Facultad de Ciencias Económicas y Empresariales

ICADE

COMPUTACIÓN CUÁNTICA Y SU POTENCIAL EN EL ÁMBITO FINANCIERO

Autor: Begoña Astarloa Domínguez

Director: Raquel Galazo García

MADRID | Marzo 2026

Agradecimientos

A mi directora, Raquel Galazo, por darme la oportunidad de realizar este trabajo y por su ayuda y dedicación durante el proceso.

A mi padre, por enseñarme la importancia de la inquietud y el valor de ir siempre un poco más allá.

A mis amigos de UTS, por animarme a adentrarme en el mundo de la cuántica.

Resumen

La computación cuántica se presenta como una de las tecnologías más disruptivas del siglo XXI, con un potencial transformador especialmente relevante para el sector financiero. Este trabajo analiza las principales aplicaciones de la computación cuántica en el sector financiero y los obstáculos que condicionan su desarrollo. Se examinan cuatro ámbitos concretos: la aceleración de simulaciones Monte Carlo, la optimización de carteras a través del *quantum annealing*, el *quantum machine learning* aplicado a la evaluación de riesgo crediticio y la amenaza de los algoritmos de Shor y Grover representan para la criptografía financiera vigente. Se examinan asimismo las limitaciones técnicas que frenan el desarrollo de esta tecnología como la decoherencia y el ruido en dispositivos NISQ, corrección de errores cuánticos y desafíos de escalabilidad del hardware. Se concluye que, si bien la mayoría de las aplicaciones se encuentran todavía en fases experimentales, la frontera entre el potencial teórico y la aplicación práctica se desplaza de forma sostenida, y que el sector financiero tiene ante sí tanto una amenaza presente, en materia de criptografía, como una oportunidad estratégica que ha lanzado una carrera hacia la supremacía cuántica, en la que participan gobiernos, instituciones e inversores privados de primer nivel.

Palabras clave

Computación cuántica, finanzas cuánticas, ventajas cuánticas, algoritmos cuánticos, optimización de carteras, simulación financiera, computación cuántica adiabática.

Abstract

Quantum computing stands as one of the most disruptive technologies of the twenty first century, with transformative potential that is particularly relevant for the financial sector. This paper examines the main applications of quantum computing in finance and the obstacles that currently constrain its development. Four specific areas are analyzed: the acceleration of Monte Carlo simulations, portfolio optimization through quantum annealing, quantum machine learning applied to credit risk assessment, and the threat posed by Shor's and Grover's algorithms to existing financial cryptographic systems. The study further addresses the technical limitations hindering progress in this field, including decoherence and noise in NISQ devices, quantum error correction challenges and hardware scalability constraints. It is concluded that, while most applications remain at an experimental stage, the boundary between theoretical potential and practical

implementation is steadily shifting. The financial sector thus faces both an immediate threat, in the domain of cryptography, and a strategic opportunity that has triggered a race towards quantum supremacy, in which governments, institutions and leading private investors are already active participants.

Key words

Quantum computing, quantum finance, quantum advantage, quantum algorithms, portfolio optimization, financial simulation, adiabatic quantum computing.

Tabla de contenido

Introducción *7*

Objetivos: **8**

Metodología **8**

CAPÍTULO 1: Marco conceptual y fundamentos de computación cuántica *10*

1. Principios básicos y desarrollo de la mecánica cuántica **10**

2. Computación cuántica **12**

3. El qubit **13**

4. Principios relevantes de la computación cuántica **15**

5. Qubits y tipos de computación cuántica **16**

5.1 Computación cuántica de puertas 17

5.2 Computación cuántica adiabática (*quantum annealing*) 17

6. El ecosistema cuántico actual **18**

6.1 Inversión y tendencias tecnológicas recientes 18

6.2 Empresas lideres en hardware cuántico 19

6.3 Software y herramientas de desarrollo 19

6.4 Respaldo institucional: dimensional internacional y nacional 20

7. De la teoría a la práctica: hacia las aplicaciones futuras **20**

CAPÍTULO 2: Principales aplicaciones en el ámbito financiero *22*

1. Mejoras cuánticas **22**

CAPÍTULO 3: Modelización y simulación financiera *24*

1. La incertidumbre como punto de partida: modelos estocásticos en finanzas **24**

2. El método Monte Carlo: fundamentos y aplicaciones financieras **24**

3. Limitaciones computacionales del Monte Carlo clásico **25**

4. Aceleración cuántica: el algoritmo de Monte Carlo cuántico (QMCI) **26**

5. Aplicación a la valoración de derivados financieros **27**

CAPÍTULO 4: Optimización y gestión de carteras *29*

1. La cartera de inversión: concepto y problema de optimización **29**

2. La teoría de Markowitz y la frontera eficiente **29**

3. Complejidad computacional del problema: restricciones y escalabilidad **30**

4. Problemas *NP-hard* y los límites de la computación clásica **31**

5. La computación cuántica como alternativa: QAOA y *Quantum Annealing* **31**

6. Resultados empíricos y aplicaciones reales **32**

CAPÍTULO 5: Machine learning cuántico *34*

1. *Machine learning* en finanzas: fundamentos y aplicaciones **34**

2. Riesgo crediticio y clasificación 35

3. Aplicación del QML al credit scoring: estado del arte y resultados 35

4. Impacto económico 36

CAPÍTULO 6: Criptografía y seguridad financiera en la era cuántica. 37

1. Los fundamentos de la criptografía y la amenaza cuántica 37

2. El riesgo real: proyecciones y vulnerabilidades del sistema financiero. 39

3. Criptografía post-cuántica: la respuesta del sector. 40

CAPÍTULO 7: Limitaciones actuales de la computación cuántica. 42

1. Decoherencia, ruido y corrección de errores cuánticos 42

2. Corrección de errores cuánticos 44

3. El desafío de la escalabilidad: hardware e ingeniería 45

CONCLUSIONES 47

Declaración de Uso de Herramientas de Inteligencia Artificial Generativa en Trabajos Fin de Grado 51

BIBLIOGRAFÍA: 53

ANEXOS: 63

Anexo 1: Tipos de qubits 63

Anexo 2: Tipos de puertas cuánticas 65

Anexo 3 – IBM Quantum Roadmap (2025). 66

Introducción

En su naturaleza más profunda, las finanzas, se enfrentan a la incertidumbre asociada al comportamiento futuro de los activos y a los precios y rendimientos, sean ganancias o pérdidas, que estos pueden generar[1]. Por ello, se trabaja con conceptos como el riesgo, la volatilidad y la predicción[2], con el objetivo de maximizar beneficios y minimizar perdidas. A pesar de que las finanzas son casi tan antiguas como la civilización misma, recientes desarrollos tecnológicos como la computación clásica a mediados del siglo pasado, han permitido realizar cálculos de una complejidad antes inabordable, agilizando y perfeccionando la ciencia del estudio de los mercados y la gestión de capital.

Paralelamente, el prometedor estudio de la aplicación de los principios de la física cuántica a la computación ha despertado el interés creciente en la industria financiera, con inversiones millonarias en investigación y desarrollo por parte de gobiernos, instituciones financieras y actores privados[3]. Y no es para menos: la computación cuántica se perfila capaz de acelerar de forma cuadrática los métodos de simulación y valoración más utilizados en el sector, resolver considerablemente más rápido problemas de optimización que hoy requieren días de procesamiento, transformar los modelos de evaluación de riesgo e incluso amenazar los sistemas criptográficos sobre los que descansa toda la infraestructura de seguridad financiera global. Unas ventajas que de materializarse a la escala que apunta la literatura académica, podrían traducirse en beneficios de magnitud extraordinaria para quienes sepan anticiparse a ellas.

Sin embargo, entre la promesa y la realidad persiste una distancia considerable. Resulta entonces pertinente preguntarse qué aplicaciones prácticas tiene hoy la computación cuántica en el ámbito financiero, hacia donde se dirige la investigación y si los avances son realmente tan prometedores como sugieren los titulares. En definitiva, si estamos ante una revolución tecnológica genuina capaz de transformar el sector. Retomo entonces una frase que John McCarthy, padre la inteligencia artificial, recuperó del biólogo inglés T.H. Huxley en un célebre artículo publicado en la revista de Stanford: "*Extinguished*

[1] Orús, Román, Samuel Mugel y Enrique Lizaso. (2019a). "Quantum computing for finance: Overview and prospects". *Reviews in Physics*, 4, p.2.
[2] Id.
[3] McKinsey & Company. (2025). *Quantum Technology Monitor.*

philosophies lie about the cradle of every science as the strangled snakes beside that of Hercules"[4][5].

Objetivos

Este trabajo tiene por objetivo global determinar las potenciales aplicaciones de la computación cuántica en el sector financiero, donde se perfila como una tecnología capaz de transformarlos de forma estructural. Para ello, se plantean los siguientes objetivos específicos:

- Establecer un marco conceptual del desarrollo de la computación cuántica y de su estado actual, incluyendo los principios físicos que la sustentan y el ecosistema tecnológico que la rodea.
- Identificar y analizar las aplicaciones existentes y potenciales de la tecnología cuántica en el ámbito financiero, con especial atención a la simulación y valoración de activos, la optimización de carteras, el aprendizaje automático y la criptografía.
- Describir los desafíos técnicos y de ingeniería a los que se enfrenta el desarrollo de la computación cuántica, y que condicionan el horizonte temporal de su adopción real.
- Evaluar de forma critica si los avances documentados en la literatura académica y empírica respaldan las expectativas generadas en torno a esta tecnología.

Metodología

El principal desafío del estudio de la computación cuántica radica en su carácter marcadamente innovador y en su estado de desarrollo aun incompleto. Se trata de una tecnología emergente, en rápida evolución, sobre la que la evidencia empírica es todavía limitada y en muchos casos provisional. Por ello, el presente trabajo adopta un enfoque cualitativo, articulado a través de un análisis descriptivo y exploratorio.

La investigación se sustenta en una revisión bibliográfica exhaustiva de literatura académica y profesional, abordada desde una perspectiva crítica y comparativa. Las

[4] McCarthy, J. (2007). What is artificial intelligence? Stanford University.
[5] ("Las filosofías extintas yacen alrededor de la cuna de toda ciencia como las serpientes estranguladas junto a la de Hércules").

fuentes consultadas incluyen artículos científicos, informes sectoriales de referencia y publicaciones institucionales.

El trabajo se estructura en siete capítulos. El primero establece el marco conceptual necesario para comprender la computación cuántica, recorriendo el desarrollo histórico de la mecánica cuántica, los principios fundamentales del paradigma cuántico y el ecosistema tecnológico actual. Los capítulos segundo al sexto se centran en las aplicaciones financieras concretas: la aceleración de métodos de Monte Carlo mediante estimación de amplitud cuántica, la optimización de carteras a través del *quantum annealing* y el QAOA, la aplicación del *machine learning* cuántico a la evaluación del riesgo crediticio y la amenaza que la computación cuántica representa para la criptografía financiera vigente, junto con las respuestas del sector. El séptimo capítulo aborda las limitaciones técnicas que frenan la materialización de estas aplicaciones: decoherencia, correcciones y escalabilidad del hardware, y las conclusiones que se derivan del análisis conjunto. A lo largo de todo el trabajo, el objetivo es mantener un equilibrio entre el rigor técnico necesario para comprender los mecanismos cuánticos y la perspectiva económica y financiera que justifica su estudio en este contexto.

CAPÍTULO 1: Marco conceptual y fundamentos de computación cuántica

1. Principios básicos y desarrollo de la mecánica cuántica

Con el fin de comprender adecuadamente la computación cuántica y sus posibles aplicaciones, introduciremos previamente un marco conceptual básico sobre los principios fundamentales de la mecánica cuántica. Aunque se trata de una rama de la física de elevada complejidad, en este apartado se abordaran únicamente aquellos conceptos esenciales que permiten entender como dichos principios se trasladan posteriormente al ámbito computacional.

El desarrollo de la mecánica cuántica tal y como la conocemos, es el resultado de una sucesión de teorías y descubrimientos desarrollados a lo largo de varias décadas. En este contexto, en 1964 en una conferencia en la Universidad de Cornell, el importante físico cuántico Richard Feynman afirmaba de forma célebre: "creo que puedo decir con seguridad que nadie entiende la mecánica cuántica", reflejando el carácter profundamente contraintuitivo y disruptivo de esta disciplina[6], centrada en el estudio del comportamiento de la materia y la energía a escalas atómica y subatómica[7].

Durante las primeras décadas del siglo XX tuvo lugar lo que conocemos como la primera revolución quántica. En este periodo, físicos como Max Planck, Niels Bohr, Albert Einstein, Erwin Schrödinger o Werner Heisenberg, comenzaron a identificar fenómenos que no podían explicarse mediante las leyes de la física clásica desarrolladas previamente por autores como Copérnico en el siglo XV, Galileo en el XVI o Newton en el XVII.

En 1900, Max Planck logró explicar el problema de la radiación de cuerpos negros al proponer que la energía no se emite de forma continua, sino en cantidades discretas, introduciendo así el concepto de cuantización y la constante de Planck[8]. Este planteamiento supuso la primera manifestación formal de la física cuántica. Además, en 1905 Albert Einstein profundizó en esta idea al explicar el efecto fotoeléctrico[9], demostrando que la radiación electromagnética puede comportarse como partículas,

[6]Griffiths, D. J. (2018). Introduction to quantum mechanics (4th ed.). *Cambridge University Press*.
[7] Universidad Internacional de La Rioja (UNIR). (s. f.). Física cuántica: qué es, principios y aplicaciones.
[8] Planck, M. (1901). On the law of distribution of energy in the normal spectrum. *Annalen der physik*, *4*(553), 1.
[9] Einstein, A. (1905). Heurística de la generación y conversión de la luz. *Ann. Phys*, *17*(1), 549-560.

denominadas fotones, además de como ondas. Este descubrimiento supuso una ruptura significativa con la visión clásica de la física y fue, de hecho, el que le valió el premio Nobel en 1921, y no su conocida teoría de la relatividad. En 1913, Niels Bohr desarrolló un modelo atómico que describía el comportamiento de los electrones en orbitas discretas alrededor del núcleo[10], estableciendo el primer puente entre la física clásica y la emergente mecánica cuántica. A partir de aquí, las cosas adquieren complejidad ya que más adelante, en 1927, Werner Heisenberg formuló el principio de incertidumbre[11], según el cual no es posible conocer simultáneamente con precisión absoluta ciertas magnitudes físicas, como la posición y el momento de una partícula. Este principio introdujo de forma definitiva el concepto de probabilidad en la descripción de los sistemas cuánticos, sustituyendo la noción clásica de trayectorias deterministas. A su vez, en 1926, Erwin Schrödinger desarrolló la ecuación de onda[12], que lleva su nombre, una formulación matemática fundamental de la mecánica cuántica que describe la evolución temporal del estado cuántico de un sistema. A diferencia de la física clásica, donde el estado de un sistema puede conocerse con precisión, la ecuación de Schrödinger refleja la naturaleza esencialmente probabilística del mundo cuántico: el estado de una partícula no queda determinado hasta el momento de su medición, sino que existe como superposición de múltiples estados posibles, cada uno asociado a una probabilidad. En notación formal, un sistema puede describirse como:

$$|\psi\rangle = \alpha|\text{estado A}\rangle + \beta|\text{estado B}\rangle \quad (1.1)$$

donde α y β representan las amplitudes de probabilidad de cada resultado. En el momento de la medición, este estado de superposición colapsa irreversiblemente hacia uno de los resultados posibles, perdiéndose la indeterminación previa.

Años más tarde, Schrödinger propuso su celebre experimento mental del gato, precisamente como una crítica a esta interpretación. En él, un gato encerrado en una caja queda vinculado al decaimiento radioactivo de un átomo: si el átomo decae, se libera un

[10] Bohr, N. (1913) 'I. On the constitution of atoms and molecules', *Philosophical Magazine* Series 6, 26: 151, 1-25.
[11] Heisenberg, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik*, *43*, 172–198.
[12]Schrödinger, E. (1926). Quantisierung als Eigenwertproblem [La cuantización como problema de autovalores]. *Annalen der Physik*, *384*(4), 361–376.

veneno que mata al animal, si no, el gato sobrevive[13]. Dado que el comportamiento del átomo obedece a las leyes cuánticas, antes de abrir la caja el sistema se describiría formalmente como:

$$|\psi\rangle = \alpha|\text{vivo}\rangle + \beta|\text{muerto}\rangle \quad (1.2)$$

Este experimento trata de evidenciar lo absurdo que resultaría aplicar la mecánica cuántica literalmente a escala macroscópica[14].

Creo que es muy importante resaltar, que estos descubrimientos no fueron solo revolucionarios en el mundo de la física, sino que causaron mucho revuelo a nivel filosófico también. La introducción de la incertidumbre y la superposición supuso una ruptura con la visión determinista del universo, dando lugar a una interpretación probabilística de la realidad física. Esta nueva concepción generó un intenso debate incluso entre los propios impulsores de la teoría, que se refleja la célebre frase de Einstein: "Dios no juega a los dados"[15].

2. Computación cuántica

La denominada segunda revolución cuántica se inicia en la segunda mitad del siglo XX y continúa desarrollándose en la actualidad. A diferencia de la primera, centrada en la formulación teórica de la mecánica cuántica, esta etapa se caracteriza por la aplicación práctica de dichos principios al desarrollo de nuevas tecnologías.

Los fundamentos de la computación cuántica comenzaron a tomar forma a principios de los años ochenta. En 1980, Paul Benioff fue el primero en proponer formalmente la idea de un ordenador cuántico[16], sugiriendo que una máquina de Turing podría reemplazarse por una secuencia de sistemas cuánticos de dos estados, llamados qubits[17]. Poco después,

[13] Schrödinger, E. (1935). Die gegenwärtige Situation in der Quantenmechanik [The present situation in quantum mechanics]. *Naturwissenschaften, 23*, 807–812, 823–828, 844–849.
[14] Contín Aylón, G. C. (2012). La paradoja del gato de Schrödinger y los problemas de la interpretación de la mecánica cuántica. *Universidad Nacional de Educación a Distancia*.
[15] Einstein, A. (1926). Carta a Max Born, 4 de diciembre de 1926. En Born, M. (ed.) (1971). *The Born-Einstein Letters*. Macmillan. p. 91.
[16] Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, *22*(5), 563–591.
[17] Gáfaro, R. E. M., Espinel, E. A. A., & Conde, H. A. P. (2025). Estado del arte de la computación cuántica sus desafíos y aplicaciones. *Revista Colombiana de Tecnologías de Avanzada*, *2*(46), p 92.

en 1982, Richard Feynman observó que ciertos fenómenos cuánticos no podían simularse eficientemente en ordenadores clásicos y planteo la posibilidad de diseñar sistemas computacionales basados directamente en principios cuánticos consolidando el concepto de computación cuántica[18].

El salto a la práctica llego en la segunda mitad de la década siguiente, con el desarrollo de los primeros algoritmos cuánticos con aplicaciones reales, el algoritmo de factorización de Peter Shor[19], en 1994, y el algoritmo de búsqueda de Lov Grover[20] en 1996, que demostraron que los principios cuánticos podrían traducirse en ventajas computacionales concretas[21]. A finales de los noventa se produjeron también los primeros hitos en *hardware*: la Universidad de California en Berkeley construyó la primera máquina de 2 qubits en 1998, IBM la primera de 3 qubits en 1999 y ese mismo año se fundó D-Wave, empresa pionera en computación cuántica comercial. Estos avances dieron el pistoletazo de salida a la segunda revolución cuántica y a la carrera global hacia la supremacía cuántica[22]. Precisamente en 2012, John Preskill definía esta supremacía como el momento en el que seamos capaces de tareas con sistemas cuánticos controlados que vayan más allá de lo que se puede conseguir con ordenadores digitales clásicos[23].

3. El qubit

La computación cuántica es fundamentalmente diferente a la computación clásica. Mientras que esta última se basa en bits que solo pueden adoptar los valores 0 o 1, la computación cuántica emplea bits cuánticos o qubits, unidad básica de información cuántica. Gracias al principio de superposición, un qubit puede encontrarse simultáneamente en una combinación de los estados 0 y 1, lo que constituye una de las principales fuentes de ventaja frente a la computación clásica[24].

---

[18] Feynman, R. P. (1982). Simulating physics with computers. *International Journal of Theoretical Physics*, *21*(6/7), 467–488.
[19] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, *26*(5), 1484–1509.
[20] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, 212–219.
[21] Gáfaro et al (2025) p.93.
[22] Id.
[23] Preskill, J. (2012). Quantum computing and the entanglement frontier.
[24] Vargas-Torres-Céliz, E., Lara-Baltazar, G., Mollinedo-Chávez, L., & Ricaldi-Arauzo, R. (2022). Computación Tradicional, Quantum y sus futuras aplicaciones. *Revista Científica de Sistemas e Informática*, *2*(1), e201-e201, p.11.

Aunque esta idea puede resultar difícil de entender, su formulación matemática puede ayudar a clarificar el concepto. El estado de un qubit puede expresarse como:

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \quad (1.3)$$

Donde ψ representa el estado cuántico, del que hablábamos con Schrödinger, y donde α y β representan las amplitudes de probabilidad asociadas a cada estado (0 y 1), que responden a su vez a la siguiente condición:

$$|\alpha|^2+|\beta|^2=1 \qquad (1.4)$$

De este modo $|\alpha|^2$ representa la probabilidad de obtener el estado 0 al medir el qubit y $|\beta|^2$ representa la probabilidad de obtener el estado 1[25]. Antes de la medición, el qubit permanece en un estado de superposición.

Para facilitar la comprensión de este comportamiento, un qubit se suele representar a través de la esfera de Bloch, una herramienta geométrica que permite visualizar de forma intuitiva los estados cuánticos posibles.

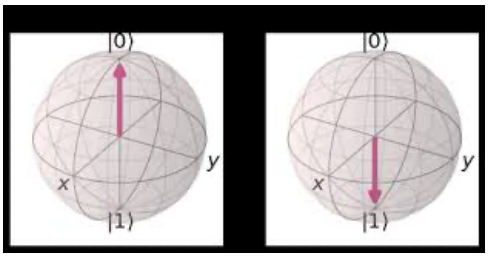

Imagen 1: esfera de Bloch: en ella los estados clásicos |0⟩ y |1⟩ se sitúan en polos opuestos, mientras que cualquier otro punto de la esfera representa un estado de superposición. Fuente: Quantum Computing Física Estadística Matemáticas (QC FEM).

Esta representación resulta especialmente útil para entender que, tanto en mecánica como en computación cuántica, se trabaja con probabilidades y no con certezas, y que el estado de superposición se mantiene hasta el momento de la medición, permitiendo a los ordenadores cuánticos explotar la inferencia cuántica entre amplitudes.

[25] SpinQ Technology. (2025). *Ultimate guide to qubit in quantum computing*.

4. Principios relevantes de la computación cuántica

A continuación, se describen algunos de los principios fundamentales de la computación cuántica que la diferencian de la computación clásica y que resultan clave para comprender su potencial impacto en el ámbito financiero y empresarial.

- Superposición

La superposición permite que un qubit se encuentre en una combinación de los estados 0 y 1, a diferencia de un bit clásico, que solo puede adoptar uno de los dos valores. En general, un sistema de n qubits puede describirse mediante una superposición de hasta 2^n estados base simultáneos[26]: así, 10 qubits permiten representar hasta 1024 estados. No obstante, esta propiedad no implica que todos esos estados puedan leerse simultáneamente, la utilidad computacional de la superposición reside más bien en que la evolución del sistema está gobernada por fenómenos de interferencia cuántica, que permiten amplificar resoluciones correctas y suprimir las incorrectas antes de realizar la medición. Una forma intuitiva de visualizarlo es imaginar una moneda lanzada al aire: mientras está en el aire, no es ni cada ni cruz, sino una combinación de ambas posibilidades[27]. Solo en el momento en el que cae, es decir al medir, el sistema colapsa a uno de los dos estados.

- Entrelazamiento

El entrelazamiento cuántico establece una correlación entre qubits de tal forma que sus estados no son separables: el estado de uno no puede describirse de forma independiente al otro, sino únicamente como parte del sistema conjunto[28]. A esto se suma el fenómeno de no localidad, dicha correlación se mantiene independientemente de la distancia física que separe los qubits, de forma que la medición de uno afecta instantáneamente al estado del otro. Imaginemos a Alice y a Bob, cada uno recibe una partícula entrelazada. Alice viaja a Marte y Bob se queda en la tierra, si Alice mide su partícula y la encuentra en un estado con espín hacia arriba, Bob sabrá instantáneamente que la suya se encuentra en un estado de espín hacia abajo, aunque no se hayan comunicado entre ellos[29]. Esta conexión

[26] Rieffel, E., & Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys, 32*(3), p 301.
[27] Hughes, C., et al. (2021). Introduction to superposition. En *Quantum Computing for the Quantum Curious*. Springer.
[28] Friis, N., et al. (2019). Entanglement certification from theory to experiment. *Nature Reviews Physics*, *1*, 72–87, p.2.
[29] SpinQ Technology. (2025). *Quantum entanglement examples explained*.

instantánea desafía la intuición clásica y constituyes una de las características fundamentales que distinguen los sistemas cuánticos de los clásicos, con implicaciones especialmente relevantes en problemas de optimización y criptografía.

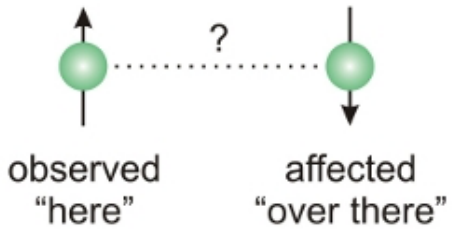

Imagen 2: Representación visual del entrelazamiento cuántico Fuente: Picoquant.

- Efecto túnel cuántico

El efecto túnel permite que una partícula atraviese una barrera energética que sería infranqueable según la física clásica[30]. Este fenómeno, que explicaremos más adelante[31], es especialmente relevante en determinados modelos de computación cuántica, como el *quantum annealing*, o computación cuántica adiabática, donde facilita la exploración eficiente de soluciones óptimas en problemas complejos.

- Coherencia

La coherencia cuántica se refiere a la capacidad de un sistema cuántico para mantener sus propiedades cuánticas sin interferencias externas. Mantener la coherencia es un requisito esencial para la superposición y el entrelazamiento[32], y constituye uno de los principales desafíos técnicos en el desarrollo de ordenadores cuánticos.

5. Qubits y tipos de computación cuántica

Como hemos visto antes, un qubit es un sistema cuántico de dos niveles. Dado que los ordenadores cuánticos se basan en principios radicalmente distintos a los de la computación clásica, se construyen empleando tecnología completamente diferente. Como la computación cuántica se encuentra aún en fase temprana de desarrollo, existen varias tecnologías empleadas para la construcción de qubits, entre las que destacan

[30] SpinQ (2025)
[31] Véase apartado 5.2 del capítulo 1..
[32] Xi, Z., Li, Y., & Fan, H. (2015). Quantum coherence and correlations in quantum system. *Scientific Reports*, *5*, 10922.

sistemas ópticos, materiales superconductores y sistemas basados en moléculas[33]. Esto da lugar a distintos tipos de qubits, cuya elección depende tanto de la arquitectura del ordenador cuántico como del tipo de problema que se desea abordar. Entre los principales tipos de qubits empleados en la actualidad se encuentran los qubits superconductores, los qubits de iones atrapados, los qubits fotónicos y los qubits topológicos, y su funcionamiento y composición se desarrollan en el Anexo 1.

A partir de estas diferentes realizaciones físicas de los qubits se desarrollan distintas arquitecturas de computación cuántica, entre las que destacan dos enfoques principales: la computación cuántica basada en puertas lógicas y la computación cuántica adiabática.

5.1 Computación cuántica de puertas

Uno de los principales modelos de computación cuántica es el basado en circuitos cuánticos, en el que la información se procesa mediante la aplicación de puertas lógicas cuánticas sobre los qubits[34]. En este modelo, los algoritmos cuánticos se construyen como una secuencia de operaciones que modifican el estado de uno o varios qubits, pudiendo incluso condicionar la acción de una puerta al estado de otro qubit, como ocurre en las puertas controladas. Físicamente, cada puerta consiste en una manipulación deliberada del estado de un qubit mediante pulsos laser, campos magnéticos y microondas, dependiendo del tipo de hardware empleado[35]. A diferencia de las puertas lógicas clásicas, las puertas cuánticas son reversibles, lo que implica que el número de qubits de entrada y salida es el mismo y que las operaciones pueden deshacerse, una característica esencial del procesamiento de información cuántica[36]. Una descripción detalla de las principales puertas cuánticas y su funcionamiento se recoge en el Anexo 2.

5.2 Computación cuántica adiabática (*quantum annealing*)

La computación cuántica adiabática, también conocida como *quantum annealing*, es enfoque de la computación cuántica especialmente diseñado para resolver problemas de

[33] Hughes, C., Isaacson, J., Perry, A., Sun, R. F., & Turner, J. (2021). Quantum computing for the quantum curious, p 13.
[34] Hughes et al (2021). Quantum Computing for the quantum curious, p 49.
[35] Williams, C. P. (2011). Quantum gates. In *Explorations in quantum computing.*
[36] Bonillo, V. M. (2013). Principios fundamentales de computación cuántica. *Universidad de la Coruna*, p 19.

optimización[37]. La idea fundamental consiste en representar el problema como un sistema físico cuyo comportamiento viene descrito por una función de energía denominada hamiltoniano. El proceso comienza con los qubits en un estado de superposición simple y evoluciona de forma gradual hacia un hamiltoniano final que codifica el problema a resolver[38]. Durante esta evolución, fenómenos cuánticos como el efecto túnel permiten al sistema atravesar barreras energéticas que en un esquema clásico conducirían a quedar atrapado en soluciones subóptimas.

Si esta evolución se realiza de manera suficientemente lenta, el sistema tiende a permanecer en su estado de menor energía de acuerdo con el teorema adiabático. En condiciones ideales, la solución final codifica el mínimo global del problema; sin embargo, en implementaciones prácticas, factores como el ruido, la temperatura o tiempos de evolución limitados pueden dar lugar a soluciones aproximadas.

Este paradigma aprovecha propiedades cuánticas como la superposición y el entrelazamiento para explorar de forma más eficiente espacios de soluciones que crecen exponencialmente con el número de qubits, como ocurre en los sistemas desarrollados por D-Wave Systems, pionero en la implementación de computación cuántica adiabática.

6. El ecosistema cuántico actual

6.1 Inversión y tendencias tecnológicas recientes

En los últimos años, la computación cuántica ha experimentado un notable impulso tanto desde el sector privado como desde las instituciones públicas. La inversión en start-ups de tecnologías cuánticas alcanzo aproximadamente los 2000 millones de dólares en 2024[39], lo que supone un crecimiento cercano al 50% respecto del año anterior, con más del 80% de dicha inversión concentrada en computación cuántica, y con previsiones de superar los 1000 millones de dólares anuales en ingresos antes de 2026[40]. Paralelamente, los avances tecnológicos más recientes se han centrado en el aumento de la calidad y fiabilidad de los qubits, el desarrollo de técnicas de corrección de errores y la mejora de

[37] D-Wave Systems. (s. f.). *Introduction to quantum annealing*.
[38] Crosson, E., & Lidar, D. (2021). Prospects for quantum enhancement with diabatic quantum annealing. *Nature Reviews Physics*, *3*, 466–489.
[39] McKinsey & Company. (2025). *Quantum Technology Monitor*. McKinsey Digital, p38.
[40] Ibid p 33.

la fidelidad de las puertas cuánticas, más que en el simple aumento del número de qubits, lo que refleja una mayor madurez del sector[41].

6.2 Empresas lideres en hardware cuántico

Este progreso está liderado por grandes empresas tecnológicas como IBM, Google o D-Wave, que en los últimos años han presentado avances significativos en procesadores cuánticos, como el reciente desarrollo del procesador Willow por parte de Google, o Condor, un procesador de 1121 qubits elaborado por IBM. Otro pionero en el sector de la computación cuántica es Rigetti Computing, que destaca por su desarrollo de Qubits superconductores y que recientemente se centra en el impulso de plataformas hibridas que combinan la computación clásica y la cuántica, facilitando la experimentación empresarial a través de servicios en la nube para fomentar la adopción de esta tecnología en diversos sectores[42].

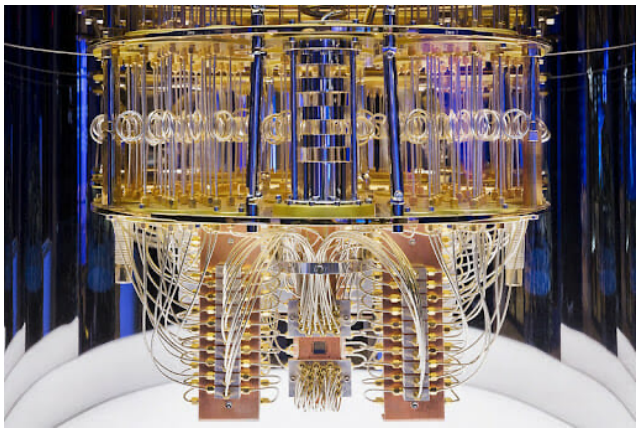

Imagen 3: El interior de un ordenador IMB System One. Fuente: IBM

6.3 Software y herramientas de desarrollo

En el ámbito del software, destaca Qiskit, el entorno de desarrollo de código abierto creado por IBM y actualmente el más utilizado a nivel mundial en el campo de la computación cuántica. Qiskit permite construir, optimizar y ejecutar circuitos cuánticos, facilitando tanto la investigación en algoritmos cuánticos como el acceso a hardware cuántico real a través de la nube. Además, incorpora simuladores cuánticos que permiten

[41] Ruane et al., (2025), pp. 104–109
[42] Redacción APD. (2025). *Empresas tecnológicas líderes en computación cuántica: Ejemplos y estrategias*. APD.

emular el comportamiento de un ordenador cuántico en hardware clásico, una herramienta esencial en la etapa actual de desarrollo, en la que el acceso a hardware cuántico fiable sigue siendo limitado. Su amplia adopción en la comunidad científica y académica lo ha consolidado como la referencia estándar para el desarrollo de aplicaciones cuánticas[43].

6.4 Respaldo institucional: dimensional internacional y nacional

La computación cuántica cuenta además con un fuerte respaldo institucional: en Estados Unidos destaca la National Quantum Initiative, mientras que en España se ha lanzado recientemente la Estrategia Nacional de Tecnologías Cuánticas, con una inversión pública prevista de 800 millones de euros[44]. De esta forma, el País Vasco se ha posicionado como un polo emergente en este ámbito al albergar uno de los ordenadores cuánticos más avanzados de Europa, con una capacidad cercana a los 200 qubits, evidenciando el creciente interés estratégico por esta tecnología a escala internacional, nacional y regional. Por otro lado, a principios de 2025 se inauguró en Barcelona el primer ordenador cuántico desarrollado con tecnología 100% europea[45], gracias al impulso de la iniciativa European High Performance Computing[46]. Ambos equipos constituyen los dos únicos ordenadores cuánticos operativos en España, conformando así el ecosistema cuántico nacional y evidenciando el creciente interés estratégico por esta tecnología.

7. De la teoría a la práctica: hacia las aplicaciones futuras

Con este marco conceptual se ha establecido la base teórica necesaria para comprender los fundamentos de la computación cuántica, su funcionamiento y su estado actual de desarrollo. A lo largo de los capítulos siguientes, estos conceptos se irán retomando y desarrollando de forma aplicada, analizando cómo la tecnología cuántica puede emplearse de manera específica en distintos ámbitos, centrándonos particularmente en el ámbito financiero, poniendo el foco en sus usos concretos, beneficios potenciales y limitaciones.

Y ahora sí, siendo sinceros, la computación cuántica no es un tema fácil de digerir, y este capítulo ha sido necesario para sentar las bases. A partir de aquí entramos en lo

[43] IBM (s.f) *Qiskit*. IBM Quantum
[44] Gobierno de España. (s. f.). *¿Qué es la Estrategia Nacional de Tecnologías Cuánticas?*
[45] Barcelona Supercomputing Center. (2025)
[46] IBM (2021).

verdaderamente interesante, el núcleo de este trabajo, analizando cómo esta tecnología puede transformar el mundo financiero y empresarial, pasando de la teoría a las aplicaciones prácticas donde la computación cuántica empieza a mostrar todo su potencial.

CAPÍTULO 2: Principales aplicaciones en el ámbito financiero

1. Mejoras cuánticas

Las instituciones financieras afrontan diariamente una amplia variedad de problemas computacionalmente complejos. Entre ellos destacan tareas de predicción, que abarcan desde la valoración de activos y la estimación del riesgo hasta la detección de transacciones anómalas o el análisis de preferencias de los clientes, así como problemas de optimización, como la selección de carteras, la determinación de estrategias óptimas de trading o el diseño de coberturas financieras eficientes. Gracias a los avances en las matemáticas financieras y en las técnicas computacionales, impulsados tanto por la industria financiera como por la comunidad científica, el sector ha desarrollado un conjunto diverso de herramientas basadas en modelización estocástica, algoritmos de optimización y modelos de aprendizaje automático para abordar estas cuestiones[47].

Por naturaleza, las finanzas se ocupan de la incertidumbre asociada al comportamiento futuro de los activos y a los rendimientos que estos pueden generar. El concepto de riesgo surge precisamente de la posibilidad de que el rendimiento efectivo difiera del rendimiento esperado inicialmente por el inversor. La cuantificación de dicho riesgo depende de la distribución probabilística de los retornos, lo que introduce conceptos fundamentales como la volatilidad, entendida como el grado de variación de los precios a lo largo del tiempo[48]. Con el objetivo de reducir el riesgo y mejorar la toma de decisiones, resulta esencial analizar el comportamiento de los activos y su relación con la información de mercado disponible. Este ámbito, conocido como predicción financiera, plantea desafíos de gran relevancia tanto práctica como teórica. En las últimas décadas, las técnicas de inteligencia artificial y aprendizaje automático han demostrado una notable eficacia en la resolución de este tipo de problemas, consolidándose como herramientas clave dentro de la infraestructura tecnológica del sector financiero[49].

En este contexto, caracterizado por la elevada complejidad computacional y la necesidad constante de procesar grandes volúmenes de información bajo condiciones de

[47] Herman, D., Googin, C., Liu, X., Sun, Y., Galda, A., Safro, I., ... & Alexeev, Y. (2023). Quantum computing for finance. *Nature Reviews Physics*, *5*(8), 450-465.
[48] Orús, Román, Samuel Mugel y Enrique Lizaso. (2019a). "Quantum computing for finance: Overview and prospects". Reviews in Physics, 4, p. 100028.
[49] Id.

incertidumbre, los avances tecnológicos como la computación cuántica se presentan como candidatos potencialmente disruptivos para el sector financiero. No obstante, conviene subrayar que los ordenadores cuánticos no son simplemente procesadores más rápidos capaces de sustituir de forma directa a los sistemas clásicos en cualquier tarea. Se trata de un mecanismo computacional fundamentalmente distinto que, aplicando los algoritmos cuánticos adecuados, puede ofrecer ventajas significativas únicamente en determinados problemas específicos[50]. De este modo, surge una cuestión central desde el punto de vista algorítmico: ¿admite la aplicación considerada una mejora cuántica real en términos de complejidad computacional? Es decir, antes de plantear la adopción de esta tecnología, resulta imprescindible analizar si el problema financiero en cuestión posee una estructura que permita explotar las propiedades de la computación cuántica, como la superposición o la interferencia, para obtener una reducción sustancial en el número de operaciones necesarias[51].

A continuación, se examinarán los principales desafíos computacionales presentes en la industria financiera, en ámbitos como la valoración de activos, la gestión del riesgo, la optimización de carteras o la detección de anomalías, y se analizarán las soluciones o mejoras específicas que la computación cuántica ofrece actualmente, así como aquellas que, según la literatura académica y el desarrollo tecnológico previsto, podrían materializarse en el medio plazo.

[50] Bouland, A., van Dam, W., Joorati, H., Kerenidis, I., & Prakash, A. (2020). Prospects and challenges of quantum finance. *arXiv preprint arXiv:2011.06492, p 2.*
[51] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79, p6.

CAPÍTULO 3: Modelización y simulación financiera

1. La incertidumbre como punto de partida: modelos estocásticos en finanzas

En el ámbito financiero, la modelización constituye una herramienta fundamental para analizar y anticipar el comportamiento futuro de variables económicas bajo condiciones de incertidumbre. Este tipo de análisis puede aplicarse al precio de una acción, al valor agregado de una cartera de inversión, a la valoración de un derivado financiero o incluso a la estimación del riesgo de impago de un préstamo. En todos estos casos, el objetivo no es predecir un único resultado determinista, sino caracterizar un conjunto de escenarios posibles y evaluar su impacto económico.

Dado que el futuro es inherentemente incierto, la modelización financiera recurre a herramientas de probabilidad y estadística para describir la evolución de los mercados. En particular, es habitual emplear modelos estocásticos, es decir, modelos matemáticos que describen la variación temporal de una variable aleatoria cuyo comportamiento futuro no está determinado, sino que este sujeto a una distribución de probabilidades[52]. De este modo, en lugar de afirmar que un activo tendrá un valor concreto en el futuro, se describe como podría evolucionar bajo distintos escenarios probabilísticos. Un ejemplo clásico de modelización estocástica es la ecuación de Black-Scholes, utilizada para calcular el precio teórico de opciones europeas sobre activos cuyo precio sigue un movimiento browniano geométrico. Este modelo, proporciona una solución analítica cerrada bajo determinados supuestos, y constituye uno de los pilares de la teoría moderna de derivados financieros[53].

2. El método Monte Carlo: fundamentos y aplicaciones financieras

Sin embargo, en la práctica financiera la mayoría de los instrumentos presentan estructuras más complejas para las cuales no existen soluciones analíticas explicitas. En estos casos, es necesario recurrir a métodos alternativos. Aquí, el método de Monte Carlo se ha consolidado como una de las herramientas más relevantes, que recibe su nombre nada menos que de la famosa casa del azar, el casino de Monte Carlo en Mónaco. Este método es una técnica computacional basada en el muestreo aleatorio masivo que permite

[52] Herman et al (2023) p.2.
[53] Black, F., & Scholes, M. (1973). The pricing of options and corporate liabilities. *Journal of Political Economy, 81*(3), 637–654.

obtener aproximaciones numéricas cuando no existe una solución determinista accesible[54].

En términos formales, el procedimiento parte de un modelo estocástico S que describe la dinámica del mercado, por ejemplo, la evolución aleatoria de los precios de distintos activos, y tiene como objetivo estimar una función f definida sobre dichas trayectorias. Esta función puede representar magnitudes diversas. Un ejemplo es el cálculo del *Value at Risk (VaR)*, donde se estima la pérdida máxima potencial de una cartera en un horizonte temporal determinado, excluyendo un pequeño porcentaje de eventos extremos. Otro ejemplo es la valoración de un derivado financiero, cuyo precio depende de forma compleja de la evolución futura del mercado. En este último caso, el valor del derivado V se define como el valor esperado de la función f, promediado sobre todos los posibles estados futuros del mercado[55].

La estimación mediante Monte Carlo consiste en simular el modelo *S* un gran número *N* de veces, generando distintas trayectorias $x_1, x_2, ..., xn$ a partir de semillas aleatorias independientes. Para cada trayectoria se calcula el valor correspondiente $f(x_i)$, que puede interpretarse como el *payoff* del derivado bajo ese escenario concreto. El valor buscado se aproxima entonces mediante la media empírica[56]:

$$\tilde{V} = \frac{1}{N}\sum_{i=1}^{N} f(x_i) \qquad (3.2)$$

Esta cantidad $\tilde{V}$ se utiliza como estimación del valor esperado real V.

3. Limitaciones computacionales del Monte Carlo clásico

El aspecto crítico de este método no reside en su formulación conceptual, sino en su coste computacional. El error de estimación disminuye proporcionalmente a $1/\sqrt{N}$, lo que implica que la precisión mejora de forma lenta a medida que aumenta el número de simulaciones. En términos prácticos, si se desea reducir el error en un factor de 10, es necesario multiplicar por 100 el número de simulaciones. Esto tiene consecuencias

[54] Montanaro, A. (2015). Quantum speedup of Monte Carlo methods. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *471*(2181), 20150301.
[55] Bouland et al (2020) p 6.
[56] Id.

significativas cuando se requieren altos niveles de precisión: alcanzar exactitudes del orden de 10^{-3} o 10^{-5} en la valoración de derivados puede exigir desde millones hasta miles de millones de simulaciones[57]. Este es el caso de las simulaciones del mercado bursátil, que suelen prolongarse durante días[58].

Por tanto, aunque el método de Monte Carlo es extremadamente versátil y ampliamente utilizado en la práctica financiera, su principal limitación es computacional. Obtener estimaciones altamente precisas implica un consumo considerable de tiempo y recursos de cálculo, lo que abre la puerta a explorar nuevas tecnologías capaces de acelerar este tipo de procesos, como la computación cuántica.

4. Aceleración cuántica: el algoritmo de Monte Carlo cuántico (QMCI)

Si tradujésemos el método matemático de Monte Carlo (MCI) a un algoritmo, hemos visto que, para obtener un margen de error aceptable en la estimación de la media μ, sería necesario ejecutarlo millones de veces, debido a la dependencia cuadrática que existe en $O(\sigma^2/\varepsilon^2)$ en el número de muestras requeridas. Sin embargo, Ashley Montanaro demostró que, utilizando un ordenador cuántico para implementar un algoritmo de Monte Carlo cuántico (QMCI), el número de ejecuciones necesarias para aproximar μ puede reducirse de forma cuadrática con respecto al límite clásico anterior[59].

Mientras que el Monte Carlo clásico genera muestras aleatorias de forma secuencial y calcula su media empírica, la versión cuántica emplea una técnica denominada Estimación de Amplitud Cuántica (QAE)[60]. Este algoritmo se fundamenta en la técnica de amplificación de amplitudes derivada del algoritmo de Grover, quien en 1996 desarrolló un procedimiento que permite buscar un elemento concreto en una base de datos no estructurada de tamaño N con una complejidad de $O(\sqrt{N})$, frente a los $O(N)$ pasos necesarios en el mejor algoritmo clásico. Lo consigue preparando una superposición de todos los posibles estados y aplicando iterativamente un proceso de amplificación de amplitudes que aumenta la probabilidad del elemento buscado mediante interferencia

[57] Ibid p7.
[58] Orús et al (2019).
[59] Montanaro, A (2015), p.2.
[60] Bouland et al (2020), p.8.

cuántica. Tras aproximadamente $\sqrt{N}$ iteraciones, la probabilidad de medir el resultado correcto es alta, logrando así una mejora cuadrática en el número de pasos requeridos[61]. Partiendo de esto, el QMCI, aprovecha la superposición y la interferencia cuántica para estimar directamente la amplitud asociada al valor[62]. En lugar de simplemente promediar muestras individuales, el sistema codifica el valor esperado en la amplitud de un qubit auxiliar y utiliza QAE para extraer dicha amplitud de manera global y más eficiente[63]. Como resultado, Montanaro demostró que las simulaciones de Monte Carlo pueden ejecutarse en un ordenador cuántico utilizando del orden de $O\ (\sigma/\varepsilon)$ muestras, lo que supone una mejora cuadrática frente al escalado clásico $O\ (\sigma^2/\varepsilon^2)$, manteniendo además una alta probabilidad de éxito[64].

5. Aplicación a la valoración de derivados financieros

Esta mejora cuántica resulta especialmente relevante en el cálculo de valores esperados en finanzas. Un derivado financiero, es un activo contractual cuyo valor se basa en el precio de uno o más activos subyacentes, como acciones, índices, tipos de interés o divisas[65]. En la valoración de derivados financieros, el precio actual puede expresarse como el valor esperado del *payoff* futuro, descontado al presente. Cuando no existe una solución analítica, se estima mediante simulaciones de Monte Carlo, sin embargo, como hemos visto esto requiere un trabajo computacional enorme, lo que conlleva mucho tiempo y grandes recursos. El enfoque cuántico reformula este problema convirtiendo el valor esperado en la probabilidad de medir un determinado estado de un qubit, de modo que el precio queda codificado en una amplitud cuántica. Mediante el QAE, esa probabilidad puede extraerse con un numero de repeticiones que escala $N= O\ (1/\varepsilon)$, logrando así una mejora cuadrática respecto al método clásico. En términos prácticos, esto significa que alcanzar altos niveles de precisión en el cálculo del precio, especialmente en productos complejos o en carteras de gran tamaño, requeriría

[61] Rieffel, E., & Polak, W. (2000). *An introduction to quantum computing for non-physicists*. *ACM Computing Surveys, 32*(3), p322.
[62] Zhou, J. (2025). Quantum finance: Exploring the implications of quantum computing on financial models. *Computational Economics*, p22.
[63] Herman et al (2023) p.4.
[64] Montanaro, A (2015).
[65] Chakrabarti, S., Krishnakumar, R., Mazzola, G., Stamatopoulos, N., Woerner, S., & Zeng, W. J. (2021). A threshold for quantum advantage in derivative pricing. *Quantum*, *5*, 463.

significativamente menos recursos computacionales que en los métodos tradicionales basados en Monte Carlo[66].

[66] Rebentrost, P., Gupt, B., & Bromley, T. R. (2018). Quantum computational finance: Monte Carlo pricing of financial derivatives. *Physical Review A*, *98*(2), 022321.

CAPÍTULO 4: Optimización y gestión de carteras

1. La cartera de inversión: concepto y problema de optimización

Mas allá de la valoración de instrumentos individuales, la computación cuántica también presenta un potencial significativo en uno de los problemas centrales de la gestión financiera: la construcción y optimización de carteras de inversión.

Una cartera de inversión es un conjunto de activos financieros (acciones, bonos, fondos, divisas u otros instrumentos) distribuidos según una proporción determinada entre ellos. Así, una cartera podría estar compuesta, por ejemplo, por un 50% en bonos alemanes, un 25% en acciones del S&P 500 y un 25% en otros valores. La clave no reside únicamente en qué activos se incluyen, sino en qué peso se le asigna a cada uno, ya que esa distribución determina tanto la rentabilidad esperada de la cartera como el riesgo que el inversor asume. Si en el caso de los derivados el desafío residía en la precisión de las estimaciones bajo incertidumbre, en la gestión de carteras el problema adopta una naturaleza distinta: no se trata de calcular el valor estimado de un único activo, sino de encontrar la combinación óptima entre múltiples activos, equilibrando rentabilidad y riesgo de forma simultánea.

2. La teoría de Markowitz y la frontera eficiente

La teoría moderna de optimización de carteras fue desarrollada en sus inicios por Harry Markowitz[67] y describe cómo la riqueza puede invertirse de forma óptima en activos que difieren en rentabilidad esperada y nivel de riesgo[68]. Para alcanzar ese equilibrio, Markowitz señalaba que es posible reducir el riesgo de mantener un activo seleccionando cuidadosamente otros activos adicionales con los que combinarlo: o activos con retornos anti correlacionados, en lo que se conoce como cobertura o *hedging*, o activos no correlacionados entre sí, en lo que denominamos diversificación[69]. Estas ideas conducen de forma natural a la definición de cartera óptima: para un nivel de riesgo dado, existe una cartera que maximiza el retorno; y para un retorno dado, existe una cartera que minimiza el riesgo[70]. El conjunto de estas carteras óptimas forma lo que Markowitz denominó la "frontera eficiente", que representa el espacio de soluciones donde el

[67] Markowitz, H. (1952). Portfolio selection. *The Journal of Finance, 7*(1), 77–91.
[68] Kerenidis, I., Prakash, A., & Szilágyi, D. (2019)
[69] Orús et al (2019).
[70] Gálvez, P., Salgado, M., & Gutiérrez, M. (2010).

inversor racional debería operar. El problema relevante es, precisamente, cómo construir dicha cartera y cómo ajustarla en función de las condiciones cambiantes del mercado.

3. Complejidad computacional del problema: restricciones y escalabilidad

Supongamos que se distribuye una inversión entre *n* activos con distintas rentabilidades esperadas y cuyos rendimientos están correlacionados de alguna manera conocida. El objetivo es minimizar el riesgo de la cartera logrando al mismo tiempo una tasa de retorno objetivo. En su forma más simple, el problema es relativamente sencillo de resolver, ya que se reduce a un único sistema lineal de ecuaciones. Sin embargo, la dificultad computacional aumenta considerablemente a medida que se incorporan restricciones más realistas[71] y crece de forma exponencial con el número de activos considerados: seleccionar una cartera de diez activos de una lista potencial de cincuenta implica evaluar más de diez mil millones de combinaciones posibles[72]. Añadir condiciones adicionales como límites de inversión por activo, costes de transacción o restricciones regulatorias agrava aún más este problema, convirtiéndolo en uno de elevada complejidad computacional.

Las restricciones que condicionan estos problemas de optimización son diversas y determinan en gran medida la complejidad del problema resultante. En la búsqueda de la cartera optima, pueden incorporarse, entre otras, restricciones de positividad, que corresponden a situaciones en las que no es posible vender un activo en corto, o restricciones presupuestarias, que limitan la cantidad de capital que puede invertirse en un subconjunto de activos y pueden depender tanto del valor de los propios activos como del tamaño de la inversión inicial[73]. La forma en que se combinan estas restricciones determina no solo la estructura matemática del problema, sino también el método computacional más adecuado para resolverlo.

Encontrar el mejor resultado posible para un problema dado en función de las condiciones que lo rigen es precisamente lo que entendemos por optimización[74]. La optimización

[71] Bouland et al (2020), p 21.
[72] McKinsey & Company, 2021.
[73] Kerenidis, I., Prakash, A., & Szilágyi, D. (2019), p 148.
[74] Zanjirdar, *Overview of portfolio optimization models*, *Advances in Mathematical Finance & Applications*, (2020), p.420.

constituye uno de los campos de estudio más relevantes en el desarrollo de la computación cuántica, razón por la cual la optimización de carteras se proyecta como una de las aplicaciones más prometedoras en el ámbito financiero. Sin embargo, dado que no existe un enfoque universal valido para todos los problemas de optimización, debido a la variedad de restricciones y amplitud de activos a considerar, a lo largo del tiempo han surgido una amplia variedad de métodos adaptados a distintos tipos de problemas[75]. En el contexto concreto de la gestión de carteras, esto ha dado lugar a un amplio espectro de formulaciones: problemas mono y multiobjetivo, de periodo único o múltiple, con o sin costes de transacción, y de naturaleza determinista o estocástica, en todas sus combinaciones posibles[76].

4. Problemas *NP-hard* y los límites de la computación clásica

Trasladados al ámbito computacional, estos métodos se clasifican en su mayoría como problemas *NP-hard*. Un problema *NP-hard* es aquel para el que no se conoce ningún algoritmo que sea capaz de resolverlo de forma exacta en un tiempo razonable según crece el tamaño del problema. En términos prácticos, esto significa que el tiempo de cómputo que el ordenador requiere para encontrar la solución óptima crece de forma exponencial con el número de variables: lo que para un problema pequeño puede resolverse en segundos, se vuelve computacionalmente inabordable cuando el número de activos y restricciones aumenta. Los problemas de programación cuadrática entera, categoría en la que se encuadra la optimización de carteras con variables binarias, son NP-hard por lo general[77], lo que explica que los ordenadores clásicos encuentren serias limitaciones cuando se enfrentan a este tipo de problemas.

5. La computación cuántica como alternativa: QAOA y *Quantum Annealing*

Frente a estos desafíos, la computación cuántica abre una vía alternativa con un potencial significativo. Por un lado, algoritmos como el Quantum Approximate Optimisation Algorithm (QAOA)[78], diseñado para ordenadores cuánticos de puertas, pueden ofrecer mejoras en ciertos escenarios, sin embargo, el avance más esperado en el horizonte próximo se asocia al *quantum annealing*. Rosenberg argumenta que el *quantum annealing*

[75] Ibid p 421.
[76] Phillipson & Bhatia, *Portfolio optimisation using the D-Wave quantum annealer*, arXiv, 2020, p.2.
[77] Ibid.
[78] Zhou (2025).

presenta una ventaja sobre los optimizadores clásicos gracias al fenómeno del efecto túnel cuántico. Este efecto permite al sistema de optimización explorar el espacio de soluciones con mayor facilidad, aumentando la probabilidad de encontrar la solución óptima y pudiendo ofrecer una mejora en velocidad respecto a los métodos clásicos, al menos para determinadas clases de problemas. En este sentido, existe un creciente interés en evaluar el rendimiento de las máquinas D-Wave, así como un debate activo sobre cómo definir la ventaja cuántica y en qué tipos de problemas cabría esperarla[79].

6. Resultados empíricos y aplicaciones reales

Los primeros resultados en esta dirección son alentadores. En su estudio, Phillipson y Bhatia consiguieron demostrar que el sistema híbrido de D-Wave, que combina computación clásica con un procesador cuántico, es capaz de encontrar soluciones al problema de optimización de carteras dentro de un margen del 3% respecto a la solución óptima para índices de hasta 400 activos como el S&P500, empleando tiempos de cómputo notablemente reducidos frente a los métodos clásicos convencionales[80]. Aunque los ordenadores cuánticos se encuentran todavía en una fase temprana de desarrollo, la evolución previsible de estos sistemas, tanto en número de qubits como en la madurez de sus *solvers* híbridos, permite anticipar que la optimización cuántica de carteras se convertirá en una herramienta de aplicación real en el sector financiero en los próximos años.

Este potencial no se limita al terreno académico. Un ejemplo concreto de su aplicación práctica lo protagonizaron BBVA y la *startup* española Multiverse Computing, que llevaron a cabo una prueba en la que evaluaron y compararon distintas plataformas de tecnología cuántica para resolver un problema de optimización dinámica de carteras con datos reales de mercado, publicando los resultados en un trabajo académico[81]. El objetivo era determinar la trayectoria de negociación óptima de una cartera compuesta por 52 activos, utilizando precios diarios reales durante un periodo de ocho años, y encontrar la mejor combinación posible entre más de diez mil candidatos de forma dinámica, ajustando los pesos de la cartera en función de la evolución del mercado. Una operación de esta magnitud habría requerido aproximadamente dos días de procesamiento en un

[79] Rosenberg et al., *Solving the optimal trading trajectory problem using a quantum annealer*, 2015.
[80] Phillipson & Bhatia, 2020.
[81] Mugel et al., *Dynamic portfolio optimization with real datasets*, *Physical Review Research*, 2022.

ordenador clásico con algoritmos convencionales; sin embargo, según los resultados del estudio, los algoritmos cuánticos permitirían realizarlo en cuestión de segundos. Los autores concluyen que las herramientas basadas en computación cuántica, así como los algoritmos de inspiración cuántica, ya podrían superar a los métodos tradicionales para esta tarea, y señalan que se trata de la primera vez que se utilizan tecnologías cuánticas para optimizar una cartera de inversión con un tamaño suficientemente grande como para tener valor comercial[82]. Este caso ilustra con claridad cómo la computación cuántica está dejando de ser una promesa teórica para convertirse en una herramienta con aplicaciones reales y tangibles en la gestión financiera.

[82] BBVA, *BBVA y Multiverse demuestran cómo la computación cuántica puede optimizar la gestión de carteras*, (2022).

CAPÍTULO 5: *Machine learning* cuántico

1. *Machine learning* en finanzas: fundamentos y aplicaciones

El *machine learning* (ML) es una rama de la inteligencia artificial que permite a los ordenadores identificar y reconocer patrones a partir de datos históricos y utilizarlos para hacer predicciones o tomar decisiones sobre nueva información, sin necesidad de ser programados explícitamente para cada tarea[83]. En términos sencillos, es como entrenar a un sistema para que, después de haber visto miles de ejemplos, sea capaz de reconocer situaciones nuevas y actuar en consecuencia. En el mundo financiero, esto resulta especialmente útil porque los mercados generan cantidades enormes de datos como precios históricos, indicadores macroeconómicos, comportamientos de clientes, transacciones, etc. El ML permite entonces extraer información relevante de estos datos y realizar predicciones, clasificaciones o segmentaciones.

El Quantum Machine Learning (QML) busca integrar propiedades cuánticas como la superposición y el entrelazamiento en estos algoritmos. Sin embargo, a diferencia de otros ámbitos de la computación cuántica, la ventaja cuántica en el machine learning no está plenamente demostrada[84]. Por ello, la investigación actual se centra en el desarrollo de modelos híbridos, enfoques que combinan componentes clásicos y cuánticos dentro de un mismo sistema. En estos modelos, ciertas partes del cálculo se delegan a un procesador cuántico, mientras que el resto se sigue ejecutando en hardware clásico[85]. Este enfoque permite combinar la solidez y madurez de los modelos clásicos ya consolidados con las capacidades que ofrece la computación cuántica, sin necesidad de depender de un hardware cuántico universal que todavía no existe.

En efecto, el sector financiero hace un uso intensivo del *machine learning* en prácticamente todas sus áreas de negocio. Entre las aplicaciones más relevantes se encuentran la gestión de riesgo, detección de fraude, predicción de precios de activos, la gestión automatizada de carteras, el *trading* algorítmico y la evaluación crediticia[86]. En todas estas aplicaciones, el reto computacional es similar: procesar volúmenes enormes de datos de alta dimensión para extraer patrones útiles, y hacerlo con la suficiente rapidez

[83] Mironowicz et al. (2024), Applications of quantum machine learning for quantitative finance.
[84] Orús et al (2019), p.7.
[85] Faruk et al (2023). Quantum computing in machine learning: A hybrid quantum-classical approach.
[86] Bouland et al (2020), p 21.

como para que el resultado sea relevante en la práctica. Es precisamente aquí donde el QML podría marcar una diferencia significativa.

Analizamos a continuación una de las aplicaciones más relevantes del *machine learning* en el sector financiero y las posibles mejoras cuánticas que se proyectan en este ámbito. Si bien el QML abarca una amplia variedad de algoritmos y enfoques, como la regresión, el *clustering* o las redes neuronales, nos centraremos en el caso de uso con mayor potencial de impacto inmediato para la industria financiera: la evaluación del riesgo crediticio y el *credit scoring*.

2. Riesgo crediticio y clasificación

El *credit risk* o riesgo crediticio hace referencia a la posibilidad de que un prestatario no cumpla con sus obligaciones de pago. Estimar este riesgo antes de conceder un préstamo es uno de los retos fundamentales del sector financiero, ya que determina directamente las condiciones que se ofrecen al cliente y es esencial para garantizar la estabilidad y sostenibilidad de la entidad prestamista[87].

Para llevar a cabo esta evaluación, los bancos utilizan algoritmos de clasificación que analizan las características de cada cliente, como su historial crediticio, sus ingresos o su nivel de endeudamiento, y los comparan con los de clientes anteriores cuyos datos ya se conocen. En términos técnicos, cada cliente se representa como un punto en un espacio multidimensional donde cada dimensión corresponde a una de sus características. El algoritmo examina los clientes históricos más similares a ese nuevo solicitante y, en función de cómo se comportaron, le asigna una categoría de riesgo[88]. Aunque existen diversas variantes, la regresión logística ha sido tradicionalmente el método de referencia en la banca para este tipo de clasificación.

3. Aplicación del QML al credit scoring: estado del arte y resultados

Aunque la aplicación del QML al *credit scoring* es todavía un campo emergente, los resultados de las investigaciones realizadas hasta la fecha apuntan en una dirección prometedora. Por un lado, los algoritmos cuánticos podrían integrarse como componentes

[87] Doosti et al. (2024), A brief review of quantum machine learning for financial services.
[88] Orús et al. (2019), Quantum computing for finance: Overview and prospects, *Reviews in Physics*, p 7.

acelerados dentro de los sistemas de clasificación clásicos ya existentes. En esta línea, Doosti et al introducen un estudio reciente que desarrolló un método de *machine learning* mejorado cuánticamente para predecir calificaciones crediticias, implementado en un procesador cuántico de átomos neutros con hasta 60 qubits. Los resultados mostraron un rendimiento competitivo respecto a los mejores modelos clásicos, con una mayor interpretabilidad y tiempos de entrenamiento comparables a los de los modelos de *random forest* más avanzados[89].

Por otro lado, una alternativa consiste en desarrollar versiones completamente cuánticas de estos algoritmos de clasificación. La idea central es que, en lugar de comparar clientes calculando distancias matemáticas de la forma habitual, un ordenador cuántico puede estimar esas mismas similitudes de forma mucho más eficiente, aprovechando la naturaleza probabilística de los estados cuánticos para realizar múltiples comparaciones de forma simultánea[90]. Aunque todavía en fases tempranas de desarrollo, este enfoque podría permitir en el futuro procesar volúmenes de datos significativamente mayores con un coste computacional notablemente inferior al de los métodos actuales.

4. Impacto económico

De esta forma, el impacto potencial del QML en la evaluación del riesgo crediticio no es solo técnico, sino profundamente económico. Un estudio de McKinsey estima que una mejora de tan solo uno o dos puntos porcentuales en la tasa de impago global, como la que podría derivarse de modelos de *credit scoring* más precisos, se traduciría en un ahorro de entre 17.000 y 33.000 millones de dólares, una cifra que supera incluso el impacto estimado de las mejoras obtenidas a través de los métodos de análisis de riesgo convencionales, valoradas entre 10.000 y 20.000 millones de dólares[91]. Estos números ilustran con claridad por qué la industria financiera sigue de cerca el desarrollo del QML, y es que, las ganancias en precisión, aunque sean marginales, pueden tener consecuencias económicas de escala extraordinaria.

[89] Leclerc et al., *Financial risk management on a neutral atom quantum processor*, *Physical Review Research*, 2023.
[90] Orús et al. (2019).
[91] McKinsey. (2021).

CAPÍTULO 6: Criptografía y seguridad financiera en la era cuántica.

1. Los fundamentos de la criptografía y la amenaza cuántica

En la nueva era tecnológica en la que vivimos, el intercambio electrónico de información se ha convertido en uno de los pilares fundamentales de la sociedad moderna. Sectores tan críticos como el sistema bancario, la sanidad o la seguridad nacional dependen por completo de la capacidad de transmitir y almacenar datos de forma segura. En este contexto, la necesidad de garantizar la confidencialidad, la integridad y la autenticidad de las comunicaciones convierte a la criptografía en una de las disciplinas más importantes de la tecnología de la información actual[92].

Etimológicamente, el término criptografía proviene del griego *kryptos*, que significa "oculto", y *graphia*, "escritura". De forma práctica, describe la ciencia que desarrolla y utiliza algoritmos codificados para proteger la información transmitida, de modo que únicamente quienes cuenten con los permisos y las claves adecuadas puedan acceder a ella[93]. En otras palabras, la criptografía actúa como un escudo que hace ininteligible cualquier comunicación para aquellos que no estén autorizados a leerla.

En la actualidad existen distintos sistemas criptográficos para proteger las comunicaciones electrónicas. Por un lado, la encriptación simétrica utiliza una única clave tanto para cifrar como para descifrar la información, siendo el sistema AES (Advanced Encryption Standard) su principal representante, ampliamente utilizado para proteger datos almacenados y comunicaciones internas[94]. Por otro lado, la encriptación asimétrica emplea un par de claves distintas, una pública y una privada, de forma que lo que una cifra solo la otra puede descifrarlo. El sistema RSA, cuyo nombre proviene de sus creadores Rivest, Shamir y Adleman, es el algoritmo asimétrico por excelencia y el más utilizado para securizar transacciones financieras a nivel global. Existen además sistemas híbridos que combinan ambos enfoques para aprovechar las ventajas de cada uno, como el protocolo TLS, que protege la gran mayoría de las conexiones seguras en internet[95].

---

[92] Dalwadi, "The future of financial data security: Challenges and opportunities of quantum computing," 2025.
[93] IBM (s.f.)
[94] Chamorro, (2024).
[95] Id.

La robustez de estos sistemas, y en particular del RSA, se fundamenta en un principio matemático aparentemente sencillo, pero computacionalmente devastador para cualquier atacante: la factorización de números primos de gran tamaño. Multiplicar dos números primos enormes es una operación trivial para cualquier ordenador, pero deducir cuáles son esos dos números a partir de su producto requiere un esfuerzo computacional colosal[96]. Para hacerse una idea de la magnitud del reto, un ordenador clásico tardaría varios meses en factorizar una clave de 512 bits, aproximadamente 1.000 años para una de 768 bits, y alrededor de un millón de años para una de 1.024 bits. En el caso de las claves RSA de 2.048 bits, el estándar actual en el sector financiero, el tiempo necesario para romperlas mediante métodos clásicos se mide en millones de años, lo que en la práctica las hace inquebrantables con la tecnología convencional[97].

Sin embargo, este equilibrio se vio sacudido en 1994, cuando el matemático Peter Shor desarrolló un algoritmo cuántico capaz de factorizar números enteros de forma exponencialmente más eficiente que cualquier método clásico conocido[98]. Lo que para un ordenador convencional requeriría millones de años, el algoritmo de Shor podría resolverlo en cuestión de horas o incluso minutos en un ordenador cuántico suficientemente potente. En términos prácticos, esto significa que la llegada de la computación cuántica a gran escala podría dejar obsoletos de un día para otro los sistemas criptográficos sobre los que descansa toda la seguridad del sistema financiero global.

Además, no debemos perder de vista el algoritmo de Grover, al que hacíamos referencia en apartados anteriores[99]. Si el algoritmo de Shor supone una amenaza directa para la encriptación asimétrica como el RSA, el algoritmo de Grover hace lo propio con los sistemas de encriptación simétrica como el AES. Al ser capaz de realizar búsquedas en bases de datos de forma cuadráticamente más rápida que cualquier método clásico, reduciría a la mitad el número de bits efectivos de cualquier clave simétrica, debilitando sustancialmente su seguridad[100]. Juntos, ambos algoritmos cuánticos representan una

[96] Id.
[97] Kleinjung et al., 2010, citado en Chamorro, 2024.
[98] Shor, (1994).
[99] Ver capítulo 1.2 y capítulo 3.4.
[100] Chamorro. (2024).

amenaza integral para la totalidad de la infraestructura criptográfica sobre la que se asienta hoy el sistema financiero global.

2. El riesgo real: proyecciones y vulnerabilidades del sistema financiero

Como hemos podido ver, el desarrollo de estos algoritmos cuánticos pondría en jaque el sistema de encriptación de información y comunicaciones tal y como está diseñado hoy en día. Si bien más adelante abordaremos las limitaciones actuales de la computación cuántica que frenan esta amenaza, y que hacen que la existencia de un ordenador cuántico capaz de romper los sistemas de encriptación vigentes sea todavía cuestión de años, sería ingenuo ignorar la dirección en la que apuntan las proyecciones.

En este sentido, los doctores Mosca y Piani, fundadores e investigadores senior de la firma especializada en seguridad cuántica Evolution Q, llevaron a cabo en 2024 una encuesta entre expertos en computación cuántica de todo el mundo para recabar su visión sobre el futuro de esta tecnología. Los resultados son reveladores: en un horizonte de 15 años, más de la mitad de los expertos consultados consideró que existe al menos un 50% de probabilidad de que exista un ordenador cuántico capaz de comprometer los sistemas criptográficos actuales, y un tercio de ellos elevó esa probabilidad por encima del 70%. Las perspectivas a 30 años son aún más contundentes: el 88% de los expertos asignó a esta amenaza una probabilidad superior al 70%, con varios de ellos situándola por encima del 99%, lo que refleja un amplio consenso sobre la inevitabilidad de esta transición a largo plazo[101].

Ante este horizonte, una de las estrategias que mayor preocupación genera entre los expertos en ciberseguridad es la conocida como *harvest now, decrypt later*, o "recolectar ahora, descifrar después". Esta táctica consiste en capturar y almacenar hoy grandes volúmenes de datos encriptados, con la intención de descifrarlos en el futuro, cuando dispongan de la capacidad cuántica necesaria para hacerlo. Esto significa que información considerada completamente segura ahora podría quedar expuesta en el futuro, lo que amenaza la confidencialidad a largo plazo de datos financieros, registros de clientes y comunicaciones sensibles[102].

[101] Mosca, M., & Piani, M. (2024). *Global Risk Institute: Quantum Threat Timeline Report 2022*.
[102] Dalwadi, P. (2025). The Future of Financial Data Security: Challenges and Opportunities of Quantum Computing, p.56.

La magnitud de esta amenaza es difícil de exagerar. Cualquier entidad que almacene información sensible a largo plazo se encuentra en el punto de mira: gobiernos, instituciones financieras, proveedores sanitarios, empresas multinacionales. Una brecha cuántica no solo implicaría filtraciones de datos, sino fallos operativos en infraestructuras críticas como redes energéticas, sistemas de transporte o plataformas financieras, con el potencial de desencadenar crisis en cascada. En el ámbito empresarial, la exposición de propiedad intelectual, secretos comerciales o estrategias corporativas podría causar daños irreparables en términos de competitividad y reputación[103]. En definitiva, la amenaza cuántica no es un riesgo futuro abstracto, sino un desafío que el sector financiero y los gobiernos deben comenzar a gestionar de forma urgente.

3. Criptografía post-cuántica: la respuesta del sector

De esta forma, gobiernos e instituciones llevan años preparándose para el eventual *Q-Day*, es decir, el momento en que los ordenadores cuánticos sean capaces de romper los sistemas de encriptación clásicos, exponiendo datos sensibles y creando una necesidad urgente de medidas de seguridad cuánticamente seguras[104]. Para hacer frente a este escenario, la comunidad científica y tecnológica trabaja en el desarrollo de lo que se conoce como Criptografía Post-Cuántica (PQC, por sus siglas en inglés), un conjunto de nuevos algoritmos criptográficos basados en las leyes de la mecánica cuántica, diseñados específicamente para resistir ataques tanto de ordenadores clásicos como cuánticos[105]. Dentro de este campo destacan algoritmos como la Distribución Cuántica de Claves (QKD) y la Generación Cuántica de Números Aleatorios (QRNG), cuyo correcto desarrollo e implementación permitirían tanto blindar la criptografía existente como sentar las bases de nuevos métodos de encriptación robustos frente a las amenazas cuánticas.

El potencial de este mercado es considerable. Según estimaciones de McKinsey, el mercado de comunicaciones cuánticas podría alcanzar entre 11.000 y 15.000 millones de dólares en 2035. Actualmente, los gobiernos y el sector de la defensa lideran este espacio con una cuota de mercado estimada del 62-66% en 2023, pero se espera que los servicios

[103] SSH Communications Security. (s.f.)
[104] McKinsey, (2025).
[105] IBM, (s.f).

financieros emerjan como uno de los principales casos de uso, con una cuota proyectada de entre el 14 y el 24% en 2035, aunque con incertidumbre significativa en cuanto a los tiempos de adopción[106].

En este contexto, ya son numerosas las iniciativas institucionales y privadas que trabajan activamente para liderar la transición hacia la era post-cuántica. A nivel institucional, el National Institute of Standards and Technology (NIST) de Estados Unidos encabeza este proceso mediante un programa de estandarización de algoritmos criptográficos resistentes a la computación cuántica, cuyo objetivo es establecer los nuevos estándares de seguridad globales. En Europa, el Quantum-Safe Financial Forum, liderado por Europol, ha instado al sector financiero a comenzar a prepararse de forma proactiva frente a los riesgos que plantean los ordenadores cuánticos, identificando los estándares criptográficos vulnerables, buscando alternativas seguras y planificando los cambios operativos necesarios para salvaguardar tanto la confidencialidad de los clientes como la autenticación de las comunicaciones[107].

En el sector privado, algunos de los actores más relevantes del panorama financiero y tecnológico ya se posicionan para afrontar la llegada del *Q-Day*. JPMorgan Chase e IBM han establecido una colaboración estratégica orientada a explorar las aplicaciones de la computación cuántica en ciberseguridad, con el objetivo de desarrollar soluciones criptográficas avanzadas capaces de proteger los datos financieros más sensibles ante las amenazas que se avecinan[108]. Iniciativas como esta reflejan que la seguridad post-cuántica ha dejado de ser una preocupación teórica para convertirse en una prioridad estratégica real dentro del sector.

[106] McKinsey, (2025).
[107] Dalwadi, P. (2025).
[108] The Quantum Insider, (2025).

CAPÍTULO 7: Limitaciones actuales de la computación cuántica

A lo largo de este trabajo hemos podido observar cómo la computación cuántica ofrece ventajas significativas en determinados problemas de gran relevancia para el sector financiero. Sin embargo, existe una distancia considerable entre lo que esta tecnología promete y lo que es capaz de ofrecer hoy de forma fiable y a escala. Esa distancia no se debe a limitaciones conceptuales del paradigma cuántico, sino a un conjunto de desafíos técnicos y de ingeniería que condicionan el ritmo al que estos avances pueden materializarse. En las páginas siguientes se exponen los principales obstáculos que enfrenta actualmente la tecnología: la decoherencia y el ruido, la corrección de errores, los retos de escalabilidad del *hardware* y la brecha que todavía separa los dispositivos actuales de los ordenadores cuánticos tolerantes a fallos que harían plenamente posibles las aplicaciones descritas a lo largo del trabajo.

1. Decoherencia, ruido y corrección de errores cuánticos

Se podría decir que el núcleo del problema, y el principal desafío que presenta la tecnología cuántica en su estado actual, tiene que ver con lo que se conoce como coherencia cuántica. Como explica el físico John Preskill, el problema fundamental reside en que cualquier observación de un sistema cuántico genera inevitablemente una perturbación incontrolable sobre él . Esto crea una contradicción inherente: el ordenador cuántico necesita estar perfectamente aislado del mundo exterior para preservar los estados cuánticos, pero al mismo tiempo debe permitir que los qubits interactúen entre sí y con el exterior para poder procesar información y leer los resultados[109].

Las perturbaciones que amenazan ese aislamiento pueden provenir de fuentes muy diversas: vibraciones mecánicas, radiación electromagnética residual, fluctuaciones térmicas, campos magnéticos externos o incluso la interacción con los propios materiales del sustrato sobre el que se fabrican los qubits[110]. En el ámbito de la computación cuántica, estas perturbaciones se denominan colectivamente *"*ruido", y su efecto sobre el sistema es lo que se conoce como decoherencia. En términos técnicos, la decoherencia describe "el proceso por el cual un qubit deja de encontrarse en un estado cuántico puro

[109] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79, p 4.
[110] SpinQ Technology. (2025). *Why coherence matters in quantum research: The 2025 Nobel Prize.*

y pasa a comportarse como una mezcla estadística de estados, perdiendo las relaciones entre los componentes de la superposición que son esenciales para que funcionen la interferencia y otros efectos cuánticos"[111]. En términos prácticos, cuando un qubit entra en estado de decoherencia el sistema pierde la ventaja cuántica frente a los ordenadores clásicos.

El propio Preskill acuñó el término NISQ, *Noisy Intermediate-Scale Quantum*, para describir la era actual de la tecnología cuántica: dispositivos con un número de qubits que oscila entre decenas y algunos miles, pero cuya fiabilidad sigue estando severamente limitada por el ruido. Un ejemplo de cómo los ingenieros tratan de combatir este problema es el de los qubits superconductores, utilizados por empresas como Google, IBM o SpinQ, que operan a temperaturas próximas al cero absoluto, equivalente a -273,15 ºC, para minimizar las interferencias externas[112]. Sin embargo, incluso en estas condiciones extremas, perturbaciones residuales como vibraciones microscópicas, radiación electromagnética o interacciones con los materiales circundantes provocan decoherencia.

Sin embargo, la investigación avanza rápidamente, y los avances más recientes muestran que la decoherencia está dejando de ser una barrera insuperable para convertirse en un problema de ingeniería abordable. El reconocimiento más significativo de este progreso llegó en octubre de 2025, cuando la Real Academia Sueca de las Ciencias concedió el Premio Nobel de Física a John Clarke, Michel H. Devoret y John M. Martinis, tres profesores de la Universidad de California Berkley, por el descubrimiento del efecto túnel cuántico macroscópico y la cuantización de la energía en un circuito eléctrico[113]. En sus experimentos, realizados en la Universidad de California en Berkeley a mediados de los años ochenta, los tres investigadores demostraron que circuitos eléctricos formados por miles de millones de electrones podían exhibir comportamiento cuántico a escala macroscópica, observable y manipulable, algo que hasta entonces se consideraba exclusivo del mundo subatómico. La relevancia de este hallazgo para el problema de la decoherencia es directa: al demostrar que la frontera entre el comportamiento cuántico y el clásico no es un límite fundamental sino una cuestión de diseño e ingeniería, su trabajo

[111] Preskill, J. (2018).
[112] Spin Q (2025-d).
[113] The Royal Swedish Academy of Sciences. (2025). *Scientific background to the Nobel Prize in Physics 2025*.

abrió la puerta al desarrollo de sistemas cuánticos artificiales en los que la decoherencia puede combatirse activamente mediante mejoras en los materiales, el diseño de circuitos y el control criogénico[114].

2. Corrección de errores cuánticos

Es precisamente en esa dirección donde se concentra hoy uno de los esfuerzos más importantes del sector: el desarrollo de la corrección de errores cuánticos, conocida por sus siglas en inglés QEC (Quantum Error Correction). La idea central consiste en combinar múltiples qubits físicos poco fiables de forma que, cuando uno de ellos comete un error, los demás puedan detectarlo y corregirlo, creando así una redundancia que permite al sistema operar sin necesidad de medir directamente el estado de cada qubit, lo que destruiría la superposición[115]. De este modo, un conjunto de qubits físicos actúa colectivamente como un número menor de qubits lógicos, mucho más resistentes al ruido y capaces de sostener cálculos más complejos[116]. Sin embargo, los avances en este frente siguen siendo limitados: los tiempos de coherencia intrínsecamente cortos de los qubits actuales, frecuentemente medidos en microsegundos, imponen una presión extrema sobre la eficiencia de los protocolos de corrección, que deben actuar más rápido de lo que los errores se acumulan.

Desarrollar un sistema de QEC lo suficientemente avanzado es un paso primordial en el camino hacia lo que se conoce como *fault-tolerant quantum computing* (FTQC) o computación cuántica tolerante a fallos, una etapa en la que los ordenadores cuánticos serían capaces de realizar operaciones de alto nivel sin ser susceptibles a niveles de error que comprometan el resultado. Para que esto sea viable, el QEC debe ser capaz de combinar múltiples qubits físicos en qubits lógicos cuya tasa de error se reduzca de forma exponencial a medida que se añaden más qubits al sistema. Sin embargo, esta supresión exponencial del error solo se produce si la tasa de error de los qubits físicos se mantiene por debajo de un umbral crítico[117]. Superar ese umbral es, precisamente, uno de los mayores retos técnicos del campo.

[114] Spin Q (2025-c).
[115] Ibid.
[116] Riverlane (2025).
[117] Trond et al. (2025), "Quantum error correction below the surface code threshold," *Nature*.

En este sentido, a finales de 2024 Google presentó un avance de gran relevancia en esta dirección: Willow, un procesador cuántico de 105 qubits superconductores diseñado específicamente para demostrar que ese umbral crítico podía superarse en la práctica. Los resultados validaron décadas de desarrollo teórico en corrección de errores cuánticos, demostrando que es posible integrar todos los avances recientes en calidad de qubits, control del hardware y estabilización de qubits lógicos en un único sistema funcional[118]. Como prueba de su alcance, Willow ejecutó un cálculo de referencia estándar en menos de cinco minutos, una tarea que los mejores superordenadores clásicos tardarían un tiempo estimado de 10^{22} años en completar[119]. Este resultado no solo establece un nuevo estándar en la demostración de ventaja cuántica, sino que representa el avance más tangible hasta la fecha en el camino hacia la computación cuántica tolerante a fallos.

Por su parte, IBM ha desarrollado su propio *roadmap* hacia la computación cuántica tolerante a fallos, en el que proyecta una serie de hitos concretos a lo largo de la década. Entre ellos destacan la demostración de los primeros ejemplos de ventaja cuántica científica y un módulo tolerante a fallos en 2026, la diversificación de esa ventaja cuántica y el entrelazamiento de módulos tolerantes a fallos en 2027, y la entrega del primer ordenador cuántico tolerante a fallos en 2029, con el objetivo de desplegar la plena capacidad de la computación cuántica a escala a partir de 2033[120]. La hoja de ruta completa se recoge en el Anexo 3 de este trabajo.

3. El desafío de la escalabilidad: hardware e ingeniería

Más allá de la decoherencia y la corrección de errores, existe un conjunto de limitaciones prácticas de ingeniería que resultan igualmente determinantes para el desarrollo de la computación cuántica a gran escala, y que a menudo quedan fuera de las discusiones teóricas.

El primero de ellos tiene que ver con el control físico de los qubits. En las arquitecturas actuales, cada qubit requiere múltiples cables para poder ser manipulado y leído. En la práctica, esto significa que un procesador de tan solo 1.000 qubits necesita aproximadamente 10.000 cables, todos ellos conectados desde la electrónica exterior

[118] Qblox. (2025). *The quantum leap that needs error correction*.
[119] Ibid
[120] IBM. (2025). *IBM quantum roadmap*. IBM.

hasta el núcleo del sistema, que opera a temperaturas cercanas al cero absoluto como veíamos antes[121]. El problema es que cada cable conduce también una pequeña cantidad de calor hacia el interior, amenazando las condiciones criogénicas necesarias para que los qubits funcionen correctamente. A medida que el número de qubits crece, la cantidad de cables requerida hace que los diseños actuales sean difícilmente escalables, y como veíamos antes, un solo qubit lógico puede requerir cientos de qubits físicos para funcionar[122]. Para abordar este problema, diversas empresas trabajan en soluciones que permitan reducir drásticamente el número de conexiones necesarias, integrando parte de la electrónica de control directamente en el propio chip[123]. A esto se suma el elevado coste energético de mantener las condiciones de funcionamiento. Los sistemas de refrigeración que mantienen los procesadores cuánticos a las temperaturas requeridas consumen una cantidad considerable de energía de forma continua[124]. La paradoja es llamativa: se necesita una infraestructura enorme y muy costosa para hacer funcionar un chip cuyo consumo efectivo es mínimo. Este desequilibrio entre los recursos necesarios y la capacidad computacional actual es uno de los principales argumentos que cuestionan la viabilidad operativa de la computación cuántica a corto plazo, y representa uno de los frentes de investigación más activos en la actualidad[125].

[121] Oxionics. (2023). *Solving quantum computing's wiring dilemma: How to build a 1000-qubit computer without tens of thousands of wires*.
[122] Tencent Cloud. (2024). *What is quantum computing?* Tencent Cloud Techpedia.
[123] Oxionics. (2023).
[124] WiFiTalents. (2026). *Quantum industry statistics*
[125] Qilimanjaro Quantum Tech. (2025). *Quantum computing: Pioneering a sustainable path for future computing*.

CONCLUSIONES

Este trabajo ha permitido examinar en detalle de qué forma la computación cuántica proyecta ventajas significativas en algunos de los problemas computacionales más relevantes del sector financiero: la aceleración de los métodos de simulación y valoración mediante Monte Carlo cuántico, la optimización de carteras de inversión a través del *quantum annealing*, la mejora de los modelos de evaluación del riesgo crediticio mediante *machine learning* cuántico, y la amenaza que esta tecnología representa para los sistemas criptográficos sobre los que descansa hoy la seguridad financiera global. En todos estos ámbitos, las mejoras teóricas están respaldadas por una base académica sólida y, en algunos casos, por resultados experimentales ya contrastados.

A pesar de que la mayoría de estas aplicaciones se encuentran todavía en fases tempranas de desarrollo, o han sido implementadas únicamente a pequeña escala y en entornos controlados, el estado actual de la investigación permite afirmar con rigor que la computación cuántica financiera no es una promesa abstracta sino un campo en transición activa, con implicaciones que, en el caso de la criptografía, son ya del todo presentes.
A continuación, se presenta una tabla a modo de síntesis de la investigación realizada. En ella se recoge, para cada una de las aplicaciones analizadas, la principal mejora cuántica que aporta, su estado actual de desarrollo, la limitación más relevante que frena su materialización y un horizonte temporal estimado para su adopción a mayor escala.

Aplicación	Mejora cuántica principal	Estado actual	Principal limitación	Horizonte estimado
Modelización y simulación (Monte Carlo)	Aceleración cuadrática mediante QAE: $O(\sigma/\varepsilon)$ frente a $O(\sigma^2/\varepsilon^2)$	Demostrado teóricamente, implementaciones experimentales en hardware NISQ con qubits limitados.	Requiere circuitos profundos, sensibles al ruido, aun no es viable a escala real.	Medio plazo (8-10 años)
Optimización de carteras	*Quantum annealing* (D-Wave) y QAOA	Primeras pruebas con datos reales (BBVS/Multiverse,	Ventaja cuántica no concluyente,	Corto medio

	para problemas *NP-hard* con variables binarias	S&P 500), resultados dentro del 3% del optimo clásico	*solvers* híbridos dependen aun de componentes clásicos.	plazo (5-7 años)
Quantum Machine Learning (credit scoring)	Clasificación y estimación de similitudes exponencialmente más eficiente sobre datos de alta dimensión	Resultados experimentales prometedores (procesadores de hasta 60 qubits), rendimiento competitivo con modelos clásicos en entornos controlados	Carga y codificación de datos clásicos en qubits (problema de cuello de botella de entrada) aun sin solución escalable	Medio plazo (8-12 años)
Criptografía y seguridad (amenaza cuántica)	Algoritmo de Shor habilita ruptura de RSA, algoritmo de Grover debilita AES	Amenaza activa (*harvest now, decrypt later*); NIST publica primeros estándares post cuánticos (2024), sector financiero en transición	No es una limitación técnica, es un riesgo directamente relacionado a la irrupción del *QDay*. Adopción migración a PQC lenta y costosa	Urgente, riesgo presente

Fuentes: *McKinsey Quantum Technology Monitor (2025); MIT Quantum Index Report (2025); Montanaro (2015); Phillipson & Bhatia (2020); Mugel et al. (2022); Mosca & Piani (2024); NIST (2024); Orús et al (2019); Zhou (2025). Los horizontes temporales son estimaciones orientativas basadas en la literatura académica y no deben interpretarse como predicciones definitivas.*

Como muestra la tabla, no todas las aplicaciones analizadas se encuentran en el mismo estado de desarrollo ni tienen el mismo tipo de implicación para el sector. La criptografía es un caso singular: no es una oportunidad futura sino una amenaza activa que exige una respuesta acelerada por parte de instituciones financieras y actores privados. Como hemos visto, la estrategia conocida como *harvest now, decrypt later* implica que datos considerados seguros hoy podrían quedar expuestos en el futuro, lo que convierte el cambio progresivo hacia estándares post-cuánticos en una prioridad que no puede subordinarse al ritmo general de maduración de la tecnología. El resto de aplicaciones, en cambio, siguen la lógica del horizonte temporal progresivo del desarrollo de la tecnología cuántica. La optimización de carteras es la más próxima a la aplicación real, respaldada ya por pruebas con datos reales como el caso de BBVA y Multiverse Computing, mientras que el quantum machine learning se perfila como la aplicación más lejana, condicionada aún por el problema no resuelto de la carga y codificación eficiente de datos clásicos en sistemas cuánticos.

No obstante, los obstáculos descritos a lo largo del trabajo, como la decoherencia y la corrección de errores, constituyen limitaciones reales, pero no permanentes. El procesador Willow de Google, el Premio Nobel de Física de 2025 y el *roadmap* de IBM hacia la computación tolerante a fallos son prueba de que el ritmo de progreso es sostenido y que la frontera entre potencial teórico y la aplicación práctica se está desplazando de forma continua. El problema de la escalabilidad física, sin embargo, se presenta como el reto de ingeniería más complejo a corto plazo: diseñar infraestructuras capaces de operar miles de qubits de forma viable, estable y energéticamente sostenible es un desafío que va más allá de los algoritmos y que requerirá soluciones de hardware aún no disponibles a escala.

Esto nos enseña que tanto las instituciones financieras como los actores privados han de ir preparándose ahora para no solo anticiparse al desarrollo cuántico como puede ser el caso de la amenaza criptográfica, sino para ser pioneros en los avances cuánticos, que pueden ser fuente de miles de millones de euros en ingresos. Los ejemplos recogidos en este trabajo apuntan en esa dirección: iniciativas como la National Quantum Initiative en Estados Unidos o la Estrategia Nacional de Tecnologías Cuánticas en España reflejan el compromiso institucional con este campo, mientras que colaboraciones como la de JPMorgan Chase e IBM en ciberseguridad cuántica, o la de BBVA con Multiverse

Computing en optimización de carteras, muestran que los actores privados más relevantes ya están operando en este terreno. La ventana para anticiparse existe, pero se está cerrando.

En definitiva, los avances en computación cuántica son cada vez más frecuentes y significativos, y las principales empresas tecnológicas del mundo se encuentran inmersas en lo que bien podría describirse como una carrera hacia la supremacía cuántica. Gobiernos, instituciones financieras y empresas les siguen de cerca, conscientes de que el impacto de esta tecnología sobre el sistema financiero global no es ya una cuestión de posibilidad sino de tiempo. Como hemos visto a lo largo de este trabajo, la irrupción de la computación cuántica en el tejido financiero no gira en torno al sí ocurrirá, sino al cuándo, y en qué medida estaremos preparados para cuando llegue. Quizás, parafraseando a Huxley, los modelos financieros que hoy conocemos terminen convertidos en las serpientes estranguladas junto a la cuna de esta nueva ciencia, aunque en el horizonte más inmediato, no obstante, la tecnología cuántica se plantea de forma híbrida a la clásica, con sistemas que combinen lo mejor de ambos paradigmas.

Declaración de Uso de Herramientas de Inteligencia Artificial Generativa en Trabajos Fin de Grado

ADVERTENCIA: Desde la Universidad consideramos que ChatGPT u otras herramientas similares son herramientas muy útiles en la vida académica, aunque su uso queda siempre bajo la responsabilidad del alumno, puesto que las respuestas que proporciona pueden no ser veraces. En este sentido, NO está permitido su uso en la elaboración del Trabajo fin de Grado para generar código porque estas herramientas no son fiables en esa tarea. Aunque el código funcione, no hay garantías de que metodológicamente sea correcto, y es altamente probable que no lo sea.

Por la presente, yo, Begoña Astarloa Domínguez, estudiante de Derecho y Administración y Dirección de Empresas de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado "Computación Cuántica y su potencial en el ámbito financiero" declaro que he utilizado la herramienta de Inteligencia Artificial Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las actividades descritas a continuación [el alumno debe mantener solo aquellas en las que se ha usado ChatGPT o similares y borrar el resto. Si no se ha usado ninguna, borrar todas y escribir "no he usado ninguna":

1. **Brainstorming de ideas de investigación:** Utilizado para idear y esbozar posibles áreas de investigación.
2. **Constructor de plantillas:** Para diseñar formatos específicos para secciones del trabajo.
3. **Corrector de estilo literario y de lenguaje:** Para mejorar la calidad lingüística y estilística del texto.
4. **Generador previo de diagramas de flujo y contenido:** Para esbozar diagramas iniciales.
5. **Sintetizador y divulgador de libros complicados:** Para resumir y comprender literatura compleja.
6. **Revisor:** Para recibir sugerencias sobre cómo mejorar y perfeccionar el trabajo con diferentes niveles de exigencia.
7. **Traductor:** Para traducir textos de un lenguaje a otro.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para que se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: 24 de marzo de 2026

Firma: Begoña Astarloa Domínguez

BIBLIOGRAFÍA:

Alonso-Robisco, A., & Carbó, J. M. (2022). Inteligencia artificial y finanzas: una alianza estratégica. Documentos Ocasionales/Banco de España, 2222.

Arute, Frank, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, ... John M Martinis. (2019). "Quantum supremacy using a programmable superconducting processor". *Nature volumen,* 574, pp. 505-510. https://doi.org/10.1038/s41586-019-1666-5

Barcelona Supercomputing Center. (2023, diciembre 5). El BSC presenta el primer ordenador cuántico de España desarrollado con tecnología 100% europea. *Barcelona Supercomputing Center.* https://www.bsc.es/es/noticias/noticias-del-bsc/el-bsc-presenta-el-primer-ordenador-cu%C3%A1ntico-de-espa%C3%B1a-desarrollado-con-tecnolog%C3%ADa-100-europea

BBVA. (2021, octubre 4). Así es el mapa mundial de la computación cuántica. *BBVA*.

BBVA. (2022, enero 18). BBVA y Multiverse demuestran cómo la computación cuántica puede optimizar la gestión de las carteras de inversión. *BBVA.* https://www.bbva.com/es/bbva-y-multiverse-demuestran-como-la-computacion-cuantica-puede-optimizar-la-gestion-de-las-carteras-de-inversion/

Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, *22*(5), 563–591.

Black, F., & Scholes, M. (1973). The pricing of options and corporate liabilities. *Journal of Political Economy, 81*(3), 637–654

Biondi, Matteo, Anna Heid, Nicolaus Henke, Niko Mohr, Ivan Ostojic, Lorenzo Pautasso, Linde Wester y Rodney Zemmel. (2021). Quantum computing: An emerging

ecosystem and industry use cases. *McKinsey & Company.*https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use- cases-are-getting-real-what-you-need-to-know

Bohr, N. (1913) 'I. On the constitution of atoms and molecules', Philosophical Magazine Series 6, 26: 151,1 — 25

Bonillo, V. M. (2013). Principios fundamentales de computación cuántica. *Universidad de la Coruna*.

Bouland, A., van Dam, W., Joorati, H., Kerenidis, I., & Prakash, A. (2020). Prospects and challenges of quantum finance. *arXiv preprint arXiv:2011.06492*.

Cabral Rochin, F. (2025). Tecnología y sociedad: Cómo la inteligencia artificial y la computación cuántica redefinen la economía y la educación. *Revista Multidisciplinar Epistemología de las Ciencias, 2*(3), julio–septiembre

Chakrabarti, S., Krishnakumar, R., Mazzola, G., Stamatopoulos, N., Woerner, S., & Zeng, W. J. (2021). A threshold for quantum advantage in derivative pricing. *Quantum*, *5*, 463.

Chohan, A. (2024). A comparative review of quantum bits: Superconducting, topological, spin, and emerging qubit technologies.

Contín Aylón, G. C. (2012). La paradoja del gato de Schrödinger y los problemas de la interpretación de la mecánica cuántica. *Universidad Nacional de Educación a Distancia*.

Crosson, E., & Lidar, D. (2021). Prospects for quantum enhancement with diabatic quantum annealing. *Nature Reviews Physics*, *3*, 466–489. https://doi.org/10.1038/s42254-021-00313-6

Dalwadi, P. (2025). The Future of Financial Data Security: Challenges and Opportunities of Quantum Computing. *International Journal of Management, Economics and Commerce*, *2*(1), 54-60.

Doosti, M., Wallden, P., Hamill, C. B., Hankache, R., Thomson Brown, O., & Heunen, C. (2024). *A brief review of quantum machine learning for financial services*. arXiv. https://arxiv.org/abs/2407.12618

D-Wave Systems. (s. f.). *Introduction to quantum annealing*. Recuperado el 10 de febrero de 2026, de https://docs.dwavequantum.com/en/latest/quantum_research/quantum_annealing_intro.html

D-Wave Quantum Inc. (s.f.). *Get started with quantum computing*. D-Wave Documentation. https://docs.dwavequantum.com/en/latest/quantum_research/index_get_started.html

Egger, Daniel J., Ricardo García Gutiérrez, Jordi Cahué Mestre y Stefan Woerner. (2021). "Credit risk analysis using quantum computers". *IEEE Transactions on Computers,* vol. 70, no. 12. https://doi.org/10.1109/ TC.2020.3038063

Einstein, A. (1905). Heurística de la generación y conversión de la luz. Ann. Phys, 17(1), 549-560.

Einstein, A. (1926). Carta a Max Born [4 de diciembre de 1926]. En M. Born (Ed.), *The Born-Einstein Letters* (p. 91). Macmillan. (Publicado en 1971).

Faruk, S. O., & Barrett, J. (2023). Quantum computing in machine learning: A hybrid quantum-classical approach.

Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6/7), 467–488.

Friebe, C., Kuhlmann, M., Lyre, H., Näger, P. M., & Passon, O. (2018). *The philosophy of quantum physics*. Springer.

Friis, N., et al. (2019). Entanglement certification from theory to experiment. *Nature Reviews Physics*, *1*, 72–87. https://doi.org/10.1038/s42254-018-0003-5

Gálvez, P., Salgado, M., & Gutiérrez, M. (2010). Optimización de carteras de inversión: Modelo de Markowitz y estimación de volatilidad con GARCH. *Horizontes Empresariales.*

Gáfaro, R. E. M., Espinel, E. A. A., & Conde, H. A. P. (2025). Estado del arte de la computación cuántica sus desafíos y aplicaciones. *Revista Colombiana de Tecnologías de Avanzada*, *2*(46), 89-101

Gobierno de España. (s. f.). *¿Qué es la Estrategia Nacional de Tecnologías Cuánticas?* Recuperado el 10 de febrero de 2026, de https://planderecuperacion.gob.es/noticias/que-es-estrategia-nacional-tecnologias-cuanticas-prtr

Griffiths, D. J. (2018). *Introduction to quantum mechanics* (4th ed.). Cambridge University Press

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, 212–219.

Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett*. **79**, 325

Heisenberg, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. Zeitschrift für Physik, 43, 172–198.

Herman, D., Googin, C., Liu, X., Sun, Y., Galda, A., Safro, I., ... & Alexeev, Y. (2023). Quantum computing for finance. *Nature Reviews Physics*, *5*(8), 450-465.

Hughes, C., Isaacson, J., Perry, A., Sun, R. F., & Turner, J. (2021). Quantum computing for the quantum curious.

Hughes, C., et al. (2021). Introduction to superposition. En *Quantum Computing for the Quantum Curious*. Springer. https://doi.org/10.1007/978-3-030-61601-4

IBM. (s.f.). *Cryptography*. IBM Think. https://www.ibm.com/es-es/think/topics/cryptography

IBM. (s.f.). *Quantum cryptography*. IBM Think. https://www.ibm.com/think/topics/quantum-cryptography

IBM. (2025). *IBM quantum roadmap*. IBM.

Kerenidis, I., Prakash, A., & Szilágyi, D. (2019). *Quantum algorithms for portfolio optimization*. En: Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT '19) (pp. 147–155). Association for Computing Machinery. https://doi.org/10.1145/3318041.3355465

Kok, P. (2018). *A first introduction to quantum physics*. Springer.

Leclerc, L., Ortiz-Guitiérrez, L., Grijalva, S., Albrecht, B., Cline, J. R. K., Elfving, V. E., Signoles, A., Henriet, L., del Bimbo, G., Sheikh, U. A., Shah, M., Andrea, L., Ishtiaq, F., Duarte, A., Mugel, S., Cáceres, I., Kurek, M., Orús, R., Seddik, A., … M'tamon, D. (2022). *Financial risk management on a neutral atom quantum processor*. arXiv. https://doi.org/10.48550/arXiv.2212.03223

López Chamorro, N. (2024). *El camino hacia la supremacía cuántica: oportunidades y desafíos en el ámbito financiero, la nueva generación de criptografía resiliente*. Documentos Ocasionales/Banco de España, 2421.

McCarthy, J. (2007). What is artificial intelligence? Stanford University.

Markowitz, H. (1952). Portfolio selection. *The Journal of Finance, 7*(1), 77–91.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications, 9*(3), 405–414.

McKinsey & Company. (2021). *Quantum computing: An emerging ecosystem and industry use cases*. McKinsey & Company.

McKinsey & Company. (2025). *Quantum Technology Monitor*. McKinsey Digital.

Mironowicz, P., Ostaszewski, M., Bieliński, P., Chruściński, T. P., & Puchała, Z. (2024). *Applications of quantum machine learning for quantitative finance*.

Montanaro, A. (2015). Quantum speedup of Monte Carlo methods. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *471*(2181), 20150301.

Mosca, M., & Piani, M. (2024). *Global Risk Institute: Quantum Threat Timeline Report 2022*.

Mugel, S., Kuchkovsky, C., Sánchez, E., Fernández-Lorenzo, S., Luis-Hita, J., Lizaso, E., & Orús, R. (2022). Dynamic portfolio optimization with real datasets using quantum processors and quantum-inspired tensor networks. *Physical Review Research, 4*(1), 013006. https://doi.org/10.1103/PhysRevResearch.4.013006

Numata, K. (2024, abril 19). *Quantum bits, gates, and circuits* [Lecture slides]. IBM Research – Tokyo.

Nuribal. (2020). *Computación Clásica vs Computación Cuántica*. Nuribal. https://nubiral.com/computacion-clasica-vs-computacion-cuantica/

Orús, Román, Samuel Mugel y Enrique Lizaso. (2019a). "Quantum computing for finance: Overview and prospects". *Reviews in Physics,* 4, p. 100028. https://doi.org/10.1016/j.revip.2019.100028

Oxionics. (2023). *Solving quantum computing's wiring dilemma: How to build a 1000-qubit computer without tens of thousands of wires*. https://www.oxionics.com/announcements/solving-quantum-computings-wiring-dilemma-how-to-build-a-1000-qubit-computer-without-tens-of-thousands-of-wires/

Phillipson, F., & Bhatia, H. S. (2020). *Portfolio optimisation using the D-Wave quantum annealer*. arXiv. https://arxiv.org/abs/2012.01121

Planck, M. (1901). On the law of distribution of energy in the normal spectrum. Annalen der physik, 4(553), 1.

Preskill, J. (2012). *Quantum computing and the entanglement frontier*. arXiv preprint arXiv:1203.5813.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79.

Qblox. (2025). *The quantum leap that needs error correction*. https://qblox.com/newsroom/the-quantum-leap-that-needs-error-correction

Qilimanjaro Quantum Tech. (2025). *Quantum computing: Pioneering a sustainable path for future computing*. https://qilimanjaro.tech/quantum-computing-pioneering-a-sustainable-path-for-future-computing/

Rebentrost, P., Gupt, B., & Bromley, T. R. (2018). Quantum computational finance: Monte Carlo pricing of financial derivatives. *Physical Review A*, *98*(2), 022321.

Redacción APD. (2025, marzo 26). *Empresas tecnológicas líderes en computación cuántica: Ejemplos y estrategias*. APD.

Rieffel, E., & Polak, W. (2000). *An introduction to quantum computing for non-physicists*. *ACM Computing Surveys, 32*(3), 300–335. https://doi.org/10.1145/367701.367709

Riverlane. (2025). *Why do quantum computers need QEC?* Recuperado el 6 de marzo de 2026. https://www.riverlane.com/blog/why-do-quantum-computers-need-qec

Rosenberg, G., Haghnegahdar, P., Goddard, P., Carr, P., Wu, K., & López de Prado, M. (2015). Solving the optimal trading trajectory problem using a quantum annealer. *Proceedings of the 8th Workshop on High Performance Computational Finance (WHPCF 2015)*. https://doi.org/10.1145/2830556.2830563

Ruane, J., Kiesow, E., Galatsanos, J., Dukatz, C., Blomquist, E., & Shukla, P. (2025, mayo). *The Quantum Index Report 2025*. MIT Initiative on the Digital Economy, Massachusetts Institute of Technology.

Schrödinger, E. (1926). Quantisierung als Eigenwertproblem [La cuantización como problema de autovalores]. *Annalen der Physik*, *384*(4), 361–376.

Schrödinger, E. (1935). *Die gegenwärtige Situation in der Quantenmechanik* [The present situation in quantum mechanics]. *Naturwissenschaften, 23*, 807–812, 823–828, 844–849.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, *26*(5), 1484–1509.

SSH Communications Security. (s.f.). *How quantum computing threats impact cryptography and cybersecurity*. SSH Academy. https://www.ssh.com/academy/how-quantum-computing-threats-impact-cryptography-and-cybersecurity

SpinQ Technology. (2025-a). *Ultimate guide to qubit in quantum computing*. Recuperado el 9 de febrero de 2026, de https://www.spinquanta.com/news-detail/ultimate-guide-to-qubit-in-quantum-computing

SpinQ Technology. (2025-b). *What is a qubit?* Recuperado el 10 de febrero de 2026, de https://www.spinquanta.com/news-detail/what-is-a-qubit

SpinQ Technology. (2025-c). *Why coherence matters in quantum research: The 2025 Nobel Prize context*. Recuperado el 6 de marzo. https://www.spinquanta.com/news-detail/why-coherence-matters-in-quantum-research-the-2025-nobel-prize-context

SpinQ Technology. (2025-d). *Understanding quantum decoherence: The ultimate expert guide*. Recuperado el 6 de marzo de 2026. https://www.spinquanta.com/news-detail/understanding-quantum-decoherence-the-ultimate-expert-guide

SpinQ Technology. (2025-e). *Quantum entanglement examples explained*. https://www.spinquanta.com/news-detail/quantum-entanglement-examples-explained

Spin Q Technology. (2025-f). 9 *Types of quibits driving quantum computing forward.* https://www.spinquanta.com/news-detail/main-types-of-qubits

Tencent Cloud. (2024). *What is quantum computing?* Tencent Cloud Techpedia. Recuperado el 6 de marzo de 2026. https://www.tencentcloud.com/techpedia/131515

The Royal Swedish Academy of Sciences. (2025). *Scientific background to the Nobel Prize in Physics 2025: For the discovery of macroscopic quantum mechanical tunnelling and energy quantisation in an electric circuit*. Nobel Committee for Physics

The Quantum Insider. (2025, July 22). *JPMorgan Chase taps former State Street executive to lead quantum advanced tech research team*. https://thequantuminsider.com/2025/07/22/jpmorgan-chase-taps-former-state-street-executive-to-lead-quantum-advanced-tech-research-team/

Trond, I., Ansmann, M., Arute, F., Arya, K., Asfaw, A., Astrakhantsev, N., ... & Lacroix, N. (2025). Quantum error correction below the surface code threshold. *Nature*, *638*, 27.

Vargas-Torres-Céliz, E., Lara-Baltazar, G., Mollinedo-Chávez, L., & Ricaldi-Arauzo, R. (2022). Computación Tradicional, Quantum y sus futuras aplicaciones. *Revista Científica de Sistemas e Informática*, *2*(1), e201-e201.

WiFiTalents. (2026). *Quantum industry statistics*. https://wifitalents.com/quantum-industry-statistics/

Williams, C. P. (2011). Quantum gates. In *Explorations in quantum computing* (pp. 51-122). London: Springer London.

Xi, Z., Li, Y., & Fan, H. (2015). Quantum coherence and correlations in quantum system. *Scientific Reports*, *5*, 10922. https://doi.org/10.1038/srep10922

Zanjirdar, M. (2020). Overview of portfolio optimization models. *Advances in Mathematical Finance & Applications, 5*(4), 419–435. https://doi.org/10.22034/amfa.2020.674941

Zhou, J. (2025). Quantum finance: Exploring the implications of quantum computing on financial models. *Computational Economics*, 1-30.

ANEXOS:

Anexo 1: Tipos de qubits

El presente anexo se ha elaborado principalmente a partir de las aportaciones de Chohan (2024) y de SpinQ (2025-f), salvo indicación en contrario.

1. Qubits Superconductores

Operan a temperaturas extremadamente bajas donde la resistencia eléctrica desaparece. Utilizan uniones Josephson para crear estados de energía distintos que representan la información cuántica. Son actualmente la tecnología más desarrollada, aunque enfrentan retos en tiempos de coherencia cortos y errores de puerta.

IBM, Google, SpinQ y Rigetti son lideres en este campo. Se utilizan para tratar de alcanzar la supremacía cuántica, como Google con el chip Willow de 105 qubits, además tienen aplicaciones comerciales y de desarrollo de procesadores a gran escala como el IBM Condor.

2. Qubits de Iones Atrapados (Trapped Ion)

Utilizan iones (átomos cargados) confinados en campos electromagnéticos. Destacan por tener las precisiones más altas, errores bajos y tiempos de coherencia más largos. El principal desafío es la complejidad física para escalar el sistema.

IonQ, Honeywell y Quantinuum son lideres, se enfocan en construir sistemas altamente precisos y totalmente conectados para ejecutar circuitos cuánticos complejos. Manipulan los estados internos de los iones mediante pulsos laser.

3. Qubits fotónicos

Utilizan fotones (partículas de luz) para codificar información en propiedades como la polarización o la fase. Son inmunes a muchos tipos de ruido y pueden operar a temperatura ambiente, lo que los hace ideales para redes de comunicación cuántica.
Xanadu y PsiQuantum son lideres en su uso en campos como la comunicación cuántica, la criptografía y la computación cuántica tolerante a fallos.

4. Qubits topológicos

Codifican su información en el trenzado de cuasipartículas llamadas anyones, iones con carga eléctrica negativa. Su mayor ventaja es la robustez intrínseca contra ruido local y la decoherencia, siendo teóricamente estables por naturaleza. Aún se encuentran principalmente en fase de investigación experimental.
Microsoft trabaja con ellos en el desarrollo de ordenadores cuánticos escalables e inherentemente tolerantes a fallos. En 2025 presentaron Majorana 1, un procesador que utiliza materiales “topoconductores”.

5. Qubits de Spin (Spin Qubits)

Aprovechan el espín de electrones o núcleos en materiales semiconductores. Son atractivos porque pueden integrarse con la infraestructura de fabricación de chips de silicio ya existentes.
Los principales desarrolladores son Intel y QuTech, además, de la UNSW en Sídney y Princeton University.

6. Centros de Vacante de Nitrógeno en Diamante (NV Centers)

Se trata de defectos en cristales de diamante donde un átomo de nitrógeno reemplaza uno de carbono. Pueden operar a temperatura ambiente y son muy estables.
Empleados por empresas como Element Six, Quantum Diamond Technologies y universidades como Harvard. Ideales para sensores cuánticos (detección de campos magnéticos) y redes de comunicación segura. La información se almacena en el espín del electrón y se manipula mediante campos de microondas y transiciones ópticas.

7. Tipos emergentes

Además, existen otros tipos de qubits como los de átomos neutros, puntos cuánticos o de resonancia magnética nuclear, más emergentes pero que también muestran resultados prometedores.

Anexo 2: Tipos de puertas cuánticas

El presente anexo se ha elaborado principalmente a partir de las aportaciones de Williams (2011), SpinQ (2025-g) y de Numata, K (2024), salvo indicación en contrario.

1. Puertas de un solo qubit

Actúan sobre un qubit individual para cambiar su probabilidad o fase:

- Puerta Hadamard (H): es fundamental porque crea superposición, permitiendo que un qubit este en los estados |0⟩ y |1⟩ simultáneamente con igual probabilidad.
- Puerta X (Pauli-X): es la versión cuántica de la puerta NOT clásica, invierte el estado del qubit (de |0⟩ a |1⟩ y viceversa).
- Puerta Z (Pauli-Z): aplica un volteo de fase cambiando el signo de amplitud del estado |1⟩ sin alterar el estado |0⟩.
- Puertas de rotación (Rx, Ry, Rz): permiten rotal el estado del qubit alrededor de los ejes X, Y o Z de la esfera de Bloch por un ángulo especifico, ofreciendo control de precisión.

2. Puertas de múltiples qubits

Son esenciales para procesar información de manera paralela y crear estados complejos:

- CNOT (NOT controlada): utiliza un qubit de control y uno de objetivo. Si el de control está en el estado |1⟩, invierte el objetivo. Es la herramienta principal para generar entrelazamiento.
- Puerta SWAP: intercambia los estados entre dos qubits
- Puerta Toffoli (CCNOT): Una puerta de tres qubits que invierte el tercero solo si los dos primeros son |1⟩. Es crucial para la lógica reversible y la corrección de errores.

IBM Technology Atlas

Quantum roadmap

The future of computing is quantum.

Updated April 2025

✅ Realized
🔄 In progress

	2024	2025	2026	2027	2029	2033+
Quantum journey	✅ ***Expand the utility of quantum computing.***	🔄 ***Extend algorithms on quantum computing + HPC and demonstrate error correction code.***	***Demonstrate first example of scientific quantum advantage and a fault-tolerant module.***	***Diversify quantum advantage and entangle fault-tolerant modules.***	***Deliver the first fault-tolerant quantum computer.***	***Unlock the full power of quantum computing at scale.***
Strategy overview	✅ Demonstrate accurate execution of a quantum circuit at a scale beyond exact classical simulation. (5K gates on 156 qubits)	We will release Quantum + HPC tools that will leverage Nighthawk, a new higher-connectivity quantum processor able to execute more complex circuits.	We will demonstrate the first examples of quantum advantage using a quantum computer with HPC.	The scale, quality, speed of the quantum computer will improve to allow executing quantum circuits at a scale of 10K gates on a 1000+ qubits.	The first fault-tolerant quantum computer will be available to clients and allow execution of 100M gates on 200 qubits.	Scale fault-tolerant quantum computers to run circuits of 1 billion gates on up to 2000 qubits, unlocking the full power of quantum computing.
Why this matters to our clients and the world	✅ We have created a platform where algorithm and application developers can develop candidate circuits at utility scale.	We will provide tools and methods for exploring quantum advantage on a pre-fault-tolerant quantum computer working alongside HPC.	Users and partners will unlock the first example of scientific advantage on a pre-fault-tolerant quantum computer working alongside HPC.	Users will be able to run an expanded set of examples demonstrating the scientific value of pre-fault-tolerant quantum computing.	Users will be able to run the next scale of applications using the first fault-tolerant quantum computer unlocking a wider, more complex set of use cases.	Quantum computers running algorithms using billions of gates are expected to enable general applications in security, chemistry, machine learning, and optimization.
The technology or innovations that will make this possible	✅ Developed and deployed Qiskit Functions with our partners to deliver domain specific applications at utility scale. ✅ Used AI to develop advanced classical transpilation methods. ✅ Demonstrated with partners a prototype quantum-centric supercomputer operating at utility scale.	Nighthawk, a modular processor with 120 square lattice qubits will allow more complex calculations using the same circuit depth. New and improved mitigation tools will leverage classical HPC to expand the set of circuits that can be accurately run with 5000 two-qubit gates. *To prepare for the future*, we will demonstrate c-couplers and next generation packaging for fault-tolerant quantum computing with the Loon quantum processor.	Our quantum processors will improve in quality to allow running 7,500 gates on up to 360 qubits. With our partners, we will define a use case benchmarking toolkit to evaluate candidates for quantum advantage. We will deliver mapping and profiling tools for quantum + HPC workflows. *To prepare for the future*, Kookaburra will demonstrate a single module out of Starling consisting of a logical processing unit and quantum memory.	The performance of our Nighthawk processor will improve to allow circuits with up to 10,000 gates on up to 1080 qubits. The first set of computation libraries will be developed to simplify and optimize quantum + HPC workflows. A new workflow accelerator will streamline execution for a known advantage-scale workflow. *To prepare for the future*, the Cockatoo processor will demonstrate entanglement of two modules using a universal adapter.	The first fault-tolerant quantum computer will power a quantum-enhanced HPC architecture with a complete fault-tolerant quantum ISA. With a fault-tolerant architecture, the size of the circuits will increase to 100M operations, enabling the development of more sophisticated circuit libraries. *To prepare for the future*, we will continue to scale electronics, infrastructure, and software to reduce footprint, cost, and energy usage in preparation for Blue Jay.	Scaling fault-tolerant quantum computing to 1 billion gates on up to 2000 qubits with a power consumption of 2 megawatts will require a new control elections and cryogenics infrastructure. Extensions of the computation and circuit libraries will scale and diversify quantum + HPC workflows across industries. *For the future*, we will scale beyond Blue Jay with the development of distributed quantum computing, bringing together the fields of quantum communication and quantum computation.
How these advancements will be delivered to IBM clients and partners	✅ The Heron processor capable of running 5,000 gates on 133 qubits will be delivered through the IBM Quantum Platform.	The Nighthawk processor with high qubit connectivity, capable of running 5,000 gates on 120 qubits, will be delivered through the IBM Quantum Platform.	The Nighthawk processor with up to three 120-qubit modules (360 qubits) capable of running 7,500 gates will be delivered through the IBM Quantum Platform.	The Nighthawk processor with up to nine 120-qubit modules (1080 qubits) capable of running 10,000 gates will be delivered through the IBM Quantum Platform.	The Starling system will be available to clients. It will be a modular, error-corrected quantum-centric supercomputer with 200 qubits capable of running 100 million gates.	A fault-tolerant quantum computer called Blue Jay, capable of running 1 billion gates on up to 2,000 qubits will become available.