuántica intervienen tres actores: los proveedores tecnológicos, que controlan la infraestructura; las entidades financieras, que acumulan conocimiento aplicado, y los Estados, que fijan las reglas del juego.

Los proveedores, como IBM, Google o D-Wave, dominan tanto el *hardware* como los entornos de desarrollo sobre los que se construyen los primeros algoritmos financieros. Por coste y especialización, la mayoría de las entidades no construirá ordenadores cuánticos propios, del mismo modo que tampoco desarrolla sus propios modelos de IA. Accederá a ellos a través de la nube o de acuerdos de colaboración, lo que reduce la inversión inicial, pero traslada el control de un recurso estratégico a unos pocos proveedores capaces de condicionar el mercado y marcar el ritmo del sector. [El caso de JPMorgan lo ilustra: pese a contar con uno de los equipos cuánticos más avanzados de la banca, ha tenido que apoyarse en los ordenadores de Quantinuum y entrar en su capital —liderando rondas de financiación de 300 millones de dólares en 2024 y de casi 600 millones en 2025— para asegurarse una posición en el proveedor del que depende⁴.](#)

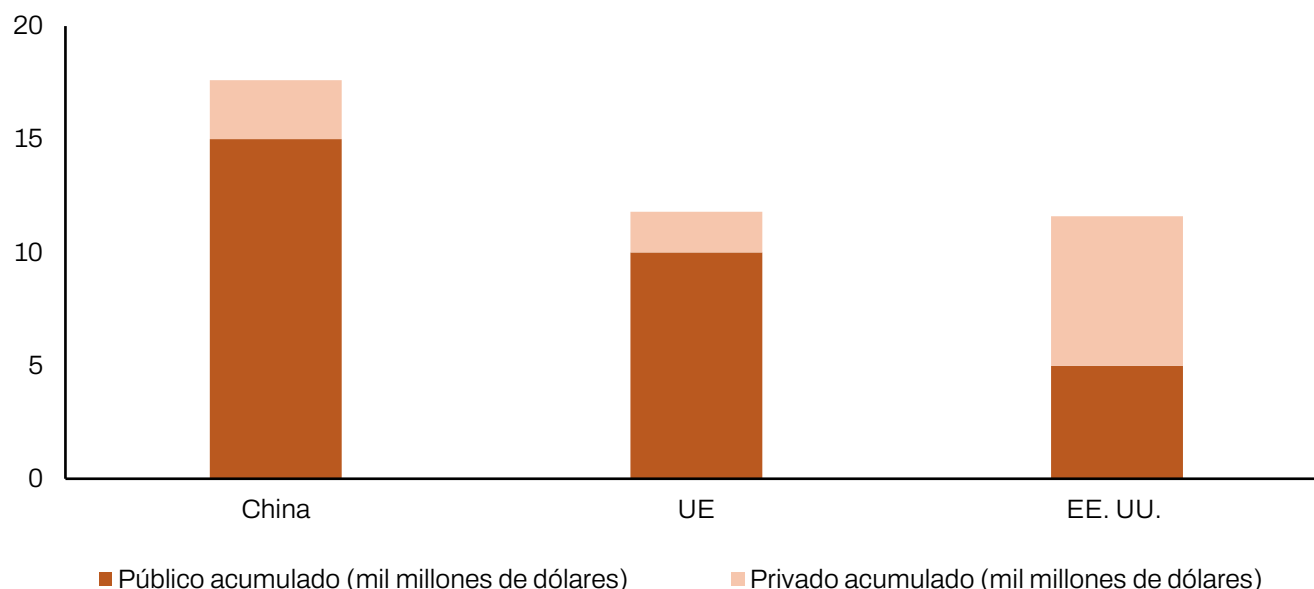
Las entidades financieras, como JPMorgan, Goldman Sachs o HSBC, ya experimentan con esta tecnología. Aprender a traducir problemas financieros en modelos cuánticos e integrarlos en entornos sujetos a estrictos controles de riesgo genera un capital de conocimiento que, con independencia del acceso al *hardware*, separa a quienes la adoptan pronto de quienes lo harán cuando esté madura.

Los Estados, con EE. UU., China y la UE a la cabeza, han incorporado la tecnología cuántica a sus políticas industriales para atraer inversión y talento y desarrollar proveedores propios. Esa intervención ya condiciona el mercado. Desde 2024, EE. UU. exige licencia para exportar ordenadores cuánticos que superen determinados umbrales de número de cúbits y tasa de error, mientras que la UE aplica controles similares desde noviembre de 2025. Además, en mayo de 2026, el Gobierno estadounidense propuso invertir 2.000 millones de dólares en participaciones minoritarias de nueve empresas cuánticas, con lo que también busca asegurarse una posición en los proveedores. Para una entidad europea que accede a través de la nube

Tres actores clave determinan el rumbo de la carrera cuántica: los proveedores tecnológicos, que controlan la infraestructura; las entidades financieras, que desarrollan conocimientos sobre sus aplicaciones prácticas; y los Estados, que establecen el marco regulatorio

a un ordenador estadounidense, las condiciones de acceso dependen también de que esa exportación siga estando permitida.

Figura 1 - Inversión pública y privada en computación cuántica hasta marzo de 2025



Fuente: [ECIPE, Benchmarking Quantum Technology Performance \(March 2025\)](#).⁵ La inversión privada es un cálculo propio a partir de los porcentajes del informe.

Riesgo sistémico: homogeneización, opacidad y seguridad

Si el acceso a los algoritmos y a la infraestructura queda concentrado en pocos proveedores, bancos y fondos podrían terminar utilizando herramientas similares. Si esos modelos interpretan una perturbación de la misma manera, distintas entidades podrían reducir a la vez su exposición a determinados activos. Esa simultaneidad amplifica el movimiento que la originó: la venta simultánea presiona los precios a la baja, confirma en apariencia la señal que emitieron los modelos y refuerza el incentivo a seguir vendiendo. Lo que empieza como una lectura de modelo termina siendo una caída del mercado.

El problema se agrava porque todo modelo depende de datos históricos y de supuestos que pueden dejar de ser válidos en periodos de incertidumbre. Si varias instituciones utilizan una misma herramienta, una estimación equivocada puede propagarse por el mercado y afectar simultáneamente a numerosas entidades. Por eso, la validación de estos modelos será aún más importante que la de los clásicos.

Y esa validación no será sencilla. Los algoritmos cuánticos devuelven resultados de naturaleza probabilística, que dos ejecuciones sucesivas no reproducen de forma idéntica, y su funcionamiento interno no admite una inspección paso a paso equivalente a la de un cálculo clásico. Ello complica tanto la auditoría interna como la revisión supervisora en un sector en el que cada decisión relevante debe poder explicarse y reconstruirse, y en el que aún no están definidos los niveles de trazabilidad exigibles a un modelo cuántico.

La amenaza más urgente se encuentra en el ámbito de la ciberseguridad, ya que un ordenador cuántico con suficiente capacidad podría vulnerar algunos de los sistemas criptográficos que permiten intercambiar claves de forma segura, verificar la identidad de los usuarios y garantizar la validez de los certificados y las firmas digitales

El riesgo más inmediato, sin embargo, afecta a la seguridad de la información: un ordenador cuántico suficientemente potente podría comprometer parte de la criptografía de clave pública utilizada para el intercambio de claves, la autenticación de usuarios y la verificación de certificados y firmas digitales. Los riesgos anteriores dependen de que las entidades adopten algoritmos cuánticos. El de la seguridad, en cambio, les afecta aunque no lleguen a utilizarlos, y es el más inmediato. Un ordenador cuántico suficientemente avanzado podría comprometer parte de la criptografía de clave pública que se utiliza para intercambiar claves, autenticar usuarios y validar certificados y firmas digitales. En agosto de 2024, el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) aprobó los tres primeros estándares de criptografía poscuántica, diseñados para sustituir progresivamente a los algoritmos que hoy protegen el intercambio de claves y la firma digital. La migración no puede esperar a que exista un ordenador capaz de ejecutar esos ataques, entre otras razones porque la información cifrada hoy puede almacenarse para descifrarla en el futuro, una estrategia conocida como *harvest now, decrypt later*. El ritmo de esa migración dependerá de los plazos que fijen los reguladores de cada país, lo que conecta este riesgo con la carrera entre Estados descrita antes.

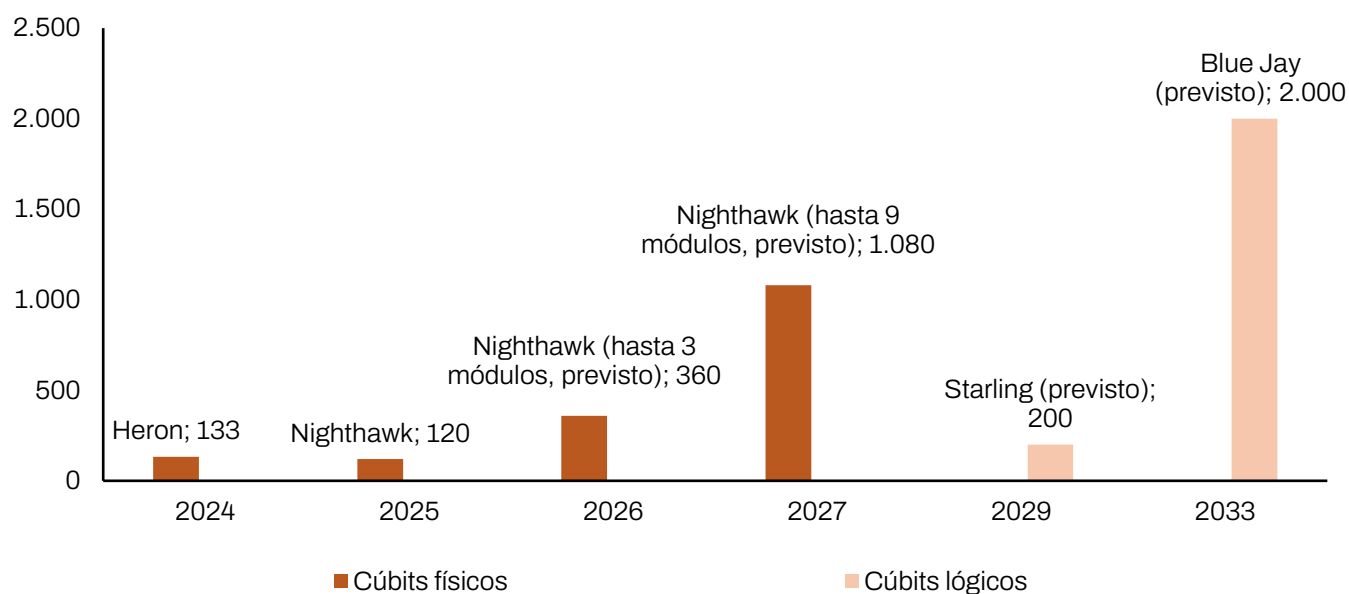
En definitiva, en todos los casos el riesgo sistémico no procede solo de fallos individuales, sino de la dependencia de unas mismas herramientas y de la propagación de vulnerabilidades en un sistema financiero estrechamente interconectado.

Qué esperar en la próxima década

[En criptografía, la Unión Europea ha fijado el final de 2030 como fecha límite para migrar los sistemas financieros críticos a estándares poscuánticos, con una transición completa prevista para 2035⁶](#). Estados Unidos ha ido más lejos: una orden ejecutiva de junio de 2026 adelantó de 2035 a 2030 el plazo para el establecimiento de claves en los sistemas federales de alto valor, y a 2031 el de las firmas digitales, y extendió la exigencia a sus contratistas.

[En el hardware, IBM sitúa hacia 2029-2033 la disponibilidad de procesadores con miles de cúbits y una corrección de errores suficiente para explotar aplicaciones que hoy están en fase de prueba de concepto. Si ese calendario se cumple, la pregunta relevante no será si el acceso seguirá pasando⁷](#) por la nube, algo que ya ocurre hoy, sino en qué condiciones. Caben dos escenarios: uno abriría ese acceso a un número amplio de entidades en términos competitivos; el otro mantendría la explotación comercial concentrada en los mismos proveedores que ya dominan el *hardware* y los servicios en la nube, que reservarían las mejores condiciones a clientes seleccionados mediante acuerdos cerrados.

El calendario importa menos que la posición desde la que cada entidad lo afronte, y esa posición depende de decisiones que ya pueden tomarse: clasificar qué información requiere protección a largo plazo, auditar cuánto depende la entidad de proveedores externos antes de que esa dependencia se vuelva estructural y fijar criterios propios para validar cualquier modelo cuántico que se incorpore. Ninguno de estos pasos exige esperar a que la tecnología madure.

Figura 2 - Hoja de ruta de IBM Quantum 2024-2033: cúbits de circuito

Fuente: IBM Quantum, hoja de ruta oficial.

Ahí reside la diferencia entre adoptar la tecnología en los términos de otros y hacerlo en los propios. La computación cuántica puede mejorar la gestión del riesgo, pero no elimina su dimensión institucional. **FI**

Referencias

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/departament-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>