EL CAMINO HACIA LA SUPREMACÍA CUÁNTICA: OPORTUNIDADES Y DESAFÍOS EN EL ÁMBITO FINANCIERO, LA NUEVA GENERACIÓN DE CRIPTOGRAFÍA RESILIENTE

2024

BANCO DE ESPAÑA
Eurosistema

Documentos Ocasionales
N.º 2421

Noemí López Chamorro

EL CAMINO HACIA LA SUPREMACÍA CUÁNTICA: OPORTUNIDADES Y DESAFÍOS EN EL ÁMBITO FINANCIERO, LA NUEVA GENERACIÓN DE CRIPTOGRAFÍA RESILIENTE

EL CAMINO HACIA LA SUPREMACÍA CUÁNTICA: OPORTUNIDADES Y DESAFÍOS EN EL ÁMBITO FINANCIERO, LA NUEVA GENERACIÓN DE CRIPTOGRAFÍA RESILIENTE (*)

Noemí López Chamorro

BANCO DE ESPAÑA

(*) Este documento fue elaborado durante la estancia de la autora como Economista en la División de Innovación Financiera del Banco de España, y agradece los valiosos comentarios de Juan Ayuso, José Manuel Marqués, Sergio Gorjón, Iván Balsategui y Ana Fernández.

Documentos Ocasionales. N.º 2421

Junio 2024

https://doi.org/10.53479/36696

ISSN: 1696-2230 (edición electrónica)

Resumen

Este documento ofrece una explicación sencilla sobre aspectos clave de la computación cuántica que resultan esenciales para entender sus ventajas, su grado de avance y sus limitaciones, así como la aplicación en diferentes sectores, dedicando especial atención a la industria financiera y a los riesgos para la criptografía actual. En una segunda parte, de carácter más técnico, se pueden encontrar ampliaciones de muchos de estos temas, siempre sin olvidar la finalidad divulgativa del artículo en su conjunto.

Si bien la computación cuántica promete ser revolucionaría en aplicaciones de muchos segmentos de la economía, aún se encuentra en un estado primigenio, lejano a su implementación, dependiente de la evolución en el *hardware* que permita incorporar plenamente los algoritmos cuánticos puros que posibilitarían una transformación sin precedentes en varios campos.

Aunque el sector financiero podría beneficiarse de importantes mejoras en el corto plazo en casos de uso con un alto nivel de dificultad computacional, también se identifica como uno de los más vulnerables por la sensibilidad de su información, si se logra el *hardware* cuántico con la potencia necesaria para romper los actuales sistemas de encriptación de esa información.

A pesar de la incertidumbre sobre su desarrollo, las implicaciones que el uso de la computación cuántica podría tener para el sector financiero exige planificar una potencial transición ordenada hacia una nueva forma de encriptación resiliente que salvaguarde la información. La elevada complejidad de esta acción requiere un trabajo temprano y un elevado nivel de coordinación internacional.

Palabras clave: computación cuántica, criptografía cuántica y postcuántica, finanzas cuánticas, supremacía cuántica.

Códigos JEL: C88, D82, O31, O33.

Abstract

This paper presents a straightforward explanation of quantum computing, including the key aspects to understand its benefits, progress level, limitations and applications across various sectors, particularly finance, along with the potential risks it poses to existing cryptographic procedures. A second, more technical section provides detailed expansions on these topics, always mindful of the overall informative purpose of the paper.

While quantum computing promises revolutionary applications across multiple economic sectors, it remains in its infancy and a long way from full implementation. Its progress will hinge on hardware advancements capable of supporting the full deployment of pure quantum algorithms, which could be the catalyst for unprecedented change in numerous fields.

The financial sector may reap short-term benefits due to significant improvements in computationally demanding use cases. However, the sector has also been marked out as one of the most vulnerable due to the sensitivity of its information, should quantum hardware become powerful enough to compromise current encryption standards.

In light of the uncertainty surrounding quantum computing's development, the potential implications for the financial sector demand strategic planning to prepare for an orderly transition to a new, robust encryption paradigm capable of safeguarding information. Given the complexity of this undertaking, preliminary groundwork and substantial international coordination are a must.

Keywords: quantum computing, quantum and postquantum cryptography, quantum finance, quantum supremacy.

JEL classification: C88, D82, O31, O33.

Índice

1 Introducción

La computación cuántica (Feynman, 1982) es una tecnología emergente que se postula como una de las grandes innovaciones de nuestra época. El procesamiento cuántico de la información proporciona soluciones nuevas, o más eficientes, para problemas de todos los sectores de la economía. En particular, ha logrado captar la atención de la industria financiera y, a pesar de que en esta etapa inicial los casos de uso son en gran medida experimentales e hipotéticos, se están acelerando los avances para propiciar su viabilidad comercial y su utilización en la industria. Si bien el desarrollo del *hardware* es el cuello de botella, cinco fabricantes han anunciado que para el año 2030 tendrían listo un ordenador cuántico universal tolerante a fallos. Este posible escenario ha impulsado que instituciones públicas y privadas comiencen a prepararse para una transición ágil hacia el nuevo paradigma cuántico. Al mismo tiempo, está creciendo la preocupación por la seguridad de la información, dado que se conocen dos algoritmos cuánticos capaces de romper la encriptación actual, una vez que estén disponibles los medios técnicos cuánticos necesarios para su ejecución.

Por otra parte, también existe un elevado grado de incertidumbre y escepticismo por su futuro uso que motiva que en este artículo, tras una breve revisión del interés y de las inversiones recientes en esta tecnología, se expliquen las características de este procedimiento de computación y se revisen las fortalezas de la computación cuántica frente a la clásica, su grado actual de avance, los desafíos a los que se enfrenta, su aplicación en diferentes sectores, con especial consideración en el financiero, y las implicaciones para la criptografía clásica.

2 El creciente interés por la computación cuántica a manos de un futuro incierto

El interés por la computación cuántica ha experimentado un paulatino crecimiento durante las dos últimas décadas. El progreso actual en la ciencia y en la tecnología demuestra un avance sin precedentes en la manipulación de partículas subatómicas, un elemento fundamental para lograr el desarrollo de ordenadores cuánticos. Aunque aún queda un largo camino por recorrer, muchos científicos anticipan que estamos en las primeras etapas de lo que se conoce como la segunda revolución cuántica.

A día de hoy, la Unión Europea y otras 13 agencias gubernamentales de todo el mundo han anunciado iniciativas de investigación a largo plazo, comprometiéndose a dedicar miles de millones de dólares a la investigación en el ámbito cuántico.

Por su parte, numerosas organizaciones de todo el mundo han tomado conciencia de que la computación cuántica puede desempeñar un papel altamente disruptivo y transformador de la realidad. Por primera vez, el Informe de Ciberseguridad y Resiliencia del Sistema Financiero (2023) de la Reserva Federal (FED, por sus siglas en inglés) califica a la computación cuántica como una amenaza para el sistema financiero. No en vano el Memorando NSM-10 (2022) de Seguridad Nacional de los Estados Unidos establece varios plazos para organizar una migración ordenada hacia una criptografía postcuántica robusta. Algunas de las acciones más notorias llevadas a cabo por las instituciones en los últimos años son los Principios de Gobernanza de la Computación Cuántica (2022) del Foro Económico Mundial; la iniciativa de investigación en la Quantum Technologies Flagship (2018) de la Comisión Europea; el Manifiesto Cuántico (2016) de la Unión Europea; el actual proyecto LEAP para explorar la criptografía postcuántica del centro del Eurosistema del BIS Innovation Hub, y la Ley Quantum de preparación para la Ciberseguridad (2022) firmada por Biden.

Se espera un crecimiento sostenido de la inversión en esta tecnología a escala mundial, pública y privada, con un incremento anual compuesto del 11,5 % para el período 2023-2027, alcanzando aproximadamente 16,4 MM de dólares para finales de 2027, según International Data Corporation (IDC) (Needham, 2023). No obstante, las numerosas incógnitas por despejar sobre el progreso de la computación cuántica podrían truncar la evolución de la inversión en esta tecnología. Las principales causas de incertidumbre afectan tanto a aspectos relacionados con el *software* como con el *hardware* necesario para implementar esta técnica.

Por la parte del *software,* se identifica la falta de transparencia sobre el verdadero impacto comercial de las soluciones cuánticas. La información detallada publicada por los desarrolladores de soluciones cuánticas es muy limitada y, en muchas ocasiones, resulta confusa, al no dejar claras las diferencias entre un algoritmo cuántico puro y una solución de inspiración cuántica[1]. Además, de momento, solo se pueden probar las aplicaciones híbridas en pruebas de concepto con muchas limitaciones y con escasa utilidad práctica.

1 Las soluciones de inspiración cuántica o híbridas son soluciones clásicas que han tomado como inspiración ciertos conceptos que provienen de la física cuántica. Hasta el momento no se ha demostrado que ostenten una clara ventaja sobre las soluciones clásicas al uso.

La segunda razón es que construir el primer ordenador cuántico universal supone un enorme reto tecnológico, indispensable para la correcta ejecución de los algoritmos cuánticos puros, que no está exento de detractores que directamente piensan que son imposibles de alcanzar.

El apartado 9.1 del documento técnico amplía la información sobre las principales iniciativas supranacionales y describe el auge de la computación cuántica, apoyándose en las inversiones actuales y en sus proyecciones futuras.

3 Ideas fundamentales de la física cuántica. Diferencias entre computación cuántica y computación clásica[2]

Por exclusión, se puede definir la mecánica cuántica como aquella rama de la física que engloba a todo aquello diferente de la mecánica clásica. Por consiguiente, todas las nociones de la física clásica se invalidan bajo la óptica del «mundo de lo pequeño», de aquellas partículas (atómicas y subatómicas) cuyas reacciones resultan extrañas, contra-intuitivas y, en la mayoría de las ocasiones, complejas de entender.

Para empezar, merece la pena aclarar que la computación cuántica supone un cambio de paradigma y, por tanto, no debe ser entendida como una continuidad de la informática clásica. Por ende, ambos tipos de informática muestran amplias diferencias respecto a la unidad de procesamiento de la información, el tipo de matemática sobre la que se construyen y las leyes físicas que la sustentan. Precisamente estos tres factores son la clave, condicionan tanto los algoritmos como el *hardware* necesario para su ejecución y, como consecuencia final, la tipología de problema que cada sistema de computación es capaz de resolver (véase esquema 1).

De una parte, el mundo digital clásico es binario por definición. Su unidad de información, el bit, está restringida a dos estados excluyentes, cero o uno, encendido o apagado o, si se prefiere, blanco o negro. La matemática que subyace detrás de esta programación es determinista y se basa en los principios de la mecánica clásica.

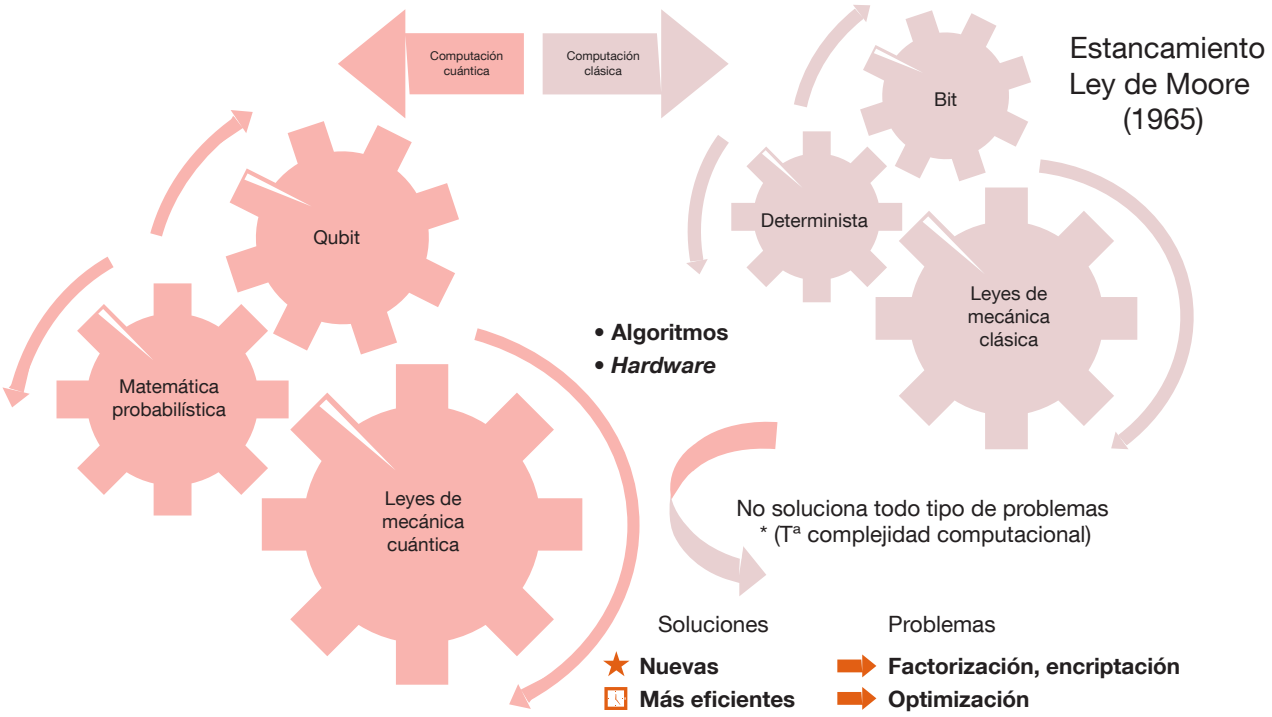
En contraste, el mundo cuántico, basado en la mecánica cuántica y en una matemática probabilística, es «multicolor», puesto que son infinitas y extremadamente sofisticadas las posibles combinaciones lineales de los estados cero y uno que conforman la unidad básica de computación cuántica, el qubit, y que, a consecuencia, expanden significativamente el universo de cálculo. Esta singularidad se sostiene en tres pilares de la mecánica cuántica: la superposición, el entrelazamiento y la interferencia.

La superposición cuántica consiste en la combinación lineal de los estados cero y uno. Esta propiedad permite adoptar, al mismo tiempo, un mayor número de estados posibles y esto incide en un aumento de la capacidad de computación. Explicado intuitivamente, podría ser semejante a hacer girar un elemento que tiene dos estados, como un átomo o, si se prefiere, una moneda. Los dos estados de la moneda son cara y cruz. Al hacerla girar estaría en superposición, no podría determinarse si está en cara o en cruz. Afinando mucho se podría formular una combinación lineal de ambos estados que irá modificándose en función del ángulo que describa su giro. Cuando la moneda pare de girar y caiga, dará lugar a un resultado final que será binario excluyente, es decir, cara o cruz, este resultado final es lo que en computación cuántica se conoce como medición.

2 Los conceptos expuestos a continuación han sido deliberadamente simplificados con fines divulgativos, priorizando ofrecer una visión de conjunto que sea accesible para el público no especializado.

Esquema 1

Diferencias entre la computación clásica y la computación cuántica



FUENTE: Elaboración propia.

El entrelazamiento en la computación cuántica se refiere a la propiedad en la que dos o más partículas cuánticas están interconectadas, de forma que el estado de una partícula instantáneamente afecta al estado de la otra, sin importar la distancia que las separa.

La interferencia en la computación cuántica se refiere a la capacidad de las partículas cuánticas para combinarse de maneras específicas, como ondas, de forma que sus estados se sumen o se cancelen entre sí, lo que es esencial para realizar cálculos y obtener resultados cuánticos útiles.

En la práctica, para que un algoritmo cuántico funcione en un ordenador cuántico requiere de tres pasos básicos. En primer lugar, que los qubits del ordenador estén en superposición, que se entrelacen los qubits para cargar/codificar los datos del problema y, por último, utilizar la interferencia para conseguir aumentar el cálculo, amplificando los posibles resultados donde estará contenida la solución. Entiéndase que, al tratarse de un cálculo probabilístico o matricial, hasta el momento de la medida (es decir, la determinación de un resultado final), se tomarán en consideración multitud de combinaciones que serían obviadas con un cálculo meramente determinista propio de un ordenador clásico. Una vez terminadas las operaciones, se concretará el resultado final, que estará expresado en un código binario de ceros y unos, de forma determinista.

El apartado 9.2 del documento técnico proporciona una idea de conjunto sobre las fortalezas y las diferencias de la computación cuántica respecto a la computación clásica, explicando en subapartados temáticos la superposición, el entrelazamiento y la medida cuántica.

4 Ventajas y usos de la computación cuántica

El ordenador cuántico basa sus cálculos en la combinación de estos tres conceptos (superposición, entrelazamiento e interferencia), con los que puede realizar tanto operaciones propias de la mecánica clásica como resolver problemas exponencialmente complejos, utilizando el poder de la mecánica cuántica y de la matemática probabilística.

Simplificando mucho conceptualmente la teoría de la complejidad computacional, podría afirmarse que los problemas matemáticos más complicados requieren para su solución de medios informáticos más complejos, como la computación cuántica. No en todos los contextos tiene sentido aplicar computación cuántica; a modo de resumen se pueden identificar dos tipos de entornos en los que su uso es más prometedor:

— En la búsqueda de soluciones computacionales más eficientes, como es el caso de problemas que, pudiendo resolverse con enfoques clásicos mediante fuerza bruta, requieren de una ingente cantidad de tiempo y de recursos, incluso utilizando supercomputadoras. Por ejemplo, la factorización y la encriptación.

— En problemas fuera del alcance de la informática clásica, como determinados problemas de optimización que implican una alta complejidad, así como la optimización dinámica de carteras de inversión de activos sujeta a restricciones.

En resumen, la computación cuántica acelera el proceso de iteración presente en el método científico. De esta forma, propicia la obtención de resultados satisfactorios en un tiempo mucho menor.

5 Primeros pasos hacia un sector financiero cuántico

Se estima que las finanzas sería uno de los primeros sectores industriales en beneficiarse de la computación cuántica a corto plazo, McKinsey & Co. (Biondi *et al.,* 2021). En consonancia, los datos de la encuesta realizada por Hyperion Research (Sorensen, 2021) recogen que el 56 % de las grandes empresas financieras reconoce estar explorando opciones y monitorizando desarrollos cuánticos con el fin de mejorar su eficiencia y su rentabilidad.

En el ámbito de la economía y de las finanzas, la aplicación de la computación cuántica se aplica a tres grandes metodologías: la modelización estocástica, la optimización y el aprendizaje automático (Bouland, Van Dam, Joorati, Kerenidis y Prakash, 2020; Herman *et al.,* 2022).

En concreto, se ha identificado una mayor eficiencia teórica en problemas como la fijación de precios de derivados, la optimización de carteras, los modelos de riesgo, el procesamiento del lenguaje natural (NLP), la detección del fraude en operaciones de tarjetas y transferencias, junto a técnicas de aprendizaje automático y en el campo del cifrado y la ciberseguridad.

Es difícil determinar cuándo la aceleración cuántica será relevante para un dominio en particular. Para ello se requiere una comprensión profunda de los propios algoritmos cuánticos, de los recursos cuánticos necesarios para ejecutar los algoritmos, la medida en que esos recursos se pueden reducir mediante el rediseño de los algoritmos, así como estimar la línea de tiempo del desarrollo del *hardware* cuántico. Según la consultora McKinsey & Co. (Masiowski, Mohr, Soller y Zesco, 2022), esta posibilidad ha propiciado un significativo y rápido aumento de nuevas empresas centradas en el desarrollo de programas cuánticos, de un puñado, en 2013, a más de 200, en 2021.

Hay dos cuestiones relevantes respecto al uso de los algoritmos cuánticos en el campo de las finanzas. La primera consiste en saber si la aplicación de una solución cuántica para un problema de interés proporciona algún tipo de ventaja respecto a la clásica. En este aspecto, los desarrolladores de *software* cuántico se esmeran por identificar posibles casos de uso, y para ello colaboran con la industria, centrándose en aquellos de mayor valor[3]. La segunda pregunta consiste en saber cuándo podría estar disponible la solución cuántica.

Actualmente, se conocen menos de 100 algoritmos cuánticos[4] con una aceleración teórica comprobada frente a la computación convencional. El trabajo inicial se basa en

3 Para ello, la mayoría de los proveedores de servicios de computación cuántica ofrecen acceso gratuito a sus plataformas en la nube, permitiendo a los primeros usuarios experimentar con la tecnología y construir comunidades de desarrolladores. Esto impulsa la identificación del uso de sus aplicaciones a problemas específicos, ayudando a mejorar la investigación y el desarrollo de paquetes cuánticos personalizados.

4 El Quantum Algorithm Zoo exhibe un catálogo completo de los algoritmos cuánticos existentes (Jordan, 2022).

adaptar estos algoritmos[5] a problemas propios del sector financiero para que estén listos para su uso, o que requieran de modificaciones menores, con la llegada del ordenador cuántico universal.

Es primordial enfatizar que la aceleración que pueden proporcionar los algoritmos cuánticos puede diferir significativamente[6], dependiendo tanto del tipo de problema como de algoritmo, según el caso.

El apartado 9.4 del documento técnico detalla las aplicaciones de la computación cuántica en las finanzas.

5 En este momento se están utilizando algoritmos híbridos o de inspiración cuántica porque su profundidad es menor. Los algoritmos de inspiración cuántica son algoritmos clásicos en los que se puede emular de forma clásica el fenómeno cuántico esencial que proporcionaría el aumento de velocidad (https://learn.microsoft.com/es-es/azure/quantum/optimization-overview-introduction). Por su parte, las arquitecturas híbridas más avanzadas aportan una integración más estrecha y enriquecida entre el cálculo clásico y cuántico (https://learn.microsoft.com/es-es/azure/quantum/hybrid-computing-concepts).

6 Para algoritmos con aceleraciones exponenciales, incluso computadoras cuánticas relativamente pequeñas, de alrededor de 100 qubits, podrían teóricamente superar a las supercomputadoras clásicas actuales. Sin embargo, para algoritmos con aceleraciones cuánticas cuadráticas se requerirán procesadores cuánticos significativamente más avanzados y potentes para demostrar ventajas prácticas sobre las computadoras convencionales más poderosas.

6 Causas de las limitaciones de la computación cuántica, los retos y la futura evolución

El avance de la computación cuántica se enfrenta a un cuello de botella, la creación de un ordenador cuántico de propósito universal, un dispositivo con la capacidad para resolver cualquier tipo de operación o de cálculo.

Esta tecnología todavía se encuentra en un incipiente grado de desarrollo, entre un nivel 1 y 2, llamados NISQ[7] (Preskill, 2018), de un total de cuatro, siendo el último de los niveles el que se conoce como supremacía cuántica[8] (Preskill, 2012) (véase esquema 5). A lo largo de la literatura es muy habitual referirse a la ventaja cuántica como una mejora en la escala del tiempo de ejecución de una tarea frente al tiempo consumido por un dispositivo convencional. Sin embargo, Gómez *et al.* (2022) defienden un enfoque más amplio que considere otras variables como el consumo de energía y el coste.

Existen diversos prototipos de ordenadores cuánticos universales, todos ellos inspirados en ejemplos de materiales de la naturaleza que mantienen propiedades cuánticas, como, por ejemplo, los superconductores y los iones atrapados.

Estos sistemas cuánticos se caracterizan por ser tremendamente frágiles, es decir, muy sensibles a la mínima perturbación exterior. Al contrario que en la física clásica, en la práctica, las partículas cuánticas son tan pequeñas y tan livianas que cualquier acción que se ejerce contra ellas, incluso su observación o medición, las altera. Esto motiva la enorme complejidad que entraña la construcción del primer ordenador universal cuántico, ya que las partículas que lo componen pierden con facilidad sus propiedades cuánticas.

Por tanto, los desarrolladores de los dispositivos cuánticos se enfrentan a dos restos: aumentar el tiempo de decoherencia y la corrección de errores.

A efectos prácticos, el tiempo de decoherencia es una medida de la duración de la coherencia[9] de los estados cuánticos de los qubits, antes de que pierdan sus propiedades y se comporten como estados clásicos debido a interacciones con el entorno. En un ordenador cuántico implica que las cualidades de los qubits se degradan y esto dificulta la realización de operaciones cuánticas precisas. La duración del tiempo de decoherencia puede variar según el sistema y las condiciones del entorno.

---

7 NISQ es el acrónimo en inglés de *Noisy-Intermediate-Scale Quantum.* Estrictamente hablando, la categoría de computadoras NISQ incluye dispositivos tanto analógicos como digitales. *De facto,* muchos autores solo incluyen los digitales, puesto que los analógicos son menos adecuados para la corrección de errores (véase recuadro 2).

8 Concepto acuñado por Preskill que hace alusión a la capacidad de un dispositivo cuántico para realizar algún cálculo bien definido que sería prácticamente imposible para las computadoras clásicas, independientemente de la utilidad de dicho cálculo. En este nivel, el ordenador cuántico universal es capaz de simular una operación cuántica y clásica.

9 Mantener la coherencia cuántica significa preservar propiedades cuánticas: la superposición, el entrelazamiento y la interferencia.

La corrección de errores en computadoras cuánticas es un conjunto de técnicas y algoritmos diseñados para mitigar y corregir los errores cuánticos que pueden ocurrir debido a la decoherencia y a otras fuentes de ruido en sistemas cuánticos. Estas técnicas buscan preservar la información cuántica de manera fiable y mejorar la robustez de las operaciones cuánticas, lo que es esencial para el desarrollo y la implementación exitosa de computadoras cuánticas. El objetivo final es conseguir corregir los errores que están presentes en los ordenadores cuánticos, de tal forma que se puedan realizar cálculos largos de manera indefinida y permanente.

Aparte, la información de la que se dispone actualmente impide que la comunidad científica alcance un acuerdo sobre qué tipo de *hardware* cuántico acabará siendo el líder o si podrían convivir más de una tecnología, Global Risk Institute (Mosca y Piani, 2021). Existen iniciativas muy prometedoras, sin diferencias sustancialmente significativas en cuanto a capacidad, que provienen de empresas de diferentes áreas geográficas y que utilizan tecnologías cuánticas como la fotónica, los iones atrapados y los superconductores, entre otras. Por este motivo, también resulta difícil aventurar el impacto medioambiental que podrían tener, si bien suponen un ahorro significativo de tiempo y de medios respecto a los ordenadores clásicos. Habría que determinar el prototipo ganador para poder realizar este análisis y calcular sus necesidades energéticas *versus* las necesidades de una supercomputadora, teniendo en cuenta el caso en cuestión. Con independencia de la tecnología, se cree que el modelo será en remoto a través de la nube. De esta forma, podrá utilizarse el lenguaje de programación favorito con librerías cuánticas que permitirán conectar con un ordenador cuántico que realizará parcial o totalmente los cálculos y devolverá el resultado al usuario. Esto ya ocurre con dispositivos clásicos que realizan computación local asistidos por una supercomputadora en la nube.

En el apartado 9.3 del documento técnico se trata con un alto grado de detalle la capacidad de los dispositivos cuánticos actuales, los algoritmos cuánticos y las previsiones futuras.

7 Encriptación cuántica y postcuántica

En la era de la digitalización, la cantidad de datos que se almacenan o transmiten es ingente. Se manejan desde datos de carácter público hasta datos más críticos con una especial trascendencia; para estos resulta fundamental garantizar la protección y la seguridad con una encriptación robusta. Esta necesidad plantea un riesgo significativo: la confidencialidad de las comunicaciones, que afecta a instituciones públicas y privadas en prácticamente todos los niveles y en diversos sectores de la economía.

La sensibilidad de la industria financiera a esta amenaza es particularmente alta, ya que un ataque exitoso podría comprometer, por ejemplo, la seguridad de los sistemas de pagos y de liquidación, poniendo en riesgo la integridad de las transacciones monetarias y la confidencialidad de la información financiera de los usuarios. La información que se utiliza con fines bancarios es sensible, esto convierte a los organismos financieros en un blanco atractivo para los ciberataques, lo que resalta la necesidad imperante de implementar sólidas medidas de encriptación y de seguridad cibernética.

La criptografía convencional se basa en la factorización de números primos y la seguridad de los códigos depende en gran medida de la longitud de las claves. Hasta el momento, este enfoque solo puede ser vulnerado de manera ineficiente mediante ataques de fuerza bruta utilizando súpercomputadoras clásicas, Kleinjung *et al.* (2010). Además, la fortaleza de la factorización de números primos (RSA, Rivest, Shamir y Adleman, 1978) se basa en una conjetura matemática, es decir, no se ha probado que no se pueda romper, simplemente no se ha hallado la forma de hacerlo, pero podría descubrirse. En este contexto, los algoritmos cuánticos pueden suponer una amenaza para la información actual, ya que podrían tener la capacidad de desencriptar la información de manera exponencialmente más rápida o al menos sustancialmente más efectiva, aunque requieren la presencia de un ordenador cuántico universal para hacerlo.

De una parte, no se puede predecir con certeza cuándo estará disponible un ordenador cuántico capaz de romper, en un tiempo razonable, los sistemas de encriptación convencionales, como RSA-2048. Concretamente, según los resultados obtenidos por Mosca y Piani (2022), el 27,5 % de los profesionales cuánticos encuestados piensan que la probabilidad de que esto suceda en 15 años es alta, es decir, igual o superior al 95 %. Para un horizonte temporal de 30 años, las cifras se duplican, el 55 % de los expertos consideran que sería altamente probable.

Mientras tanto, cada día sin una solución supone un día más de exposición al riesgo. La explicación reside en que hoy en día resulta relativamente económico almacenar millones de datos de información sensible, que seguirá siendo comprometida durante años o décadas, y que dejará de estar protegida en el momento en que el ordenador universal cuántico esté disponible. Así, la información está expuesta al fenómeno SNDL (Store Now Decrypt Later), «Guarda ahora, descifra después», que consiste en almacenar los datos y en un futuro recuperar aquellos que sigan siendo valiosos y descifrar su mensaje, sometiéndolos al procesamiento cuántico (véase esquema 6).

Por estos motivos, organizaciones como el Innovation Hub del Banco de Pagos Internacionales (BIS-IH), el Foro Económico Mundial (WEF), el Instituto Nacional de Estándares y Tecnología (NIST), la Agencia de Seguridad Nacional (NSA) y el Gobierno de los Estados Unidos, han comenzado a tomar medidas proactivas para abordar esta creciente vulnerabilidad.

La necesidad de actuar está respaldada por la teoría, que demuestra que algoritmos de encriptación ampliamente utilizados, como RSA, DH, AES y SHA-3[10], pueden ser descompuestos por la computación cuántica. Esto implica que los sistemas de encriptación actuales deben evolucionar hacia nuevos algoritmos resistentes a los avances de la computación cuántica. Para proteger la información de un futuro ataque hay dos soluciones posibles: la encriptación postcuántica, y la propia encriptación cuántica, que es por definición inquebrantable.

La encriptación postcuántica busca algoritmos que sean inmunes a los ataques de la computación cuántica. Sin embargo, elegir los algoritmos adecuados es un desafío, ya que debe hacerse de manera cuidadosa y con una profunda comprensión de las implicaciones. La elección equivocada podría exponer sistemas críticos a vulnerabilidades, y además, la migración de sistemas de encriptación también es costosa y requiere una coordinación meticulosa para evitar incompatibilidades de código o resquicios sin protección por donde pueda producirse un ataque.

Por otro lado, la encriptación cuántica es, por definición, inquebrantable, debido a las propiedades de la mecánica cuántica. La implementación de esta tecnología en sistemas de seguridad bancaria proporcionaría una defensa sólida contra los ataques de la computación cuántica. Esto significa que los datos estarían protegidos de manera inquebrantable desde el principio, sin necesidad de migraciones costosas.

En la actualidad, varios proyectos internacionales están trabajando en la identificación de algoritmos postcuánticos, aunque esto es un proceso que requiere tiempo y esfuerzo, ya que se trata de anticipar amenazas que aún no han surgido completamente. La ciberseguridad de las instituciones financieras y de otros sectores se basa en gran medida en tomar medidas proactivas para proteger los datos a largo plazo. Esto incluye identificar el grado de vulnerabilidad de los algoritmos de encriptación utilizados, realizar un inventario que los ordene para establecer prioridades y la implementación anticipada de tecnologías cuánticas en sus sistemas de seguridad.

El apartado 9.5 del documento técnico profundiza en el contexto de la encriptación actual y sus riesgos.

10 Shor (1994) puede romper el RSA y el DH, mientras que Grover (1996) junto con la fuerza bruta puede comprometer las claves de AES y SHA-2.

8 Conclusiones finales

El análisis del potencial de la tecnología cuántica revela que destaca para determinados tipos de problemas, como la optimización y la encriptación, pero no resuelve todos los desafíos computacionales. Si bien la industria financiera podría beneficiarse en el corto plazo tanto de una mayor eficiencia computacional como de soluciones a problemas complejos fuera del alcance de la informática clásica, es vital abordar su implementación con cautela y realismo, reconociendo la brecha entre expectativas y limitaciones.

La computación cuántica se presenta como una herramienta extraordinaria con implicaciones muy disruptivas, pero con un alto grado de incertidumbre. Se plantean preguntas cruciales, como la elección de un prototipo de *hardware* triunfador, la efectividad de los algoritmos NISQ y una medida universal de su eficiencia energética frente a los ordenadores convencionales. La falta de consenso en la comunidad científica y empresarial sobre los enfoques que se han de seguir y la ventaja cuántica real plantea desafíos significativos. Se están explorando enfoques híbridos que combinan sistemas cuánticos y clásicos, lo que agrega una capa adicional de incertidumbre. En este contexto, la adaptabilidad continua se convierte en un componente esencial debido a la evolución constante de esta tecnología.

A pesar de los desafíos actuales, se vislumbra un escenario prometedor para el año 2030. Se espera que existan dispositivos cuánticos más potentes y algoritmos de mayor profundidad. Este avance permitirá aplicaciones aún más poderosas y revolucionarias de la computación cuántica. No obstante, alcanzar este potencial requerirá esfuerzos sostenidos de investigación, de inversión y de colaboración entre distintas instituciones y actores del sector.

En el camino hacia este futuro cuántico, la preparación y la colaboración se tornan aún más esenciales. Las instituciones deben anticipar el impacto de los algoritmos cuánticos en la ciberseguridad, fomentar la colaboración en investigación cuántica para un uso responsable y abordar el desafío de desarrollar criptografía postcuántica resistente. Estos factores se presentan como pilares cruciales para garantizar un mundo cuántico seguro y eficiente.

9 Documento técnico

9.1 El auge de la computación cuántica: inversiones, proyecciones futuras y principales iniciativas supranacionales

En los últimos veinte años se ha acrecentado el interés por la computación cuántica, una nueva tecnología que promete importantes innovaciones en prácticamente todas las industrias. Entre el año 2002 y 2021 el total de la inversión privada mundial destinada a su investigación se situó en 3,3 MM de dólares, McKinsey & Co. (Masiowski, Mohr, Soller y Zesco, 2022). En el ámbito concreto de los servicios financieros, una encuesta realizada por Hyperion Research (2021) recoge que el 56 % de las grandes empresas financieras reconoce estar explorando opciones y monitorizando desarrollos cuánticos, con el fin de mejorar su eficiencia y rentabilidad. Se estima que las finanzas serán el primer sector industrial en beneficiarse de la computación cuántica a corto plazo, McKinsey & Co. (Biondi, 2021). La segunda revolución cuántica podría brindar un futuro transformado, tanto por soluciones a problemas hasta ahora intratables por la computación clásica como por la minoración del cómputo de tiempo demandado por problemas caracterizados por conjuntos de datos masivos y complejos.

Sin embargo, las estimaciones sobre las inversiones futuras discrepan, a modo de ejemplo, McKinsey & Co. (2022) las situó entre 9 y 93 MM de dólares para el año 2040; International Data Corporation (Needham, 2023), en 16,4[11] MM de dólares para finales de 2027, e Inside Quantum Technology (2022), por encima de 630 M de dólares en 2027 y en unos 2,2 MM de dólares para 2030. Aun asumiendo ciertas discrepancias en la métrica, la gran amplitud en la horquilla de las cifras demuestra el elevado grado de incertidumbre sobre el futuro cuántico. Las principales causas se atribuyen a la falta de transparencia sobre el verdadero impacto comercial de las soluciones cuánticas, puesto que la información detallada es muy limitada, y al enorme reto tecnológico que supone desarrollar el primer ordenador cuántico universal, un hito imprescindible para la correcta ejecución de los algoritmos cuánticos puros, no exento de detractores, como el matemático de Yale, Kalai (2016).

El incipiente desarrollo de la tecnología cuántica[12] (Benioff, 1980) motiva que la mayoría de los fondos para la investigación provengan principalmente de fuentes públicas, un total de 31 MM de dólares a nivel mundial, de los cuales, 15,3 MM de dólares pertenecen a China; 7,2 MM de dólares a la Unión Europea, y 1,9 y 1,8 MM de dólares a Estados Unidos y Japón, respectivamente (McKinsey & Co., 2022). En el *ranking* de publicaciones científicas relevantes en el campo cuántico (Nature Index, 2021) el primer puesto es para China (24,7 %), muy de cerca Estados Unidos (23,9 %), ambos seguidos por la Unión Europea (22,3 %).

Por su parte, el Foro Económico Mundial ha puesto el foco en implantar las directrices globales para evaluar y gestionar las oportunidades y los riesgos de la computación cuántica,

11 En el cálculo se incluyen las inversiones realizadas por instituciones públicas y privadas, el gasto gubernamental en todo el mundo, el gasto en I+D de los proveedores de tecnología y servicios, y la financiación externa de los inversores de capital riesgo y las empresas de capital privado.

12 Las tres principales áreas de la tecnología cuántica son la computación, las comunicaciones y los sensores cuánticos.

fomentando valores fundamentales como la transparencia, la accesibilidad, la equidad, la inclusión y la responsabilidad, entre otros. Con este incentivo incluyó los Principios de Gobernanza de la Computación Cuántica en su agenda para 2022.

En Europa, la Comisión Europea lanzó la iniciativa *Quantum Technologies Flagship* (2018) para impulsar la investigación y la innovación cuántica a largo plazo. Con la publicación del Manifiesto Cuántico de 2016, la Unión Europea decidió destinar a lo largo de 10 años una suma de 1 MM de euros a diferentes proyectos de tecnología cuántica, destacando *OpenSuperQ*[13] y *AQtion*[14]. En la Agenda Estratégica de Investigación sobre Tecnologías Cuánticas se estableció el desarrollo del Internet cuántico[15] como objetivo a largo plazo. En este sentido, diferentes instituciones manifestaron una creciente inquietud por la seguridad de la criptografía actual, que podría romperse fácilmente cuando la tecnología cuántica esté suficientemente desarrollada, escenario plausible a partir del año 2030 (Mosca, 2018). Esta preocupación está en la raíz del anuncio hecho por el BIS, en junio de 2022, de que el centro del Eurosistema del BIS Innovation Hub[16] exploraría las implicaciones de la criptografía postcuántica[17] para los sistemas de pagos.

Mientras, en Estados Unidos, el 21 de diciembre de 2022, Joe Biden firmó la Ley Quantum de preparación para la Ciberseguridad, estrechamente relacionada con el Memorando de Seguridad Nacional (NSM-10[18]). En esta misma línea, la Agencia de Seguridad de los Estados Unidos (NSA[19]) fijó dos fechas claves, entre los años 2025 y 2027 muchas aplicaciones debían utilizar por defecto la criptografía postcuántica y el año 2035 fue establecido como límite para abandonar por completo la criptografía vulnerable a la computación cuántica.

---

13 OpenSuperQ es un proyecto en el que colaboran 10 socios internacionales de la academia y la industria para diseñar, construir y operar un sistema de procesamiento de información cuántica, basado en tecnología de superconductores, de hasta 100 qubit. Se presume que esta escala le permitirá situarse entre las plataformas líderes a escala mundial y a la cabeza de Europa. Dado su enfoque abierto e integrador, será puesto a disposición de forma sostenible y centralizada para usuarios externos con el fin de fomentar el progreso científico, sin supeditar su acceso o explotación a la inversión individual de los participantes. Uno de los principales resultados será el establecimiento de un prototipo funcional de un sistema de computación cuántica de alto rendimiento en el Forschungszentrum Jülich (FZJ) (https://opensuperq.eu/project).

14 *AQtion* es un proyecto europeo de investigación que tiene como objetivo desarrollar una computadora cuántica de 50 qubits con una tecnología de iones atrapados, robusta y compacta donde los usuarios no especialistas puedan diseñar y realizar aplicaciones. Para ello, están desarrollando un sistema escalable que es compacto, transportable y no necesita un entorno de laboratorio ultra estable para su funcionamiento. https://www.aqtion.eu/

15 Se piensa que el desarrollo de la próxima generación de Internet estará basado en la teleportación cuántica que permite transferir información cuántica de un lugar a otro, a través de una red de nodos. En este aspecto destaca que, por primera vez, Hermans, Pompili, Beukers, Baier, Borregaard y Hanson (2022) lograron la teleportación de información cuántica en una red entre nodos que no estaban conectados de forma directa.

16 El BIS *Innovation Hub* tiene como objetivo desarrollar bienes públicos de base tecnológica para apoyar a los bancos centrales y mejorar el funcionamiento del sistema financiero. Cuenta con varios centros en todo el mundo, establecidos en colaboración con los bancos centrales correspondientes. El centro del Eurosistema fue inaugurado en marzo de 2023.

17 La criptografía postcuántica hace referencia a aquella no dependiente del problema de la factorización que será tratado en los subapartados 9.4.3 y 9.4.4 del documento técnico.

18 El NMS-10, titulado «National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems», fue pubicado el 4 de mayo de 2022, en la página web de la Casa Blanca y firmado por Joe Bidden. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

19 NSA es el acrónimo, en inglés, de National Security Agency.

Por su parte, la FED, en su informe sobre ciberseguridad y resiliencia del sistema financiero de 2023, califica a la computación cuántica como una amenaza para el sistema financiero[20].

9.2 Fortalezas de la computación cuántica y diferencias con la clásica

La computación cuántica es una tecnología incipiente basada en procesos físicos completamente distintos a los de la computación convencional, no obedece a las leyes de la mecánica clásica, sino a las de la mecánica cuántica (Plank, 1900), lo que conlleva fuertes implicaciones en la forma de procesar información.

La principal diferencia entre la computación cuántica y la clásica consiste en las unidades fundamentales de almacenamiento de la información. En la cuántica se utiliza el qubit[21] frente al clásico bit[22]. En consecuencia, no es posible hacer uso de los ordenadores y de las aplicaciones tradicionales para desarrollar operaciones cuánticas, sino que es necesario el uso de algoritmos y de ordenadores cuánticos que procesen y transmitan la información de acuerdo a este nuevo paradigma[23].

La particularidad de un qubit es que es el resultado de la combinación lineal de dos estados, mientras el bit binario solo puede estar en un único estado de los dos posibles, cero o uno. Esta característica supone un cambio en la forma de cálculo, la matemática que subyace detrás es probabilística, a diferencia del cálculo determinista propio de la informática tradicional. De esta forma, la aplicación de la física cuántica a la informática permite nuevos algoritmos que pueden comprimir masivamente el tiempo de cálculo o abordar determinadas operaciones que están fuera del alcance de la informática tradicional. Entender mejor qué es un qubit, para tener una visión global de las propiedades diferenciadoras de la computación cuántica y su potencial, exige unas nociones mínimas de mecánica cuántica, que se explican a continuación.

En este epígrafe se introducen tres conceptos fundamentales de la física cuántica que, aplicados a la informática, logran un desarrollo extraordinario frente a la computación convencional. El primero de estos conceptos es la superposición de los qubits que incrementa la potencia de cálculo de la computación cuántica. En segundo lugar, el entrelazamiento cuántico que es indispensable para la comunicación cuántica y, por último, la medida cuántica que garantiza la seguridad de la encriptación cuántica. El objetivo de las explicaciones ofrecidas a lo largo de este epígrafe es aportar un conocimiento básico que permita comprender en qué se fundamenta la computación cuántica, por lo que han sido deliberadamente simplificadas.

20 Cybersecurity and Financial System Resilience Report (RaaS). https://www.federalreserve.gov/publications/cybersecurity-and-financial-system-resilience-report.htm

21 El termino qubit procede del inglés, «quatum bit».

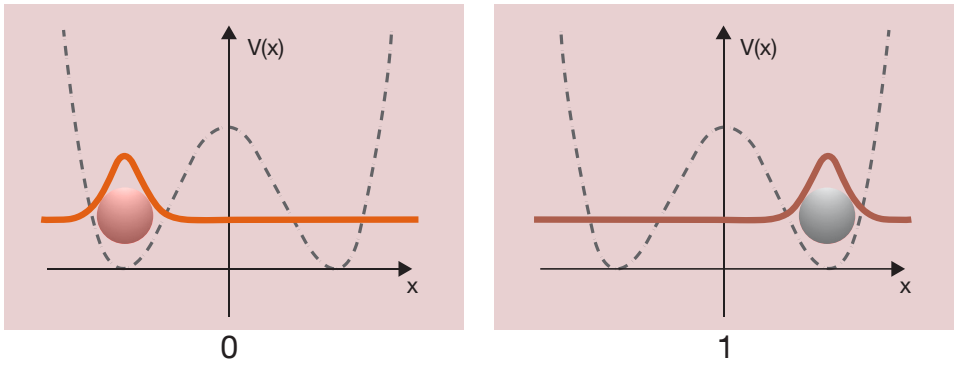
22 El término bit procede del inglés, «binary digit».

23 En el apartado 9.3 del documento técnico se plantea qué es un ordenador cuántico y su estado actual.

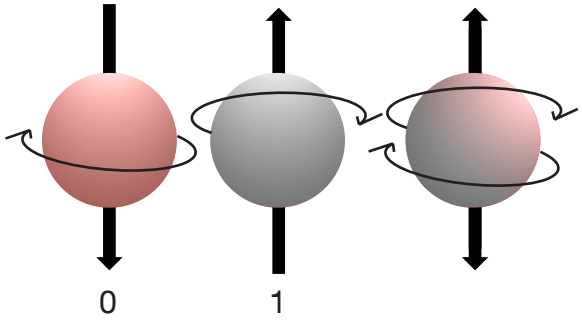
Esquema 2

Ilustraciones de ejemplos de sistemas cuánticos en la naturaleza

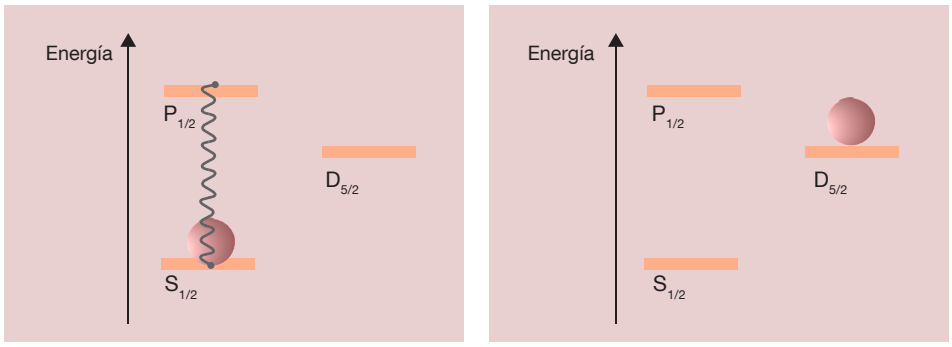
Posiciones de un átomo



Espín de una partícula



Niveles electrónicos de un átomo o ión



FUENTE: Elaboración propia.

9.2.1 La superposición. Computación cuántica

Aunque el concepto de qubit, *a priori,* puede parecer abstracto, en la naturaleza existen sistemas cuánticos que, al igual que los qubits, son el resultado de la superposición de dos estados. La posición de un átomo, el espín de una partícula o los niveles electrónicos de un átomo o un ión, son algunos de los ejemplos que sirven de inspiración a los científicos para diseñar los diferentes prototipos de ordenadores cuánticos (véase esquema 2).

La superposición cuántica se define como la suma de cada uno de los estados posibles del sistema (cero y uno), ponderados por su probabilidad asociada o su amplitud de probabilidad, alpha, para el estado cero, y beta, para el estado uno[24]. Estos dos parámetros, alpha y beta, son números complejos que pueden dar lugar a infinitas combinaciones de los estados, conformando un qubit en superposición.

Concepto de superposición de un qubit

Un qubit es una superposición de dos posibles estados (0 y 1).

$$\text{Qubit} = \alpha 0 + \beta 1 \quad \alpha, \beta, \in, C$$

donde, los dos posibles estados son 0 y 1; y sus respectivas probabilidades asociadas o amplitudes de probabilidad son α y β, de forma que:

$$|\alpha|^2 = \text{Probabilidad de obtener 0}$$

$$|\beta|^2 = \text{Probabilidad de obtener 1}$$

$$\rightarrow \quad |\alpha|^2 + |\beta|^2 = 1$$

$$\text{Qubit} = \frac{1}{\sqrt{2}}\,0 + \frac{1}{\sqrt{2}}\,1 \quad \leftarrow$$

$$\text{Probabilidad de obtener 0} = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} = 50\,\%$$

$$\text{Probabilidad de obtener 1} = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} = 50\,\%$$

La consecuencia de estas infinitas combinaciones posibles es que tanto la cantidad de información codificada en un qubit como su velocidad de procesamiento aumentan de forma exponencial[25] frente al bit. A modo de ejemplo intuitivo, la capacidad de almacenamiento y procesamiento de 8 qubits es equivalente a la de 256 bits clásicos. La expresión matemática de esta ley exponencial establece lo siguiente: 2^n bits equivalen n qubits (véase esquema 3).

9.2.2 El entrelazamiento. Comunicación cuántica

El entrelazamiento (Schrödinger, 1935) es una propiedad fundamental de la mecánica cuántica, sin equivalente en la física clásica, solo observable a nivel microscópico bajo unas determinadas condiciones.

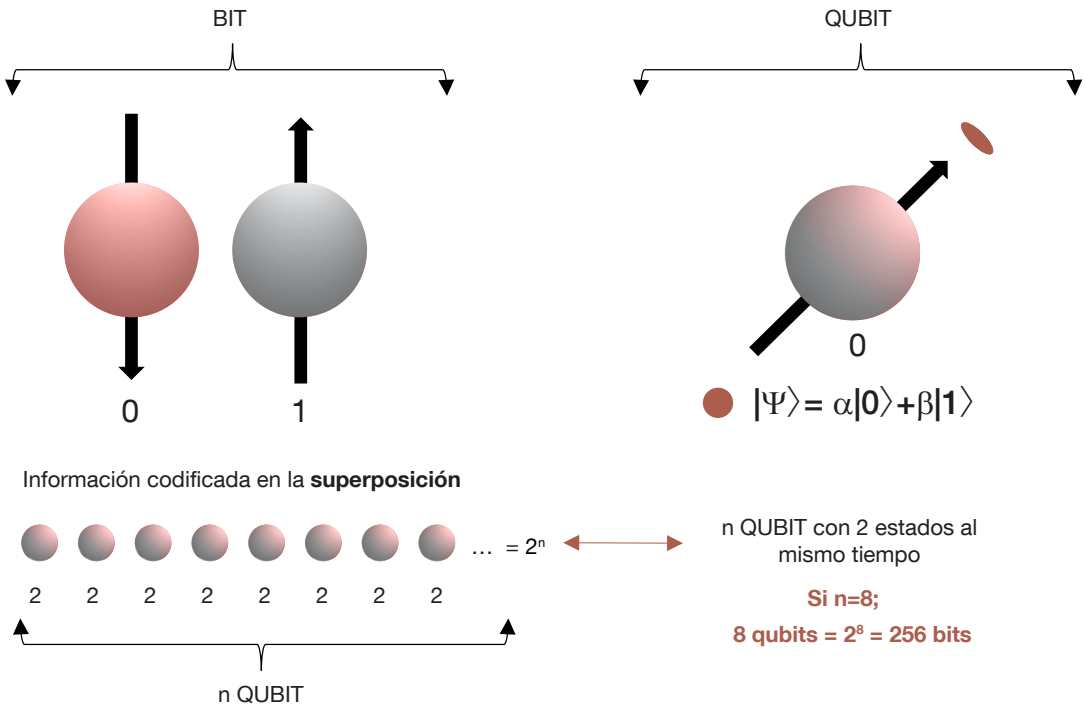
El concepto de entrelazamiento hace referencia a la conexión instantánea entre dos o más partículas, aun cuando estas se encuentren distanciadas espacialmente. El ejemplo más sencillo en la computación cuántica serían dos qubits entrelazados.

24 La suma de estos alpha y beta en valor absoluto elevados al cuadrado es igual a la unidad.

25 Por simplicidad se afirma que existe un aumento exponencial en la velocidad de procesamiento de la información. Teóricamente es así, aunque existen diferencias de potencia entre diferentes tipos de algoritmos cuánticos, según el cálculo que realicen. Algunos permiten un aumento exponencial y otros tan solo un aumento cuadrático.

Esquema 3

BIT *vs* QUBIT. La superposición cuántica



Formulación del Estado Cuántico en Notación de Dirac

Nº qubit	Nº estados en superposición	Estados posibles	Formulación del Estado Cuántico
1	$2^1 = 2$	$\|0\rangle$ $\|1\rangle$	$\|\Psi\rangle = \alpha\|0\rangle+\beta\|1\rangle$
2	$2^2 = 4$	$\|00\rangle$ $\|01\rangle$ $\|10\rangle$ $\|11\rangle$	$\|\Psi\rangle = a_0\|00\rangle + a_1\|01\rangle + a_2\|10\rangle + a_3\|11\rangle$
3	$2^3 = 8$	$\|000\rangle$ $\|001\rangle$ $\|010\rangle$ $\|011\rangle$ $\|100\rangle$ $\|101\rangle$ $\|110\rangle$ $\|111\rangle$	$\|\Psi\rangle = a_0\|000\rangle + a_1\|001\rangle + a_2\|010\rangle + a_3\|011\rangle + a_4\|100\rangle + a_5\|101\rangle + a_6\|110\rangle + a_7\|111\rangle$

FUENTE: Elaboración propia.

El estudio de este fenómeno, tan complejo como desconcertante, se encuentra en pleno auge dentro la comunidad científica dedicada a la información cuántica[26], entre otras razones, porque es la base de la comunicación cuántica, una de la principales áreas de la

26 En 2022, los físicos Alain Aspect, John F. Clauser y Anton Zeilinger recibieron el premio Nobel de física por sus trabajos sobre el entrelazamiento cuántico y la teleportación cuántica.

tecnología cuántica que incluye todas aquellas actividades relacionadas con la transmisión, almacenamiento y manipulación de la información cuántica, y que permite la teleportación cuántica, el Internet cuántico y la encriptación cuántica[27].

La encriptación cuántica puede ser utilizada para mantener la confidencialidad de todo tipo de información, ya sea financiera, empresarial, militar, gubernamental o relativa a la investigación y el desarrollo. Para comprender cómo se garantiza la inviolabilidad de la información cuántica y la plena seguridad de las claves cuánticas es necesario dar un paso más y describir otro concepto, algo complejo y no exento de controversia: la medida cuántica.

9.2.3 La medida. Seguridad de la información cuántica

Técnicamente, en computación cuántica medir equivale a observar un bit cuántico que colapsa a uno de los valores 0 y 1 del eje en el que se ha realizado la medición[28] (véase esquema 4). En física clásica, medir un sistema es una operación determinista que consiste en poner de manifiesto las propiedades que se encontraban presentes en dicho sistema. Sin embargo, esta asunción es errónea en la mecánica cuántica, puesto que el sistema cambiará de forma incontrolable durante el proceso de medición y, por esto, solo se pueden calcular las probabilidades de obtener un resultado u otro.

Concretamente, el proceso de medición en mecánica cuántica es bastante drástico y de carácter irreversible, no se puede recuperar el estado inicial con absoluta certeza. Esta particularidad se traslada a la computación cuántica, de forma que al medir un qubit se observa que su estado inicial se destruye, no se puede recuperar, garantizando la plena confidencialidad y seguridad de la información contenida en el qubit. La medición de la posición de un qubit conlleva pasar de un sistema probabilístico a un sistema determinista, de ahí la severidad del proceso de medición en términos cuánticos.

Los protocolos de encriptación cuántica brindan un sistema de seguridad demostrado y garantizado basado en tres pilares de las leyes de la física cuántica: el Teorema de no clonación (Wootters y Zurek, 1982)[29], que determinan que el entrelazamiento cuántico no se puede compartir y que la acción de medir en física cuántica destruye la posición del qubit[30]. La consecuencia final es que la información no puede ser interceptada por un tercero, por la propia naturaleza de su codificación y, por tanto, se infiere la propiedad de invulnerabilidad a la encriptación cuántica.

Además de las aplicaciones que supone en términos de encriptación cuántica, esta peculiaridad de la medida propicia que la computación cuántica sea ideal para tratar problemas

27 QKD es el acrónimo en inglés de *Quantum Key Distribution,* el término utilizado para la encriptación cuántica.

28 Queda fuera de las pretensiones de este documento el debate en relación a las distintas interpretaciones que filósofos y físicos hacen de la medición en la mecánica cuántica.

29 El Teorema de no clonación garantiza que un estado cuántico arbitrario no se puede copiar.

30 No existe la posibilidad de retorno al estado inicial para poder averiguar su posición.

Esquema 4

La medida cuántica. Representación de un qubit en la esfera de Bloch

Proyectar = Medir = Colapsar

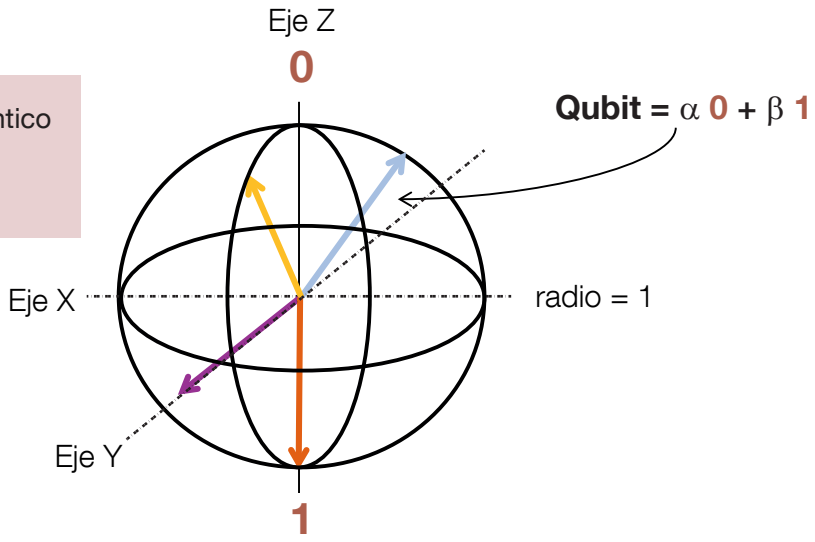
Los puntos se representan gráficamente como puntos en la esfera de Bloch

Infinitos puntos ➡ Infinitas combinaciones posibles

Qubit = Bit cuántico

0 1

Bit clásicos



Todos los ejes tienen **un 0 y un 1,** pero no son el 0 y el 1 de la computación clásica.
En **computación cuántica,** los qubits no están definidos en los estados 0 y 1.
Se habla de la **probabilidad de observar** el qubit en el **estado 0 o 1** cuando se mide.

FUENTE: Elaboración propia.

con numerosas posibles soluciones, tantas como las posiciones de los qubits, que al ser medidas colapsan, arrojando como resultado la mejor opción con una probabilidad asociada.

9.3 El presente y el futuro cuántico

Hoy en día, la investigación de la computación cuántica persigue principalmente dos objetivos: desarrollar algoritmos cuánticos que resuelvan problemas útiles más rápido y construir una plataforma de *hardware* robusta que utilice qubits para poder ejecutar dichos algoritmos. En esta etapa inicial, los casos de uso son en gran medida experimentales e hipotéticos, aunque se están acelerando los avances para propiciar su viabilidad comercial y su utilización en la industria. En última instancia, el máximo potencial de la computación cuántica podrá alcanzarse cuando se consiga el ordenador cuántico universal (véanse esquema 5 y recuadro 1).

En este epígrafe se explican algunos de los grandes retos del ordenador cuántico, así como el estado actual de los procesadores cuánticos; se abordan cuestiones sobre su potencial evolución futura, y las posibilidades que ofrecen los algoritmos cuánticos.

Recuadro 1

EL ORDENADOR CUÁNTICO UNIVERSAL

Construir el primer ordenador cuántico universal (LSUQC[1]) es un desafío tanto técnico como estructural, un factor determinante que condiciona el desarrollo y el uso de la computación cuántica.

En sus respectivos trabajos, los físicos Richard Feynman (1982) y David Deustch (1985) determinaron las condiciones para el desarrollo de un ordenador cuántico universal, definido como aquel dispositivo que combina la potencia de la computación clásica con la cuántica.

Las tres condiciones necesarias para considerar un ordenador cuántico universal según Feynman y Deustch son las siguientes:

- Se necesitan qubits con superposición y con entrelazamiento y un set de puertas lógicas cuánticas: CNOT, Hadamard y T.
- Ha de ser capaz de simular cualquier operación propia de un ordenador clásico.
- Adicionalmente, debe contar con la capacidad para simular sistemas físicos especialmente referidos a la física cuántica.

¿Cómo estamos de lejos del primer ordenador cuántico universal? Es posible medir el grado de avance en función de diferentes hitos o niveles.

1 Large Scale Universal Quantum Computer, en inglés. «Large Scale», generalmente significa que la capacidad de la computadora cuántica se adapta a ejemplos de problemas prácticos, mientras que el término «Universal» hace referencia a que puede ejecutar cualquier tipo de algoritmo cuántico.

9.3.1 La capacidad de los dispositivos cuánticos actuales

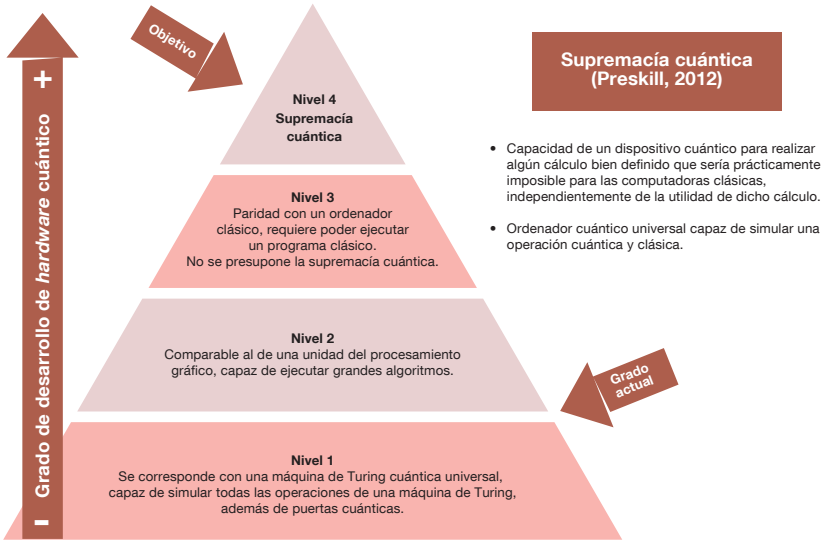
Como se comenta en el apartado 9.2 del documento técnico, no es posible usar el *hardware* tradicional para poner en práctica la tecnología cuántica. La realización de una computadora cuántica es una tarea extremadamente desafiante ya que, por lo general, los efectos de la mecánica cuántica se hacen evidentes solo a escalas muy pequeñas, cuando los sistemas cuánticos están adecuadamente aislados de los entornos circundantes. Para que un dispositivo cuántico pueda proporcionar resultados exactos y matemáticamente precisos se necesita corregir su computación y que esta sea totalmente tolerante a fallos.

Los dispositivos cuánticos actuales, llamados NIS (Preskill, 2018), están compuestos por decenas de qubits, pero en un futuro se espera que sean escalables a cientos. El número y la calidad de los qubits son actualmente bajos, lo que hace que las computadoras cuánticas sean propensas a errores y, a menudo, poco fiables en sus cálculos. De hecho, existe cierta polémica sobre si pueden aportar un valor significativo antes de que sean altamente tolerante a fallos (FTQC[31], en adelante). No cabe duda de que, en cualquier caso, a pesar de sus limitaciones, los dispositivos actuales constituyen un logro científico muy significativo en cuanto a la capacidad alcanzada para controlar sistemas cuánticos.

31 FTQC es el acrónimo en inglés de *Fault Tolerant Quantum Computer.* En general, un dispositivo tolerante a fallos es aquel que es capaz de funcionar con eficacia incluso cuando sus componentes elementales son imperfectos. La mayoría de los expertos están de acuerdo en que lo dominarán a largo plazo, sin ser posible determinar con certeza cuándo se producirá este hecho.

Esquema 5

Niveles que miden el grado de desarrollo del *hardware* cuántico



FUENTE: Elaboración propia.

Respecto a las perspectivas del futuro, la falta de transparencia[32] hace que sea complejo realizar una evaluación objetiva. Los criterios para establecer con firmeza la supremacía cuántica[33], si un dispositivo cuántico es más potente que una supercomputadora clásica, son difusos, en este sentido puede considerarse un objetivo dinámico, porque las computadoras clásicas y los algoritmos mejoran con el tiempo[34]. A lo largo de la literatura es muy habitual referirse a la ventaja cuántica como una mejora en la escala del tiempo de ejecución de una tarea frente al tiempo consumido por un dispositivo convencional. Sin embargo, Gómez *et al.* (2022) defienden un enfoque más amplio que considere otras variables, como el consumo de energía y el coste.

Actualmente, el grado de avance de los procesadores cuánticos se sitúa entre el nivel 1 y el nivel 2; son capaces de realizar operaciones lógicas, algunos algoritmos, pero no han alcanzado la paridad con el ordenador clásico. Esto se traduce en un modelo híbrido formado por dos máquinas separadas, un ordenador clásico que controla al procesador cuántico, en lugar de una única máquina universal.

32 Los Principios de Gobernanza de la Computación Cuántica del Foro Económico Mundial proponen un entorno de «Innovación Abierta» (Tema 3) para fomentar la trasparencia y «Crear Conciencia» (Tema 4), desacreditando los mitos actuales y disipando las exageraciones en relación a los hallazgos de la tecnología cuántica.

33 De forma general, la supremacía cuántica (Preskill, 2012) puede describirse como la capacidad de un dispositivo cuántico para realizar algún cálculo que sería prácticamente imposible para las computadoras clásicas, independientemente de la utilidad de dicho cálculo.

34 Aunque Boixo *et al.* (2018) están convencidos de que la supremacía cuántica puede lograrse a corto plazo con dispositivos cuánticos superconductores de aproximadamente cincuenta qubits, sin corrección de errores.

Recuadro 2

LOS SIETE REQUISITOS[1] QUE UN ORDENADOR CUÁNTICO UNIVERSAL DEBE CUMPLIR

1 Largos tiempos de coherencia cuántica, entendida como la estabilidad de la superposición de los qubits.

2 Alta escalabilidad, es decir, ordenadores cuánticos con gran cantidad de qubits para poder ejecutar los algoritmos cuánticos y de esta forma lograr alcanzar la supremacía cuántica. Esto requiere que previamente se realice una selección de qubits que asegure que sean escalables.

3 Alta tolerancia a los errores provocados por sobrecalentamiento, pérdidas en el sistema y errores en la ejecución de una puerta lógica.

4 Capacidad de inicializar los qubits en el estado deseado.

5 Set de operaciones cuánticas universales.

6 Capacidad de medir qubits al final y obtener el resultado después del proceso.

7 Transmisión de flyqubits[2]. Aunque no es considerado un requisito técnicamente necesario para la construcción de un ordenador cuántico universal, lo cierto es que tener interconectados varios ordenadores cuánticos a través del Internet cuántico permitiría explotar todo su potencial.

1 En la lista original elaborada por DiVinzenzo (2000) solo constan los criterios: 1, 2, 4, 5 y 6.
2 Los flyqubits o quibits voladores pueden transmitirse de manera fiable a distancias y a temperaturas macroscópicas, manteniendo intacta su información cuántica.

Recuadro 3

TIPOS DE DISPOSITIVOS CUÁNTICOS

El concepto de NISQ engloba a cualquier dispositivo cuántico, analógico o digital, de escala media, en el que se producen errores (ruido). Nótese que existen tres principales tipos de computadoras cuánticas. De menor a mayor alcance práctico general y potencia computacional: *quantum annealers*[1], *quantum simulators*[2], y finalmente, los ordenadores cuánticos universales o de propósito general, que son dispositivos digitales que explotan directamente la superposición, el entrelazamiento y la interferencia para resolver, en principio, cualquier tipo de problema. Aunque, inicialmente, tanto los *quantum annealers* como los quantum *simulators* se clasificarían como NISQ, hay parte de la literatura que considera que los NISQ son solo los dispositivos digitales (algunos *simulators),* y los diferencian de los analógicos todos los *quantum annealers* y otros *simulators* porque la corrección de los errores es más complicada (Sevilla y Riedel, 2020).

1 Son dispositivos analógicos capaces de resolver un conjunto limitado de problemas de minimización y de optimización. D-Wave ofrece este tipo de dispositivos desde 2011 (Merali, 2011).
2 Aprovechan la superposición y el entrelazamiento para simular modelos inspirados en sistemas reales, normalmente de naturaleza física, aunque también pueden implementarse problemas de optimización más generales. Pasqal es un proveedor de este tipo de dispositivos tanto digitales como analógicos (Henriet, 2020).

En un futuro, conforme se superen los diferentes niveles de avance en la computación cuántica, se podría llegar al nivel 4, la supremacía cuántica respecto a la computación clásica. De forma general, la supremacía cuántica (Preskill, 2012) puede describirse como la capacidad de un dispositivo cuántico para realizar algún cálculo que sería prácticamente imposible para las computadoras clásicas, independientemente de la utilidad de dicho cálculo.

Para lograr mayor grado de alcance en los procesadores cuánticos se precisa de una combinación de capital, experiencia tanto en física cuántica experimental como teórica y un dominio profundo de las opciones relevantes para su implementación. Actualmente, existen limitaciones tecnológicas respecto al *hardware* que impiden una completa preservación y control del comportamiento cuántico. Cualquier implementación específica de un sistema cuántico, a través la tecnología disponible a día de hoy, tiene el problema de la decoherencia: los sistemas son particularmente propensos a interactuar con su entorno y a perder las características cuánticas con las que ha sido diseñado para codificar y procesar la información, por lo tanto, se pierde el control sobre él. Las computadoras cuánticas podrían ser tan fiables como sea necesario una vez alcanzado un mínimo estándar de calidad y cierta escalabilidad e integración de los qubits físicos subyacentes. En el recuadro 2 se indican los siete retos pendientes a día de hoy para alcanzar un ordenador cuántico universal.

9.3.2 Algoritmos cuánticos

Por su parte, un algoritmo cuántico consiste en una serie de operaciones cuánticas, puertas lógicas, realizadas en un ordenador cuántico, que se aplican sobre varios qubits para modificar su estado y obtener un resultado. Al medir la salida de un algoritmo cuántico se obtiene un resultado con una probabilidad asociada, debido a la particularidad de la medida cuántica. Gracias a la superposición y al entrelazamiento de los qubits, la capacidad de almacenamiento y el procesamiento de la información cuántica siguen una ley exponencial respecto a la convencional. Por tanto, la computación cuántica es un modo diferente de programación que permite nuevos algoritmos, no constituye una versión mejorada de las técnicas o de los equipos utilizados en las actuales supercomputadoras[35].

Según la teoría de la complejidad computacional, los algoritmos cuánticos son específicamente más eficientes resolviendo problemas de decisión tipo BQP[36] (tiempo polinomial cuántico con error acotado), que se caracterizan por tratar información de entrada y de salida muy pequeña y arrojan un gran número de resultados posibles. La idea que subyace es que los algoritmos cuánticos no tienen el alcance suficiente para resolver cualquier tipo de problema matemático, sino una determinada clase acotada de problemas, como, por ejemplo, la factorización.

Hay dos cuestiones relevantes respecto al uso de los algoritmos cuánticos, saber si la aplicación actual para un problema de interés admite una aceleración cuántica y cuándo podrá ponerse en práctica. Actualmente, se conocen menos de 100 algoritmos cuánticos (Jordan, 2022) con una aceleración teóricamente comprobada frente a la computación convencional. Además, el *hardware* cuántico no está lo suficientemente avanzado como para resolver cualquier problema de relevancia práctica más rápido que las computadoras clásicas, como se detalla en el apartado 9.4. del documento técnico.

---

35 Esta afirmación es completamente cierta en el caso de algoritmos cuánticos puros. Sin embargo, existen adaptaciones de los algoritmos cuánticos, los algoritmos de inspiración cuántica y los híbridos, a medio camino entre los algoritmos cuánticos y clásicos, pudiendo ser entendidos como una evolución de los tradicionales.

36 El acrónimo en inglés de BQP significa *Bounded-Error Quantum Polynomial-Time.*

Es importante destacar que la aceleración que pueden proporcionar los algoritmos cuánticos puede diferir significativamente.

En el medio plazo, hasta conseguir un dispositivo de computación cuántica que sea accesible y asequible, lo más probable es que las aplicaciones comercialmente viables de computación cuántica se centren en adaptar los algoritmos[37] a los casos de uso que reporten un mayor valor[38].

Para determinar cuándo la aceleración cuántica será relevante para un dominio en particular se requiere una comprensión profunda de los propios algoritmos cuánticos, de los recursos cuánticos necesarios para ejecutar los algoritmos, la medida en que esos recursos se pueden reducir mediante el rediseño de los algoritmos, así como estimar la línea de tiempo del desarrollo del *hardware* cuántico. Según la consultora McKinsey & Co. (Masiowski, Mohr, Soller y Zesco, 2022), esta posibilidad ha propiciado un significativo y rápido aumento de nuevas empresas centradas en el desarrollo de programas cuánticos, de un puñado, en 2013, a más de 200, en 2021.

9.3.3 Previsiones futuras

Por lo general, se cree que, hasta alrededor de 2030, los casos de uso de la computación cuántica tendrán un modelo operativo híbrido, donde, por ejemplo, las computadoras convencionales de alto rendimiento podrán beneficiarse de los algoritmos de inspiración cuántica.

Son varias las empresas que afirman que podrán ofrecer un dispositivo de computación cuántica tolerante a fallos (FTQC) entre 2026 y 2030, aunque algunos expertos de la industria son más pesimistas. A medida que el *software* de computación cuántica continúe desarrollándose, las organizaciones podrán actualizar sus herramientas de programación hasta que, finalmente, usen herramientas completamente cuánticas personalizadas. En un futuro, se espera que la industria madure lo suficiente como para ofrecer una computación cuántica personal, prestando un servicio llave en mano que genere grandes beneficios para quienes la controlen.

Gómez *et al.* (2022) consideran que es difícil predecir la evolución de la tecnología cuántica en los próximos 5 o 10 años. Estiman que la tecnología disponible será insuficiente[39]

---

37 En este momento se están utilizando algoritmos híbridos o de inspiración cuántica porque su profundidad es menor. Los algoritmos de inspiración cuántica son algoritmos clásicos en los que se puede emular de forma clásica el fenómeno cuántico esencial que proporcionaría el aumento de velocidad (https://learn.microsoft.com/es-es/azure/quantum/optimization-overview-introduction). Por su parte, las arquitecturas híbridas más avanzadas aportan una integración más estrecha y enriquecida entre el cálculo clásico y el cuántico. (https://learn.microsoft.com/es-es/azure/quantum/hybrid-computing-concepts).

38 Para ello, la mayoría de los proveedores de servicios de computación cuántica ofrecen acceso gratuito a sus plataformas en la nube, permitiendo a los primeros usuarios experimentar con la tecnología y construir comunidades de desarrolladores. Esto impulsa la identificación del uso de sus aplicaciones a problemas específicos, ayudando a mejorar la investigación y el desarrollo de paquetes cuánticos personalizados.

39 Constará de una docena de qubits (físicos o lógicos) con errores en operaciones mayores que 10-5 que pueden ejecutar circuitos pequeños, de unos 1000 pasos, antes de que el resultado colapse a valores inútiles y sin sentido.

Recuadro 4

PRINCIPALES PROPUESTAS DE PLATAFORMAS DE QUBITS FÍSICOS PARA UN PROTOTIPO DE COMPUTADORA CUÁNTICA DE PROPÓSITO UNIVERSAL[1]

1 Superconducting qubit: lo siguen IBM, Google, D-Wave y diversas universidades.

2 Iones atrapados: Universidades, Peter Zoller e Ignacio Cirac (1995).

3 Quantum dots: Intel.

4 Topological qubits: Microsoft, Bell Labs.

5 Diamond vacancies Quantum: diamon technologies.

6 Photonic qubits: Universidades.

7 Nuclear Magnetic Resonance: IBM.

1 Las diferentes propuestas de prototipos de dispositivos cuánticos se diferencian en el tipo de plataforma en la que se realizan los qubits físicos y en cómo se implementa la corrección del error cuántico (QEC, en inglés), particularmente, en su última forma de tolerancia al error. No se exhibe una lista exhaustiva de todas las realizaciones físicas estudiadas hasta la fecha, tan solo las más relevantes.

para la satisfactoria ejecución de los algoritmos cuánticos teóricos que requieren una cantidad extremadamente alta de qubits y/o implican un circuito de pasos demasiado profundo con respecto al tiempo de coherencia realista.

Por su parte, Sevilla y Riedel (2020) estimaron que era poco probable[40] tener un dispositivo FTQC basado en la tecnología de superconductores antes de 2026 y que existan dispositivos cuánticos capaces de factorizar RSA-2048[41] antes de 2039, y en el subapartado 9.5.1 del documento técnico se explica con más detalle el fundamento y la vulnerabilidad de este tipo de algoritmos.

En 2021, los expertos cuánticos consideraron que la plataforma de qubits físicos (véase recuadro 4) cuyo desarrollo parecía más prometedor era la de los superconductores, seguida por la de iones atrapados (Mosca y Piani, 2021). Sin embargo, en 2022, los importantes avances en las plataformas de computación cuántica de átomos fríos (Bluvstein *et al.* 2022) captaron también la atención de los especialistas cuánticos. En general, hay algunas propuestas que son líderes, pero no se ha identificado un claro ganador e incluso es posible que más de una plataforma finalmente desempeñe un papel importante (Mosca y Piani, 2022). Los superconductores continúan siendo la opción favorita del 47 % de los expertos para la implementación física con la que realizar una computadora cuántica de aproximadamente 100 qubits lógicos en los próximos 15 años. La siguen los iones atrapados, la óptica cuántica (que incluye los fotones integrados) y los átomos fríos.

Sin duda, el desarrollo futuro de la tecnología cuántica se verá condicionado por la capacidad de obtener resultados satisfactorios en línea con la publicidad y las expectativas

40 Poco probable es cuantificado con un nivel de confianza inferior al 5 % en el ajuste.

41 El RSA-2048 es un algoritmo de encriptación internacionalmente usado en la seguridad bancaria y estatal. La clave RSA-2048 bits requiere millones de años para ser factorizada por un ordenador clásico, Kleinjung *et al.* (2010).

Recuadro 5

AVANCES ALENTADORES EN COMPUTACIÓN CUÁNTICA

Algunos científicos opinan que los qudits[1] podrían ser la clave para facilitar la funcionalidad y la creación de la computación cuántica. La consecuencia de los estados adicionales que proporcionan los qudits es el aumento de su potencia computacional, son más eficientes en términos de tiempo que los qubits y, por tanto, desempeñan un mismo volumen de trabajo en un menor tiempo. «Un qudit con cuatro o cinco niveles es capaz de funcionar como un sistema de dos qubits ordinarios. Y ocho niveles son suficientes para imitar un sistema de tres qubits», Popov, Kiktenko, Fedorov y Man'ko (2016). En esta línea, el estudio de Chi *et al.* (2022) muestra que se podría acelerar la construcción de una computadora cuántica a gran escala. Presentaron un procesador cuántico programable en qudits, con una tecnología cuántica fotónica integrada y qudits con capacidad, precisión y eficiencia mejoradas. El control y la programación de dispositivos cuánticos en qudits brinda la posibilidad de comunicaciones cuánticas resistentes al ruido, simulaciones moleculares cuánticas delicadas y cálculos cuánticos eficientes, exhibiendo un gran potencial para mejorar las capacidades de las tecnologías cuánticas basadas en qubits.

Otro ejemplo de avance muy alentador es el mostrado por Kiczynski, *et al.* (2022), que describieron observaciones de más de 150.000 qubits de silicio de tipo «centro T» de fotones-espín, un hito importante que abre oportunidades inmediatas para construir ordenadores cuánticos de escala masiva y el Internet cuántico para su conexión, ya que el silicio puede producir qubits muy estables y duraderos. Además, la industria mundial de semiconductores dedicada a la fabricación de dispositivos convencionales ya es capaz de fabricar a escala chips informáticos de silicio a bajo coste con un grado de precisión asombroso. Los autores opinan que encontrar la forma de crear procesadores cuánticos en silicio, reutilizando la industria de semiconductores, representaría una ventaja competitiva casi insuperable en la carrera internacional por el ordenador cuántico.

1 Qudit, proviene del inglés «quantum dit», es la unidad de información cuántica descrita por d-estados en superposición, donde el número de estados es un número entero siempre superior a 2. Por tanto, engloban a los qutrits y a los ququarts, con tres y cuatro estados posibles, respectivamente.

generadas (véase recuadro 5). En caso contrario, la inversión podría congelarse o incluso reducirse, dando lugar al llamado «invierno cuántico» (Mosca y Piani, 2021), que implica un progreso lento y una disminución de la financiación, lo que llevaría a una desaceleración sustancial en el desarrollo de una computadora cuántica relevante.

9.4 Aplicaciones de la computación cuántica en las finanzas

En un futuro, esta nueva metodología podría revolucionar la industria financiera, una vez que estén disponibles computadoras cuánticas robustas a gran escala, aunque la cuestión de fondo, sobre cuándo exactamente se materializará su implementación, es una controvertida incógnita. Bajo el supuesto de un escenario positivo, en el que se descuenta que en esta misma década las computadoras cuánticas superarán las capacidades de las clásicas, muchos de los principales bancos e instituciones financieras están invirtiendo una gran cantidad de recursos en proyectos cuánticos. El objetivo final es que la computación cuántica se integre en sus operaciones habituales, reduciendo el tiempo y la memoria computacional, conduciendo a una escalabilidad y una precisión sin precedentes en los cálculos. Más prudentes en cuanto a los plazos, los expertos independientes consideran que actualmente se trata de una mera especulación, resultando complicado identificar con claridad aquellas áreas donde la computación cuántica desempeñaría un papel fundamental de forma casi inminente.

El gran reto es la adaptación de los algoritmos cuánticos conocidos a problemas financieros específicos para su rápida implementación. En términos generales, los

desarrolladores de los algoritmos afirman que la computación cuántica es extremadamente eficiente en el campo de las finanzas, resolviendo problemas de optimización de carteras, fijación de precios de derivados, modelos de riesgos, procesamiento del lenguaje natural, detección de fraudes de tarjetas y transferencias, análisis de redes junto con el aprendizaje automático y, al igual que en otros sectores, en ciberseguridad.

A lo largo de este epígrafe, se presenta la identificación de los casos de uso más relevantes en el sector financiero que, al estar condicionada por la incertidumbre antes descrita, se limita a un ejercicio de carácter preliminar y no exhaustivo.

Metodologías

Tomando como inspiración las clasificaciones propuestas por Bouland, Van Dam, Joorati, Kerenidis y Prakash (2020) y Herman *et al.* (2022) se identifican tres grandes metodologías cuánticas para resolver problemas propios de la banca: la modelización estocástica, la optimización y el aprendizaje automático. A continuación, se describen los hallazgos, las posibles implementaciones y/o las limitaciones y los casos de uso.

9.4.1 Modelización estocástica: Montecarlo y ecuaciones diferenciales parciales

En finanzas, la modelización estocástica se utiliza para calcular el valor esperado de una determinada variable aleatoria que describe las condiciones de los mercados financieros o para tomar decisiones de inversión; generalmente con el objetivo de maximizar el rendimiento y/o minimizar el riesgo. Algunos ejemplos de uso son los precios de las acciones, el pago esperado de un derivado financiero en un momento futuro que determina el precio del derivado o los tipos de interés y sus volatilidades.

Para realizar este cálculo es necesario resolver las ecuaciones diferenciales estocásticas (EDE, en adelante), que rigen la evolución de los procesos estocásticos con los que se calcula el valor esperado de la variable aleatoria en cuestión. Si bien para algunos de los casos simples, como la ecuación de Black-Scholes (1973) para opciones europeas, las soluciones analíticas proporcionadas por las EDE funcionan muy bien; lo cierto es que la gran mayoría de los modelos financieros involucran enfoques numéricos más complejos que conllevan técnicas como la integración de Montecarlo y las ecuaciones diferenciales parciales (EDP, en adelante) que en numerosas ocasiones presentan deficiencias que podrían ser corregidas en su versión cuántica.

Montecarlo

Con el método de integración clásico de Montecarlo (MCI, en adelante) se logra obtener una solución aproximada a problemas del ámbito financiero que incluyen un elemento de incertidumbre o de aleatoriedad en su predicción y son considerados intratables analíticamente o que, debido a su gran dimensión, escalan mal los métodos numéricos. Concretamente, en el ámbito financiero, el MCI resulta de especial utilidad para la gestión del riesgo, la evaluación de carteras de inversión y la estimación del precio de derivados. Los

inconvenientes de la metodología clásica residen en que para hallar una solución altamente precisa se requiere de grandes cantidades de tiempo y de potencia computacional, y, adicionalmente, se recurre a simplificaciones de las expresiones matemáticas que desvirtúan en mayor o en menor medida el problema. Estas circunstancias motivan el atractivo de la aplicación de un enfoque cuántico.

Precisamente, Montanaro (2015), Brassard, Hoyer, Mosca y Tapp (2000) y Heinrich (2002) demostraron teóricamente que existe un algoritmo cuántico MCI (QMCI, en adelante) que soluciona estas dificultades, proporcionando una aceleración cuadrática con el mismo error deseado que la versión clásica y, bajo ciertas consideraciones, además, contaría con la capacidad para abordar casos bastante genéricos (Gómez *et al.,* 2022). Sin embargo, el QMCI se enfrenta a dos requisitos que comprometen su implementación: (a) no existe una computadora cuántica tolerante a fallos a gran escala, y (b) necesita la preparación previa de un estado cuántico arbitrario, un problema altamente complejo que todavía no se ha resuelto satisfactoriamente[42].

La limitación de la ventaja cuántica del algoritmo QMCI (véase recuadro 6) se ha puesto de manifiesto en la práctica cuando ha sido utilizado en ejercicios de análisis y de gestión del riesgo, a través del cálculo del Valor en Riesgo (VaR) y el Valor en Riesgo Condicional (CVaR) o para fijar el precio de una cartera de 5 activos. En ambos casos se concluye que es imprescindible una mejora significativa del *hardware*[43]; en el caso del VaR y el CVaR, para modelizar escenarios más realistas, Woerner y Egger (2019) y Egger, García, Cahué y Woerner (2021)[44]; y en el caso de la cartera de activos, para poder ampliar el número de variables estocásticas incluidas, así como para la precisión de los cálculos (Sanz-Fernández *et al.,* 2021)[45].

En cuanto a la estimación de los precios de derivados aplicando el QMCI, en el corto plazo cuenta con un importante obstáculo, y es que los dispositivos cuánticos experimentales (NISQ) cuentan con una capacidad insuficiente para realizar una rigurosa corrección del error cuántico[46] y un posterior cálculo (Bouland, Van Dam, Joorati, Kerenidis y Prakash, 2020).

---

42 Las soluciones hasta ahora estudiadas presentan diversos inconvenientes, por ejemplo, el algoritmo Grover-Rudolph (2002), si bien es muy eficiente en la carga de distribuciones integrables, también conlleva la pérdida de la aceleración cuadrática que proporciona QMCI frente su homónimo clásico (Chakrabarti, Krishnakumar, Mazzola, Stamatopoulos, Woerner y Zeng, 2021). Otras alternativas como los métodos unitarios (Rattew y Rebentrost, 2023), (Gómez *et al.* 2022) y (Rattew y Koczor, 2022) suelen ser incompatibles con el algoritmo cuántico de ampliación de estimación cuántica (Quantum amplitude estimation, QAE, en adelante) y por tanto impracticables.

43 Se necesita una computadora cuántica con mayor el número de qubits y una reducción de los errores.

44 Fue utilizado el dispositivo NISQ del IBM Quantum Experience. *IBM Quantum Composer* e *IBM Quantum Lab* forman una plataforma en línea que permite el acceso público y prémium a los servicios de computación cuántica basados en la nube proporcionados por *IBM Quantum. IBM Quantum Composer* permite crear circuitos con una interfaz que luego pueden ejecutarse en simuladores o *hardware* cuánticos reales. *IBM Quantum Lab* permite crear programas o experimentos con un kit de desarrollo de *software, Qiskit,* en un entorno *Jupyter Lab* personalizado. Para más información se recomienda visitar la página https://www.ibm.com/quantum/tools.

45 Sanz-Fernández *et al.* (2021) eligieron algoritmos de carga y de lectura que permitieron fijar el precio de una cartera compuesta por 5 activos con dos de las computadoras cuánticas disponibles actualmente basadas en iones atrapados (IonQ y AQtion Project), logrando estimar eficientemente el valor intrínseco a largo plazo de la cartera con un método basado en el QAE y una nueva implementación de Gordon-Shapiro (1956). Sus resultados, además de consistentes con el *bechmark* clásico de Montecarlo, mostraron errores estadísticos cuadráticamente inferiores con el mismo coste computacional.

46 Supone técnicamente un notable incremento de los gastos generales de preparación del estado para el algoritmo cuántico y una pérdida de la cantidad de los qubits físicos disponibles para el cálculo en sí, la consecuencia final es una menor velocidad de cálculo (véase recuadro 5).

Recuadro 6

LIMITACIONES DEL MONTECARLO CUÁNTICO Y LA REDUCCIÓN DE LOS RECURSOS COMPUTACIONALES

Bouland, Van Dam, Joorati, Kerenidis y Prakash (2020) consideran que la principal limitación de los algortimos QMCI es la profundidad del circuito que requieren, por lo que las investigaciones están orientadas a averiguar en qué medida podría relajarse este supuesto mediante la implementación de diferentes técnicas. Si bien no se puede recuperar la aceleración total del algoritmo cuántico puro con circuitos menos profundos, se cree que podría existir la posibilidad de recuperar una aceleración parcial. Entre las soluciones técnicas propuestas, Kerenidis y Prakash (2017) proponen desarrollar algoritmos NISQ híbridos[1], lo que podría considerarse una solución con vista al futuro, puesto que los NISQ actuales tampoco cuentan con la potencia suficiente para su ejecución. Por tanto, la relevancia de estos nuevos métodos QMCI dependerá del futuro progreso del *hardware* cuántico.

Los dos parámetros claves para controlar la aceleración cuántica de estos nuevos algoritmos cuánticos de menor profundidad se determina por dos parámetros esenciales: la tasa de error y la velocidad de tiempo efectiva[2].

La velocidad de las tecnologías cuánticas actuales es más lenta que las de la CPU clásicas, y esta ralentización podría ser más significativa si el algoritmo requiere la corrección de errores cuánticos, debido a los gastos generales que precisan. Por lo tanto, se debe esperar que un futuro dispositivo cuántico funcione con una ralentización inicial en relación a los dispositivos clásicos actuales.

La tasa de error efectiva del dispositivo cuántico es la tasa de ruido presente en las computadoras cuánticas actuales, limita la profundidad de los cálculos cuánticos que se pueden realizar sin errores, por lo que no podrán realizar variantes profundas del algoritmo de Kerendis y Prakash (2020) al no poder realizar muchas «muestras cuánticas» en serie. Cuanto mayor sea la tasa de error de las máquinas cuánticas, mayor será su limitación en el uso de estos algoritmos.

También es crucial la interacción entre estos dos parámetros: las máquinas con una tasa de error más bajas pueden proporcionar aceleraciones cuánticas más grandes (ya que pueden ejecutar circuitos más profundos) y los dispositivos cuánticos con velocidad de tiempo más rápidos también pueden generar aceleraciones cuánticas más fácilmente (sufren de menor desaceleración inicial). Idealmente, en un futuro sería deseable poder tener máquinas cuánticas con bajas tasas de error y con alta velocidad de tiempo.

En resumen, los métodos QMCI de baja profundidad amplían la posibilidad de aceleraciones cuánticas a regímenes de parámetros mucho más grandes, a los que uno puede comenzar a acercarse a medida de que se disponga de puertas más rápidas y de mejor calidad (ya sea por tasas de error físico más bajas o por la implementación de corrección de errores). Dada la incertidumbre en la línea de tiempo para el desarrollo del *hardware* cuántico, la respuesta a la pregunta de cuándo se podrían ejecutar los métodos cuánticos de Montecarlo a escala seguirá evolucionando tanto con la llegada de nuevo *hardware* como con mejores algoritmos y códigos de corrección de errores. A pesar de que el *hardware* actual no puede cumplir con los requisitos, ni siquiera de los métodos de Montecarlo de baja profundidad.

1 Estos algoritmos NISQ híbridos consisten en una combinación de técnicas clásicas y cuánticas de Montecarlo para utilizar circuitos de menor profundidad, aumentando el número de ejecuciones paralelas con qubits con mucha menor calidad que los necesitados por el algoritmo cuántico estándar, preservando una aceleración demostrable frente a los clásicos, y su escalado de rendimiento es óptimo.

2 La velocidad de tiempo efectiva de la computadora cuántica determina cuánto tiempo lleva realizar una muestra cuántica con el dispositivo.

No obstante, a largo plazo, cuando las computadoras cuánticas tolerantes a fallos estén disponibles, se espera que el algoritmo QMCI pueda estimar los precios de los derivados[47] con una altísima precisión y prácticamente en tiempo real (Gupt y Bromley, 2018).

Ecuaciones diferenciales parciales

Las ecuaciones diferenciales parciales (EPD) son una alternativa al MCI para resolver este tipo de problemas financieros donde se necesita estudiar procesos estocásticos subyacentes. Un ejemplo de uso son las EDP de Black-Scholes (1973) para la fijación de precios de

47 Rebenstrot, Gupt y Bromley (2018) exploraron la aplicación del algoritmo cuántico para la fijación de precios de bonos y opciones de compra simples. Concretamente para opciones europeas y asiáticas.

derivados financieros. La conexión entre las EDE y EDP se establece con las fórmulas de Feynman-Kac (Kac, 1949; Feynman, 2005), que cuentan con diferentes adaptaciones de su enunciado según el problema matemático, aunque, y a pesar de ello, presentan problemas de convergencia (Kloeden y Platen, 1992).

La combinación de algoritmos para resolver EDP con el aprendizaje automático cuántico (QML[48], en adelante) es muy esperanzadora (Gómez *et al.* 2022), porque se ha demostrado que el QML puede ser implementado en un NISQ, obteniendo resultados robustos que pueden presentar algunas ventajas teóricas[49] interesantes sobre sus homólogos clásicos (Huang *et al.* 2021). Sin embargo, el inconveniente es que los ejemplos del mundo real implican una dimensión demasiado grande para ser tratada eficientemente usando las computadoras cuánticas actuales. Hasta el año 2020, este algoritmo solo se ha probado en sistemas con un puñado de qubits, por lo que no ha sido posible demostrar una ventaja sobre los métodos clásicos. Por este motivo, se piensa que este tipo de algoritmos no podrán ser utilizados en un futuro próximo, e incluso entonces es posible que su aplicación sea limitada. En el apartado de aprendizaje profundo se comentan los últimos hallazgos de un subtipo de redes neuronales aplicado a la resolución de las EDP.

9.4.2 Optimización de carteras

Para el diseño de fondos de inversión, de planes de pensiones y de fondos cotizados (ETF, en adelante) es especialmente útil la optimización de carteras de inversión[50] (Markovitz, 1952); un problema considerado NP-hard por la teoría de la complejidad computacional, que resulta intratable mediante los medios clásicos en su versión discreta y que se complica todavía más conforme se incorporan restricciones más realistas[51], implicando un ejercicio dinámico de rebalanceo.

Existen distintos enfoques de algoritmos cuánticos para resolver o para aproximar la solución a la optimización de una cartera. Cada uno de ellos conlleva un diferente grado de aceleración cuántica dependiendo de la complejidad de las restricciones impuestas.

Por una parte, la implementación del algoritmo cuántico para la optimización de carteras con restricciones de positividad (Kerenidis, Prakash y Szilágyi, 2019) está muy limitada por el alcance previsto para los NISQ en el corto y el medio plazo, siendo el principal desafío de esta técnica lograr la reducción de requisitos de *hardware.*

---

48 *Quantum Machine Learning,* en inglés.

49 Mediante la utilización del concepto de «proyección cuántica de kernel» se logra reducir la dimensión del problema, mostrando resultados numéricos que prometen una ventaja cuántica en el aprendizaje de los algoritmos.

50 En 1952 Markowitz desarolló la Teoría Moderna de Carteras, asumiendo el supuesto de que los inversores son adversos al riesgo y, consecuentemente, prefieren una cartera con el mínimo riesgo para un determinado rendimiento objetivo.

51 Por ejemplo, no permitir la venta al descubierto (restricción de positividad), que los activos tengan incrementos fijos de volumen (restricciones de números enteros), el impacto de los movimientos de la cartera en el mercado o establecer límites superiores en la cantidad a invertir, por limitaciones en la liquidez. A esto se debe añadir la variación a lo largo del tiempo de las correlaciones entre activos y los costes de transacción, por todo esto, la trayectoria no tiene un óptimo local en cada momento.

De otra parte, para establecer un límite en la cantidad que se ha de invertir en cada activo, en la optimización con restricciones de enteros, se ha propuesto utilizar algoritmos cuánticos basados en técnicas de optimización combinatoria[52].

En la práctica se ha mostrado cómo implementar con éxito restricciones complejas al problema de la optimización cuántica de una cartera de inversión utilizando datos reales (S&P100 y S&P500) en un tipo de NISQ, el QA-híbrido de D-Wave (Palmer, Shain, Hernández, Muget y Orús, 2021). A pesar de tener un gran potencial para la generación de ETF, esta metodología entraña una importante limitación, y es que no incorpora dinámica.

Se están realizando importantes avances para mejorar la complejidad del modelo de optimización cuántica de una cartera, de forma que incluyan términos adicionales tales como la reinversión de dividendos, los costes de transacción por el reequilibrio de la propia cartera y una mayor diversidad de activos que permitan la creación de ETF. Con este fin, se han implementado técnicas para limitar el ejercicio de optimización a un subconjunto de activos, restricciones de cardinalidad, en un dispositivo NISQ[53], logrando resultados muy satisfactorios (Palmer *et al.,* 2022).

Aunque lejos todavía de ser considerado un caso de uso con valor comercial, se logró la optimización dinámica de una cartera para diferentes perfiles de riesgo, utilizando el algoritmo híbrido cuántico-clásico propuesto por Mugel, Abad, Bermejo, Sánchez, Lizaso y Orús (2021) en el dispositivo NISQ (D-Wave 2000Q). Si bien, debido a la limitación de los recursos cuánticos actuales en los NISQ, se precisó de una reducción dimensional del problema. Mugel, Abad, Bermejo, Sánchez, Lizaso y Orús (2021) opinan que, con arquitecturas cuánticas más avanzadas, como las sugeridas por Gyongyosi e Imre (2021), se podría acelerar la implementación de este tipo de algoritmos de computación cuántica para resolver problemas de la vida real.

También han sido sugeridos algoritmos de optimización de inspiración cuántica como el HRPQ[54] (Alipour, Adolphs, Zaribafiyan y Rounds, 2016), que goza de grandes ventajas: tiene en cuenta la correlación entre grupos de activos, por lo que minimiza la pérdida de información[55]; mejora el desempeño en la optimización de la cartera[56], y es independiente del *hardware*[57]. Entre sus desventajas, no incorpora restricciones ni dinámica.

---

52 En la práctica se han propuesto algoritmos heurísticos tanto de enfoque clásico como cuántico, estos últimos son adaptaciones al NISQ que se subdividen en: (a) basados en la técnica del templado cuántico (Adame y McMahon, 2020), como el algoritmo de optimización adiabática cuántica (Farhi, Goldstone, Gutmann y Sipser, 2000), y (b) modelos de circuitos cuánticos.

53 Concretamente, con el solucionador híbrido D-Wave Leap.

54 HRPQ es el acrónimo en inglés de *Quantum-inspired hierarchical risk parity.*

55 En particular, QHRP utiliza la correlación entre activos para construir una estructura jerárquica que está basada en la información contenida en la matriz de covarianzas, pero que no requiere su inversión. Al usar un árbol de agrupamiento, el algoritmo recursivamente actualiza los pesos de las asignaciones de los activos de la cartera hasta que se obtiene un portfolio bien diversificado.

56 Los resultados de la evaluación comparativa mostraron que QHRP supera a otros enfoques alternativos en una amplia variedad de medidas de riesgo.

57 Puede ser implementado tanto en un ordenador clásico como en un dispositivo cuántico *annealing* (QA).

Hasta el momento, no se han obtenido conclusiones concisas para determinar cuál es el mejor algoritmo y/o la plataforma de *hardware*[58] para la optimización dinámica de carteras, en su formulación discreta, con determinadas restricciones y realizado con datos reales (Mugel, Lizaso y Orús, 2022). En base a esto, se propone la futura investigación de un enfoque híbrido que combine el procesamiento cuántico y las redes de tensores.

9.4.3 Aprendizaje automático cuántico

En la actualidad no se conoce ninguna aplicación integral de aprendizaje automático cuántico (QML) que logre una aceleración exponencial respecto a su homónimo clásico, aunque sí se ha demostrado que el QML puede llegar a ofrecer un factor de aceleración teórico de más de un millón en comparación con los algoritmos clásicos y de inspiración cuántica (Kerenidis y Prakash, 2017), si bien este grado de aceleración varía significativamente en función de la tipología de problema.

El inconveniente técnico, una vez más, es que los algoritmos de QML, listos para ser usados, necesitan computadoras cuánticas a gran escala y disponer de una memoria cuántica de acceso aleatorio (QRAM), que es el análogo cuántico de la memoria clásica de acceso aleatorio (RAM), y *a priori* parece que estos requisitos serán difíciles de alcanzar en un futuro cercano. Recientemente, para solucionar esta limitación, se han desarrollado cargadores cuánticos (Kerenidis, 2020a) que sirven para codificar eficientemente datos clásicos en estados cuánticos y para realizar cálculos rápidos con ellos, acercando el QML a la era NISQ. En general, para que estos modelos muestren una clara ventaja en la práctica frente a los modelos clásicos se necesitan ciertas adaptaciones del código y una mayor potencia de *hardware* cuántico que permita núcleos cuánticos más profundos.

Por otra parte, descubrir las primeras aplicaciones cuánticas a problemas típicos de las finanzas es un desafío formidable que requiere el esfuerzo de expertos tanto en finanzas como en algorítmica cuántica, y que está en continuo progreso. Hasta el momento se han identificado posibles efectos positivos del empleo del QML[59] en tareas de la industria financiera que implican:

- La detección de anomalías que ayudarían a identificar el fraude en tarjetas de crédito y en transferencias instantáneas (Lloyd, Mohseni y Rebenstrot, 2013; Kerendis y Prakash, 2017); (Kerenidis, Landman, Luongo y Prakash, 2019; Kyriienko y Magnusson, 2022).

- La inversión en primas de riesgo de activos cruzados (Kerenidis, 2020b).

---

58 Los resultados, altamente dependientes de las figuras de mérito, fundamentalmente el ratio de Sharpe, el porcentaje de ganancias y el tiempo de cálculo, demostraron que D-Wave 2000Q es notablemente más rápido, mientras que las redes de tensor pueden proporcionar mejores carteras a cambio de un mayor tiempo de cálculo, siendo ambos capaces de tratar los sistemas más grandes con fines demostrativos.

59 Las distintas técnicas de aprendizaje automático se entremezclan y se combinan en los diferentes estudios; por este motivo y con el fin de centrar el foco en los posibles casos de uso, se ha prescindido de una descripción detallada de la técnica adoptada por cada uno de los autores.

— En problemas de regresiones lineales, como la fijación del precio de los activos y el cálculo de estrategias de seguimiento de tendencias de múltiples activos (Chakraborty, Gilyén y Jeffery, 2019; Kerenidis y Prakash, 2020).

— La estimación de la volatilidad en la operativa con divisas (Kerenidis, Prakash y Szilágyi, 2019).

— El análisis del riesgo de carteras de inversión (Kerenidis, Landman, Luongo y Prakash, 2019; Kerenidis, Landman y Prakash, 2020).

— La identificación de los regímenes de mercado como volatilidad alta/baja, tipos ascendentes/descendentes, inflación creciente/decreciente (Kerenidis Landman, Luongo y Prakash, 2019; Kerenidis, Landman y Prakash, 2020).

— La detección de billetes falsos; esta técnica se extiende a otros ámbitos de la economía que permiten clasificar en función de diferentes aspectos. Por ejemplo, diferentes países según su macro, clientes idóneos para las campañas de marketing, individuos en función de su nivel de riesgo para la concesión de un préstamo (Kerenidis y Prakash, 2017; Gilyén, Su, Hao Low y Wiebe, 2019; Kerenidis y Luongo, 2020).

— La fijación de precios de activos (Chen, Pelger y Zhu, 2019), riesgo hipotecario (Giesecke, Sirignano y Sadhwani, 2016) y libros de órdenes limitadas (Sirignano, 2019).

— El *trading* de mercado (Debérius, Granat y Karlsson, 2019), (Ganesh, Vadori, Xu, Zheng, Reddy, y Veloso, 2019), y (Karpe, Fang, Ma y Wang, 2020).

— La predicción de una crisis financiera en una red financiera compleja[60] (Ding *et al.,* 2023).

— La predicción de rebajas de la calificación crediticia, imprescindible para la gestión de riesgos (Lecrerc, *et al.* 2022).

9.5 El contexto de la encriptación actual y sus riesgos

En la era digital confluyen diferentes tipologías de encriptación para proteger la privacidad de la información, cuya complejidad se intensifica a medida que aumenta la sensibilidad de los datos.

60 Es un problema clasificado como NP-Hard por la teoría de la complejidad computacional (Hemenway y Khanna, 2016), esto significa que los algoritmos hasta ahora conocidos para abordar este tipo de problemas no garantizan que se pueda encontrar una solución óptima de forma eficiente en términos de tiempo. De hecho, dado el conocimiento global de una red financiera, se estima que el tiempo necesario para calcular las consecuencias de una perturbación superaría con creces la edad del universo.

El problema reside en que los algoritmos de encriptación clásica más ampliamente utilizados, como RSA, DH, AES y SHA, pueden ser descompuestos por la computación cuántica con relativa facilidad. Por ejemplo, el algoritmo cuántico de Shor (1994) podría descomponer el algoritmo RSA en cuestión de segundos. El único requisito necesario para que los algoritmos cuánticos puedan ejecutarse es un *hardware* cuántico lo suficientemente maduro y esto podría estar disponible en las próximas décadas.

La vulnerabilidad de la encriptación actual tiene un alcance amplísimo, afecta tanto a instituciones públicas como privadas de diversos sectores económicos. La industria financiera se encuentra particularmente expuesta a este riesgo, es un blanco muy atractivo para los ciberataques porque maneja información extremadamente sensible. Por ejemplo, un ataque exitoso comprometería, entre otros aspectos, a la seguridad de los sistemas de pagos y a la liquidación. Esto no solo pondría en peligro la integridad de las transacciones monetarias, sino que también afectaría a la confidencialidad de la información financiera de los usuarios.

La gravedad de las implicaciones fomenta la urgente necesidad de implementar medidas de encriptación resilientes, antes de que se convierta en una realidad tangible con la llegada de los primeros ordenadores cuánticos universales. Esto ha motivado que organismos como el BIS-IH (Innovation Hub del Banco de Pagos Internacionales) ya estén trabajando en proyectos para desarrollar una criptografía postcuántica, diseñada para resistir la potencia de procesamiento cuántico mejorada. El objetivo es probar y adaptar soluciones criptográficas en sistemas de pago, asegurando su funcionamiento óptimo frente a la llegada de la computación cuántica.

No obstante, existe también una oportunidad en la misma tecnología que representa la amenaza: la encriptación cuántica. Su implementación anticipada en los sistemas de seguridad financiera podría proporcionar una defensa inquebrantable contra los ataques a la encriptación actual. Si se adopta con prontitud, esta tecnología podría garantizar la integridad de los sistemas de pagos y de liquidación, fortaleciendo la seguridad de la información confidencial en el sector financiero.

9.5.1 Vulnerabilidad del algoritmo RSA frente a la computación cuántica

El RSA (Rivest, Shamir y Adleman, 1978) es uno de los algoritmos más populares de encriptación clásica, fue el primero de su tipo y su uso está muy extendido para cifrar y firmar digitalmente. La seguridad del algoritmo RSA se basa en que un ordenador clásico necesita una cantidad elevadísima para resolver la factorización de números primos (véase recuadro 7).

Hasta el momento, este enfoque solo puede ser vulnerado de manera ineficiente mediante ataques de fuerza bruta utilizando supercomputadoras clásicas. La fortaleza de la factorización de números primos (RSA, 1978) se basa en una conjetura matemática, es decir, no se ha probado que no se pueda romper, simplemente no se ha hallado la forma de hacerlo, pero podría descubrirse (véase recuadro 8).

Recuadro 7

LA FACTORIZACIÓN COMO BASE DE LA ENCRIPTACIÓN ACTUAL: EL ALGORITMO RSA

La factorización de un número compuesto consiste en encontrar los factores primos que, al multiplicarlos entre sí, dan como resultado el número original. A fecha de hoy no se conoce ningún algoritmo clásico capaz de resolver este problema matemático en un ordenador convencional de forma eficiente en términos de tiempo cuando se trata de números enteros de gran tamaño. En esta debilidad se basa la seguridad del sistema criptográfico de clave pública RSA desarrollado por el Instituto Técnico de Massachusetts (MIT).

Con el algoritmo RSA, los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos de gran tamaño elegidos al azar y mantenidos en secreto. Actualmente estos números primos son del orden de 10^{300}, y se prevé que su tamaño se incremente conforme aumente la capacidad de cálculo de los ordenadores clásicos. Aunque la capacidad de procesamiento de los ordenadores clásicos está supeditada a la reducción del tamaño de los microchips y esto físicamente tiene un límite, porque llegado a un umbral de tamaño dejan de funcionar correctamente, conllevando el estancamiento de la Ley de Moore (1965).

En concreto, se trata de meses, 1000 años y 1.000.000 años para un número compuesto de 512 bits, 768-bits y 1024 bits, respectivamente. Para el caso de la clave RSA de 2048 bits requiere millones de años para ser factorizada por un ordenador clásico, Kleinjung *et al.* (2010).

El problema de la factorización reside en que si el número es muy grande, la secuencia de operaciones «simples» crece rápidamente. Matemáticamente, el problema consiste en dividir N entre todos los primos desde 2 hasta $\sqrt{N}$, y esto equivale a 2d, donde d es el número de bits.

La seguridad del algoritmo de encriptación RSA se basa en el hecho de que son un conjunto de parámetros privados (en el ejemplo ilustrado: p, q, d, r), que no se comparten y que difícilmente pueden obtenerse mediante algoritmos clásicos. La dificultad de su obtención estriba en que deben derivarse de un número grande N.

Cuadro 1
Factorización del algortimo RSA

RSA-bits	Tiempo de resolución por ordenador clásico
512	Meses
768	1.000 años
1024	1.000.000 años

FUENTE: Encriptación de la información con el algoritmo RSA. Factorization of a 768-bit RSA-modulus, Kleinjung *et al.* (2010).

Esquema 1
Encriptación de la información con el algoritmo RSA

FUENTE: Elaboración propia.

Recuadro 8

VULNERABILIDADES DEL ALGORITMO RSA. EL ALGORITMO DE SHOR

El algoritmo clásico de encriptación RSA basa su seguridad en la dificultad que tienen los computadores clásicos para resolver el problema de la factorización de grandes números enteros. Aunque actualmente no exista una solución en computación clásica eficiente por el tiempo requerido, no significa que dicha solución no pueda ser encontrada en un futuro. No hay un teorema matemático que respalde esta asunción, por lo que es una mera conjetura[1]. Adicionalmente, la computación cuántica pone en jaque a la seguridad de la criptografía clásica basada en la factorización de números enteros grandes.

Concretamente, el algoritmo de factorización cuántico de Shor supera en velocidad a cualquier algoritmo de factorización clásico conocido. El algoritmo de Shor aprovecha el hecho de que el problema de la factorización se puede transformar en un problema que consiste en buscar el período de una función periódica, conocido como el problema del orden.

El algoritmo de Shor utiliza la superposición y la interferencia para aplicar la transformación cuántica de Fourier, que es una versión para equipos cuánticos de la transformada de Fourier discreta. Así, el algoritmo de Shor usa la transformación para encontrar el período de la función más rápidamente que cualquier algoritmo clásico conocido hasta la fecha.

1 En la ciencia existen otros ejemplos de hipótesis que años después han sido demostradas, como la conjetura de Poincaré (1904), que se convirtió en el teorema de Poincaré cuando posteriormente fue demostrada por Perelman en 2006.

Sin embargo, el algoritmo de factorización cuántico de Shor, utilizando la superposición y la interferencia, supera en velocidad a cualquier algoritmo de factorización clásico conocido hasta la fecha, y como resultado evidencia la vulnerabilidad de la encriptación actual y puede ser utilizado contra la criptografía asimétrica (véase recuadro 9).

A esto se suma el algoritmo cuántico de Grover (1996), que puede aplicarse contra criptografía simétrica (como AES, SHA), que tiene la capacidad de desencriptar la información de manera exponencialmente más rápida o al menos sustancialmente más efectiva.

9.5.2 Impacto futuro de la computación cuántica

Aunque no se puede predecir con certeza cuándo estará disponible un ordenador cuántico capaz de romper sistemas de encriptación convencionales (como RSA-2048) en un tiempo razonable, existe una encuesta anual realizada a los profesionales más relevantes del sector cuántico que arroja algo de luz sobre esta cuestión. Concretamente, según los resultados obtenidos por Mosca y Piani (2022), el 27,5 % de los profesionales cuánticos encuestados piensan que la probabilidad de que esto suceda en 15 años es altamente probable, igual o superior al 95 %. Si el horizonte temporal aumenta a 30 años, las cifras se duplican, el 55 % de los expertos consideran que sería altamente probable.

Sin embargo, mientras transcurre este lapso de tiempo, cada día sin una solución representa un incremento en la exposición al riesgo. Esta situación se debe a que en la actualidad resulta relativamente económico almacenar grandes cantidades de información sensible que permanecerá comprometida durante años o incluso durante décadas, hasta que el ordenador cuántico universal esté disponible y pueda ser descifrada. Este fenómeno se conoce como

Recuadro 9

EL ALGORITMO DE SHOR SE COMPONE DE TRES PARTES

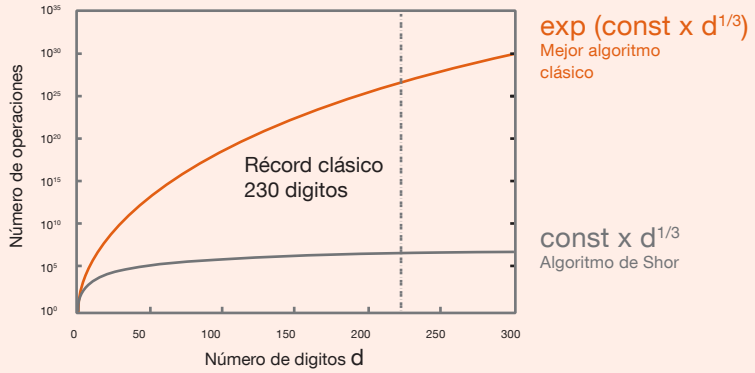
La primera parte es ejecutable en computación clásica, consiste en transformar la factorización de N en la búsqueda de un período r de una función periódica. Dados dos números coprimos, sin divisores en común, a y N, tal que, $1 < a < N$ consiste en encontrar el orden r de a mod N que sigue la expresión $a^r \bmod N = 1$, equivalente a $\frac{a^r}{N}$ con resto igual a 1.

La segunda parte, ejecutable en computación cuántica, consiste en encontrar el período r mediante la transformada cuántica de Fourier.

La tercera y última parte se ejecuta en un ordenador clásico. Consiste en deducir los factores de N del período r utilizando técnicas de teoría de números. En concreto, los factores primos serán el máximo común divisor de $a^{\frac{r}{2}} \pm 1$ y N. El algoritmo de Shor itera hasta encontrar los factores primos.

Aunque existen otros algoritmos clásicos muy sofisticados que implican herramientas avanzadas de teoría de números. El algoritmo clásico más conocido y más eficiente para la factorización de números enteros mayores de 100 dígitos es el de criba general del cuerpo de números. El récord del mejor algoritmo clásico de encriptación está en 230 dígitos (Patil y Vijayalakshmi, 2021) (véase gráfico 1). Para conseguir encriptar un determinado número de dígitos, el número de operaciones que se necesitan por el mejor algoritmo clásico sigue la fórmula $\exp(\text{constant} \times d^{\frac{1}{3}})$, mientras que el algoritmo de Shor necesitaría $\text{constant} \times d^3$ operaciones. Por este motivo, el algoritmo de Shor es exponencialmente más rápido que el mejor de los algoritmos clásicos de factorización (véase gráfico 1).

Gráfico 1
Mejor algoritmo clásico *vs* Shor. Número de operaciones por dígito desencriptado



Exponencialmente más rápido que el algoritmo clásico más conocido.

FUENTE: Fundamental Machine Learning Routines as Quantum Algorithms on a Superconducting Quantum Computer (Sangskriti, Nag y Haque, 2021).

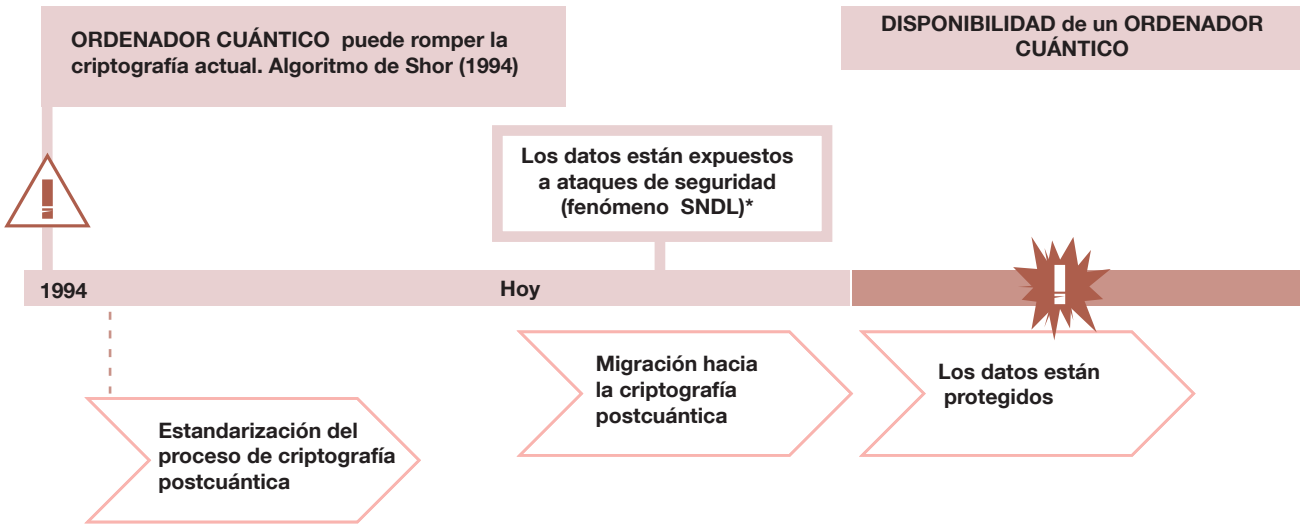
SNDL[61] (Store Now, Decrypt Later) o «Guarda Ahora, Descifra Después» (véase esquema 6), que implica almacenar los datos actualmente para recuperarlos en el futuro, identificando aquellos que aún posean valor y sometiéndolos al procesamiento cuántico para descifrar su contenido.

9.5.3 Acciones y preparación ante la vulnerabilidad

La ciberseguridad de las instituciones financieras y de otros sectores se basa en gran parte en tomar medidas proactivas para proteger los datos a largo plazo. Con este objeto, organizaciones como el BIS-IH, el Foro Económico Mundial (WEF), el Instituto Nacional de

61 El fenómeno SNDL también es denominado HNDL, del inglés *Harvest Now, Decrypt Later.*

Esquema 6
Fenómeno SNDL



FUENTE: Elaboración propia, inspirado en PROYECTO LEAP de BIS-IH.

Estándares y Tecnología (NIST), la Agencia de Seguridad Nacional (NSA), la Agencia de Seguridad de Infraestructuras y CiberSeguridad (CISA) y el Gobierno de los Estados Unidos, han comenzado a tomar medidas proactivas para abordar esta creciente vulnerabilidad.

Para proteger la información de un futuro ataque hay dos soluciones posibles: la encriptación postcuántica y la propia encriptación cuántica, que es, por definición, inquebrantable.

CISA, NSA y NIST instan a las instituciones a ir organizando, con un enfoque integral, el cambio hacia una criptografía postcuántica para protegerse ante el avance de las futuras capacidades de la computación cuántica, que podrían tener efectos adversos comprometiendo los sistemas de clave pública actuales. En el documento que publicaron conjuntamente en agosto de 2023 (CISA, 2023), se establece una estrategia reflexiva en la que, mediante un inventario de criptografía, se permita identificar los sistemas con mayor vulnerabilidad y, de esta forma, priorizar en colaboración con los proveedores la migración hacia una criptografía segura según el riesgo.

9.5.4 Soluciones, propuestas y desafíos

La necesidad imperiosa de desarrollar algoritmos resistentes a los avances de la computación cuántica surge como un requisito fundamental para salvaguardar la información sensible. Se estudian dos soluciones: la criptografía postcuántica y cuántica.

La encriptación postcuántica se orienta a encontrar algoritmos capaces de resistir los ataques cuánticos. Sin embargo, la selección de estos algoritmos representa un desafío significativo que requiere un enfoque cauteloso y una comprensión profunda de sus implicaciones. Una elección errónea podría exponer sistemas críticos a vulnerabilidades, mientras que la migración de sistemas de encriptación se convierte en un proceso costoso que demanda una coordinación meticulosa para evitar cualquier brecha de seguridad que pudiera ser explotada. NIST está trabajando para publicar los primeros protocolos de critptografía postcuántica, que serán publicados en 2024.

En contraste, la encriptación cuántica se presenta como una solución inherentemente sólida debido a las propiedades únicas de la mecánica cuántica, como la medida cuántica y el teorema de no clonación. La implementación de esta tecnología en la seguridad bancaria, por ejemplo, ofrecería una defensa robusta contra los ataques de la computación cuántica. Esto implica que, desde el inicio, los datos estarían protegidos de manera incuestionable, evitando la necesidad de migraciones costosas.

Actualmente, varios proyectos internacionales están inmersos en la búsqueda de algoritmos postcuánticos. Este proceso es complejo y demanda tiempo, pues implica anticiparse a amenazas que aún no se han materializado por completo. Para las instituciones financieras y otros sectores, la ciberseguridad depende en gran medida de tomar medidas proactivas para proteger los datos a largo plazo. Esto abarca desde identificar la vulnerabilidad de los algoritmos de encriptación utilizados hasta priorizar su actualización, así como anticipar la implementación de tecnologías cuánticas en los sistemas de seguridad.

En resumen, la amenaza que representa la computación cuántica para la encriptación actual es una realidad inminente que requiere una respuesta inmediata. Tanto la encriptación postcuántica como la encriptación cuántica emergen como soluciones clave para proteger la información sensible en el mundo digital. La elección cuidadosa de algoritmos postcuánticos y la implementación temprana de tecnologías cuánticas pueden brindar una protección sólida desde el principio. La seguridad cibernética sigue siendo un desafío en constante cambio, y la preparación se revela como un elemento esencial para salvaguardar la integridad de los datos en un futuro incierto y dinámico.

Bibliografía

Adame, Juan Ignacio, y Peter McMahon. (2020). "Inhomogeneous driving in quantum annealers can result in orders-of-magnitude improvements in performance". *Quantum Science and Technology.* https://doi.org/10.1088/2058-9565/ab935a

Alipour, Elham, Clemens Adolphs, Arman Zaribafiyan y Maxwell Rounds. (2016). "Quantum-inspired hierarchical risk parity". *White paper,* 1Qbit. https://1qbit.com/files/white-papers/1QBit-White-Paper-%E2%80%93-Quantum-Inspired-Hierarchical-Risk-Parity.pdf

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

Benioff, Paul. (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), pp. 563-591. https://doi.org/10.1007/BF01011339

Benioff, Paul. (1982a) "Quantum mechanical models of Turing machines that dissipate no energy". *Physical Review Letters,* 48, no. 23, p. 1581. https://doi.org/10.1103/PhysRevLett.48.1581

Benioff, Paul. (1982b). "Quantum mechanical Hamiltonian models of Turing machines". *Journal of Statistical Physics,* 29, no. 3, pp. 515-546. https://doi.org/10.1007/BF01342185

Bennett, Charles H., y Gilles Brassard. (2020). *Quantum cryptography: Public key distribution and coin tossing.* https://doi.org/10.48550/arXiv.2003.06557

Bharti, Kishor, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S. Kottmann, Tim Menke, Wai-Keong Mok, Sukin Sim, Leong-Chuan Kwek y Alán Aspuru-Guzik. (2022). "Noisy intermediate-scale quantum algorithms". *Reviews of Modern Physics,* 94, no. 1, p. 015004. https://doi.org/10.1103/RevModPhys.94.015004

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

Black, Fischer, y Myron Scholes. (1973). "The Pricing of Options and Corporate Liabilities". *Journal of Political Economy,* 81 (3), pp. 637-654. doi:10.1086/260062. http://dx.doi.org/10.1086/260062

Bluvstein, Dolev, Harry Levine, Giulia Semeghini, Tout T. Wang, Sepehr Ebadi, Marcin Kalinowski, Alexander Keesling, Nishad Maskara, Hannes Pichler, Markus Greiner, Vladan Vuletic y Mikhail D. Lukin. (2022). "A quantum processor based on coherent transport of entangled atom arrays". *Nature,* 604, no. 7906, pp. 451-456. https://doi.org/10.1038/s41586-022-04592-6

Boixo, Sergio, Sergei V. Isakov, Vadim N. Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J. Bremner, John M. Martinis y Hartmut Neven. (2018). "Characterizing Quantum Supremacy in Near-Term Devices". *Nature Physics,* 14, pp. 595-600. https://doi.org/10.1038/s41567-018-0124-x

Bouland, Adam, Wim van Dam, Hamed Joorati, Iordanis Kerenidis y Anupam Prakash. (2020). *Prospects and challenges of quantum finance.* https://doi.org/10.48550/arXiv.2011.06492

Bouwmeester, Dik, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter y Anton Zeilinger. (1997). "Experimental quantum teleportation". *Nature,* 390, no. 6660, pp. 575-579. https://doi.org/10.1038/37539

Brassard, Gilles, Peter Hoyer, Michele Mosca y Alain Tapp. (2000). "Quantum amplitude amplification and estimation". *Contemporary Mathematics,* 305, pp. 53-74. https://doi.org/10.1090/conm/305/05215

Bravyi, Sergey, Oliver Dial, Jay M. Gambetta, Darío Gil y Zaira Nazario. (2022). "The future of quantum computing with superconducting qubits". *Journal of Applied Physics,* 132, no. 16, pp. 160902. https://doi.org/10.48550/arXiv.2209.06841

Chakrabarti, Shouvanik, Rajiv Krishnakumar, Guglielmo Mazzola, Nikitas Stamatopoulos, Stefan Woerner y William J. Zeng. (2021). *A Threshold for Quantum Advantage in Derivative Pricing.* https://doi.org/10.22331/q-2021-06-01-463

Chakraborty, Shantanav, András Gilyén y Stacey Jeffery. (2019). "The power of block-encoded matrix powers: improved regression techniques via faster Hamiltonian simulation". *Proceedings of 46th International Colloquium on Automata, Languages and Programming (ICALP).* https://doi.org/10.4230/LIPIcs.ICALP.2019.33

Chen, Luyang, Markus Pelger y Jason Zhu. (2019). *Deep learning in asset pricing.* https://dx.doi.org/10.2139/ssrn.3350138

Chi, Yulin, Jieshan Huang, Zhanchuan Zhang, Jun Mao, Zinan Zhou, Xiaojiong Chen, Chonghao Zhai, Jueming Bao, Tianxiang Dai, Huihong Yuan, Ming Zhang, Daoxin Dai, Bo Tang, Yan Yang, Zhihua Li, Yunhong Ding, Leif K. Oxenløwe, Mark G. Thompson, Jeremy L. O'Brien, … Jianwei Wang. (2022). "A programmable qudit-based quantum processor". *Nature Communication,* 13(1), p. 1166. https://doi.org/10.1038/s41467-022-28767-x

Choudhary, Dhruv, Arun Kejariwal y Francois Orsini. (2017). "On the runtime-efficacy trade-off of anomaly detection techniques for real-time streaming data". https://doi.org/10.48550/arXiv.1710.04735

Chow, Jerry, y Jay Gambetta. (2020). "Quantum takes flight: Moving from laboratory demonstrations to building systems". *IBM Research Blog.* https://www.ibm.com/blogs/research/2020/01/quantum-volume-32/

Cibersecurity and Infraestructure Security Agency, National Security Agency, and National Institute of Standards and Technology. (2023). *Quantum-Readiness: Migration to Post-quantum Cryptography.* https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

Comisión Europea. (2023). *Configurar el futuro digital de Europa. Comisión Europea.* https://digital-strategy.ec.europa.eu/es/policies/quantum-technologies-flagship

Coppersmith, Don. (2002). *An approximate Fourier transform useful in quantum factoring.* https://doi.org/10.48550/arXiv.quant-ph/0201067

Debérius, Kevin, Elvin Granat y Patrik Karlsson. (2019). "Deep execution-value and policy based reinforcement learning for trading and beating market benchmarks". *Social Science Research Network.* https://doi.org/10.2139/ssrn.3374766

Deutsch, David. (1985). "Quantum theory, the Church-Turing principle and the universal quantum computer". *Proceedings of the Royal Society A. Mathematical and Physical Sciences,* 400, no. 1818, pp. 97-117. https://doi.org/10.1098/rspa.1985.0070

Ding, Yongcheng, Javier González-Conde, Lucas Lamata, José D. Martín-Guerrero, Enrique Lizaso, Samuel Mugel, Xi Chen, Román Orús, Enrique Solano y Mikel Sanz. (2023). "Toward prediction of financial crashes with a d-wave quantum annealer". *Entropy,* 25, no. 2, p. 323. https://doi.org/10.3390/e25020323

DiVincenzo, David P. (2000). "The physical implementation of quantum computation". *Fortschritte der Physik: Progress of Physics,* 48.9-11, pp. 771-783. https://doi.org/10.1002/1521-3978(200009)48:9/11%3C771::AID-PROP771%3E3.0.CO;2-E

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

Ekert, Artur K. (1991). "Quantum cryptography based on Bell's theorem". *American Physical Society,* vol. 67, no. 6, pp. 661-663, https://doi.org/10.1103/PhysRevLett.67.661

"El Presidente Biden firma la Ley Quantum de Preparación para la Ciberseguridad". (2022). *Ciberseguridad Latam.* https://www.ciberseguridadlatam.com/2022/12/24/el-presidente-biden-firma-la-ley-quantum-de-preparacion-para-la-ciberseguridad/

Farhi, Edward, Jeffrey Goldstone, Sam Gutmann y Michael Sipser. (2020). "Quantum computation by adiabatic evolution". https://doi.org/10.48550/arXiv.quant-ph/0001106

Federal Reserve. (2023). *Cybersecurity and Financial System Resilience Report.* https://www.federalreserve.gov/publications/cybersecurity-and-financial-system-resilience-report.htm

Fernández-Caramés, Tiago M. (2020). "From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things". *IEEE Internet of Things Journal,* vol. 7, no. 7, pp. 6457-6480. https://doi.org/10.1109/JIOT.2019.2958788

Feynman, Richard P. (1982). "Simulating physics with computers". *International Journal of Theoretical Physics.* https://doi.org/10.1007/BF02650179

Feynman, Richard P. (2005). "The principle of least action in quantum mechanics. In Feynman's Thesis-A New Approach to Quantum Theory". *World Scientific,* pp. 1-79. https://doi.org/10.1142/9789812567635_0001

Friis, Nicolai, Oliver Marty, Christine Maier, Cornelius Hempel, Milan Holzäpfel, Petar Jurcevic, Martin B. Plenio, Marcus Huber, Christian Roos, RainerBlatt y Ben Lanyon. (2018). "Observation of entangled states of a fully controlled 20-qubit system". *Physical Review,* X 8, no. 2, p. 021012. https://doi.org/10.1103/PhysRevX.8.021012

Ganesh, Sumitra, Nelson Vadori, Mengda Xu, Hua Zheng, Prashant Reddy y Manuela Veloso. (2019). *Reinforcement learning or market making in a multi-agent dealer market.* https://doi.org/10.48550/arXiv.1911.05892

Giesecke, Kay, J. Sirignano y A. Sadhwani. (2016). "Deep learning for mortgage risk". Technical report, Working paper, Stanford University. https://doi.org/10.48550/arXiv.1601.01987

Gilyén, András, Yuan Su, Guang Hao Low y Nathan Wiebe. (2019). "Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics". *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing,* pp. 193-204. ACM. https://doi.org/10.1145/3313276.3316366

Gómez, Andrés, Álvaro Leitao, Alberto Manzano, Daniele Musso, María R. Nogueiras, Gustavo Ordóñez y Carlos Vázquez. (2022). "A Survey on Quantum Computational Finance for Derivatives Pricing and VaR". *Archives of Computational Methods in Engineering,* pp. 1-27. https://doi.org/10.1007/s11831-022-09732-9

Gordon, Myron J., y Eli Shapiro. (1956). *Capital Equipment Analysis: The Required Rate of Profit.* https://www.jstor.org/stable/2627177

Grinko, Dimitry, Julien Gacon, Christa Zoufall y Stefan Woerner. (2021). "Iterative quantum amplitude estimation". *Npj Quantum Information,* 7, p. 52. https://doi.org/10.1038/s41534-021-00379-1

Grover, Lov K. (1996). "A fast quantum mechanical algorithm for database search". *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing,* pp. 212-219. https://doi.org/10.48550/arXiv.quant-ph/9605043

Guo, Mingchao, Hailing Liu, Yongmei Li, Wenmin Li, Fei Gao, Sujuan Qin y Qiaoyan Wen. (2022). "Quantum algorithms for anomaly detection using amplitude estimation". *Physica A: Statistical Mechanics and its Applications,* 604, p. 127936. https://doi.org/10.1016/j.physa.2022.127936

Gyongyosi, Laszlo, y Sandor Imre. (2021). *Scalable distributed gate-model quantum computers.* https://doi.org/10.1038/s41598-020-76728-5

Hauke, Philipp, Helmut G. Katzgraber, Wolfgang Lechner, Hidetoshi Nishimori y William D. Oliver (2020) "Perspectives of quantum annealing: Methods and implementations". *Reports on Progress in Physics,* 83, no. 5. p. 054401. https://doi.org/10.48550/arXiv.1903.06559

Heinrich, Stefan. (2002). "Quantum Summationwith an application to integration". *Journal of Complexity,* 18(1), pp. 1-50. https://doi.org/10.48550/arXiv.quant-ph/0105116

Hemenway, Brett, y Sanjeev Khanna. (2016). "Sensitivity and computational complexity in financial networks". *Algorithmic Finance,* 5, no. 3-4, pp. 95-110. https://doi.org/10.48550/arXiv.1503.07676

Henriet, Loïc, Lucas Beguin, Adrien Signoles, Thierry Lahaye, Antoine Browaeys, Georges-Olivier Reymond y Christophe Jurczak. (2020). "Quantum computing with neutral atoms", *Quantum,* 4, p. 327. https://doi.org/10.22331/q-2020-09-21-327

Herman, Dylan, Cody Googin, Xiaoyuan Liu, Alexey Galda, Ilya Safro, Yue Sun, Marco Pistoia y Yuri Alexeev . (2022). *A survey of quantum computing for finance.* https://doi.org/10.48550/arXiv.2201.02773

Hermans, S .L. N., M. Pompili, H. K. C. Beukers, S. Baier, J. Borregaard y R. Hanson. (2022). "Qubit teleportation between non-neighbouring nodes in a quantum network". *Nature,* 605, pp. 663-668. https://doi.org/10.1038/s41586-022-04697-y

Howard, Ronald A. (1971). "Semi-Markov and Decision Processes", *Dynamic Probabilistic Systems,* vol. 2, pp. 87-91. https://doi.org/10.48550/arXiv.2007.00017

Huang, Hsin-Yuan, Michael Broughton, Masoud Mohseni, Ryan Babbush, Sergio Boixo, Hartmut Neven y Jarrod R. McClean. (2021). "Power of data in quantum machine learning". *Nature communications,* 12, no. 1, pp. 1-9. https://doi.org/10.1038/s41467-021-22539-9

Jäger, Jonas, y Roman V. Krems. (2023) "Universal expressiveness of variational quantum classifiers and quantum kernels for support vector machines". *Nature Communications,* 14.1, p. 576. https://doi.org/10.1038/s41467-023-36144-5

Jordan, S. (2022). *Quantum Algorithm Zoo.* [DATASET]. https://quantumalgorithmzoo.org

Kac, Mark. (1949). "On distributions of certain Wiener functionals". *Transactions of the American Mathematical Society,* 65(1), pp. 1-13. https://doi.org/10.1090/S0002-9947-1949-0027960-X

Kalai, Gil. (2016). "The quantum computer puzzle". *Notices of the AMS,* 63, no. 5, pp. 508-516. https://doi.org/10.1090/noti1380

Karpe, Michaël, Jin Fang, Zhongyao Ma y Chen Wang. (2020). *Multi-agent reinforcement learning in a realistic limit order book market simulation.* https://doi.org/10.48550/arXiv.2006.05574

Kerenidis, Iordanis. (2020a). *A method for loading classical data into quantum states for applications in machine learning and optimizations.* U.S. Patent Application No. 16/986,553. U.S. Patent and Trademark Office.

Kerenidis, Iordanis. (2020b). *A method for loading classical data into quantum states for applications in machine learning and optimizations.* U.S. Patent Application No. 16/987,235. U.S. Patent and Trademark Office.

Kerenidis, Iordanis, Jonas Landman, Alessandro Luongo, y Anupam Prakash. (2019). *Q-means: A quantum algorithm for unsupervised machine learning.* https://doi.org/10.48550/arXiv.1812.03584

Kerenidis, Iordanis, Jonas Landman, y Anupam Prakash. (2020). "Quantum algorithms for deep convolutional neural networks". *Proceedings of International Conference on Learning Representations (ICLR).* https://doi.org/10.48550/arXiv.2111.03598

Kerenidis, Iordanis, y Alessandro Luongo. (2020). "Classification of the MNIST data set with quantum slow feature analysis". *Physical Review A,* 101(6), p. 062327. https://doi.org/10.1103/PhysRevA.101.062327

Kerenidis, Iordanis, y Anupam Prakash. (2020). *A method for amplitude estimation with noisy intermediate-scale quantum computers.* U.S. Patent Application No. 16/892,229, 2020. U.S. Patent and Trademark Office.

Kerenidis, Iordanis, y Anupam Prakash. (2017). “Quantum recommendation systems”. *Proceedings of the 8th Innovations in Theoretical Computer Science Conference.* https://doi.org/10.48550/arXiv.1603.08675

Kerenidis, Iordanis, y Anupam Prakash. (2020). “Quantum gradient descent for linear systems and least squares”. *Physical Review A,* 101(2), p. 022316. https://doi.org/10.1103/PhysRevA.101.022316

Kerenidis, Iordanis, Anupam Prakash, y Dániel Szilágyi. (2019). *Quantum Algorithms for Portfolio Optimization.* https://doi.org/10.48550/arXiv.1908.08040

Kiczynski, M., S. K. Gorman, H. Geng, M. B. Donnelly, Y. Chung, Y. He, J. G. Keizer, y M. Y. Simmons. (2022). “Engineering topological states in atom-based semiconductor quantum dots”. *Nature,* 606, pp. 694-699. https://doi.org/10.1038/s41586-022-04706-0

Kleinjung, Thorsten, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thomé, Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev & Paul Zimmermann. (2010). “Factorization of a 768-bit RSA modulus”. *Annual Cryptology Conference,* pp. 333-350. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14623-7_18

Kyriienko, Oleksandr, y Einar B. Magnusson. (2022). *Unsupervised quantum machine learning for fraud detection.* https://doi.org/10.48550/arXiv.2208.01203

Lechner, Wolfgang, Philipp Hauke, y Peter Zoller. (2015). “A quantum annealing architecture with all-to-all connectivity from local interactions”. *Science Advances,* vol. 1, no. 9. https://doi.org/10.1126/sciadv.1500838

Leclerc, Lucas, Luis Ortiz-Guitiérrez, Sebastián Grijalva, Boris Albrecht, Julia R. K. Cline, Vincent E. Elfving, Adrien Signoles, Loïc Henriet, Gianni del Bimbo, Usman Ayub Sheikh, Maitree Shah, Luc Andrea, Faysal Ishtiaq, Andoni Duarte, Samuel Mugel, Irene Cáceres, Michel Kurek, Román Orús, Achraf Seddik, … Didier M’tamon. (2022). *Financial Risk Management on a Neutral Atom Quantum Processor.* https://doi.org/10.48550/arXiv.2212.03223

Lin, Wei-Yang, Ya-Han Hu y Chih-Fong Tsai. (2011). “Machine learning in financial crisis prediction: a survey”. *IEEE Transactions on Systems,* Man, and Cybernetics, Part C, Applications and Reviews, 42, no. 4, pp. 421-436. http://dx.doi.org/10.1109/TSMCC.2011.2170420

Lloyd, Seth, Masoud Mohseni y Patrick Rebentrost. (2013). *Quantum algorithms for supervised and unsupervised machine learning.* https://doi.org/10.48550/arXiv.1307.0411

Longstaff Francis A., y Eduardo Schwartz. (2015). “Valuing american options by simulation: A simple least-squares approach”. *Review of Financial Studies,* vol. 14, pp. 113-147. https://doi.org/10.1093/rfs/14.1.113

Markowitz, Harry. (1952). *Portfolio selection.* https://doi.org/10.2307/2975974

Masiowski, Mateusz, Niko Mohr, Henning Soller y Matija Zesco. (2022). “Quantum computing funding remains strong, but talent gap raises concern”. *McKinsey Digital.* https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern

Merali, Zeeya. (2011). “First sale for quantum computing”, *Nature,* 474, 18. https://doi.org/10.1038/474018a

Mohseni, Masoud, Peter Read, Hartmut Neven, Sergio Boixo, Vasil Denchev, Ryan Babbush, Austin Fowler, Vadim Smelyanskiy y John Martinis. (2017). “Commercialize quantum technologies in five years”. *Nature,* 543, no. 7644, pp. 171-174. https://doi.org/10.1038/543171a

Montanaro, Ashley. (2015). “Quantum speedup of Monte Carlo methods”. *Proceedings of Royal Society A. Mathematical, Physical and Engineering Sciencies.* https://doi.org/10.1098/rspa.2015.0301

Mosca, Michele. (2018). “Cybersecurity in an era with quantum computers: will we be ready?”. *IEEE Security & Privacy,* 16, no. 5, pp. 38-41. https://doi.org/10.1109/MSP.2018.3761723

Mosca, Michele, y Marco Piani. (2021). *Quantum threat timeline report 2020.* Global Risk Insitute. https://globalriskinstitute. org/publications/quantum-threat-timeline-report-2020

Mosca, Michele, y Marco Piani. (2022). *Quantum threat timeline report 2022.* https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

Mugel, Samuel, Mario Abad, Miguel Bermejo, Javier Sánchez, Enrique Lizaso y Román Orús. (2021). “Hybrid quantum investment optimization with minimal holding period”. *Scientific Reports,* 11, no. 1, p. 19587. https://doi.org/10.1007/978-3-030-97273-8_15

Mugel, Samuel, Alessio Celi, Pietro Massignan, János K. Asbóth, Maciej Lewenstein y Carlos Lobo. (2016). “Topological bound states of a quantum walk with cold atoms”. *Physical Review A,* 94, no. 2, p. 023631. https://doi.org/10.1103/PhysRevA.94.023631

Mugel, Samuel, Carlos Kuchkovsky, Escolástico Sánchez, Samuel Fernández-Lorenzo, Jorge Luis-Hita, Enrique Lizaso y Román Orús. (2020). “Dynamic portfolio optimization with real datasets using quantum processors and quantum-inspired tensor networks”. *Physical Review Research* 4, no. 1, p. 013006. https://doi.org/10.1103/PhysRevResearch.4.013006

Mugel, Samuel, Enrique Lizaso y Román Orús. (2022). “Use cases of quantum optimization for finance”. *Credible Asset Allocation, Optimal Transport Methods, and Related Topics,* pp. 211-220. Springer International Publishing. https://doi.org/10.1007/978-3-030-97273-8_15

National Security Agency. (2022). *Announcing the Commercial National Security Algorithm Suite 2.0.* Cybersecurity Advisory. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

Needham, Mass. (2023). *IDC Forecasts Worldwide Quantum Computing Market to Grow to $7.6 Billion in 2027*. International Data Corporation Media Center. https://www.idc.com/getdoc.jsp?containerId=prUS51160823

Nielsen, Michael A., e Isaac L. Chuang. (2000). "Quantum information and quantum computation". *Cambridge University Press* 2, no. 8, p. 23. https://doi.org/10.1017/CBO9780511976667

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

Orús, Román, Samuel Mugel y Enrique Lizaso. (2019b). "Forecasting financial crashes with quantum computing". *Physical Review A,* 99, no. 6, p. 060301. https://doi.org/10.1103/PhysRevA.99.060301

Ozfidan, I., C. Deng, A. Y. Smirnov, T. Lanting, R. Harris, L. Swenson, J. Whittaker, F. Altomare, M. Babcock, C. Baron, A. J. Berkley, K. Boothby, H. Christiani, P. Bunyk, C. Enderud, B. Evert, M. Hager, A. Hajda, J. Hilton, … M. H. Amin. (2020). "Demonstration of a Nonstoquastic Hamiltonian in Coupled Superconducting Flux Qubits". *Phys. Rev. Applied,* 13, 034037. https://doi.org/10.1103/PhysRevApplied.13.034037

Palmer, Samuel, Konstantinos Karagiannis, Adam Florence, Asier Rodríguez, Román Orús, Harish Naik y Samuel Mugel. (2022). *Financial Index Tracking via Quantum Computing with Cardinality Constraints.* https://doi.org/10.48550/arXiv.2208.11380

Palmer, Samuel, Serkan Sahin, Rodrigo Hernández, Samuel Mugel y Román Orús. (2021). *Quantum portfolio optimization with investment bands and target volatility.* https://doi.org/10.48550/arXiv.2106.06735

Patel, Raj G., Chia-Wei Hsing, Serkan Sahin, Samuel Palmer, Saeed S. Jahromi, Shivam Sharma, Tomás Domínguez, Kris Tziritas, Christophe Michel, Vincent Porte, Mustafa Abid, Stephane Aubert, Pierre Castellani, Samuel Mugel y Román Orús. (2022). *Quantum-Inspired Tensor Neural Networks for Option Pricing.* https://doi.org/10.48550/arXiv.2212.14076

Patil, S. S., y Vijayalakshmi, D. S. (2021). *Quantum Computing-An Introduction and Cloud Quantum Computing.* http://www.jetir.org/papers/JETIR2105402.pdf

Peruzzo A, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik y Jeremy L. O'Brien. (2014). "A variational eigenvalue solver on a photonic quantum processor". *Nature Communications.* https://doi.org/10.1038/ncomms5213

Pfitzinger, Johann, y Nico Katzke. (2019). *A constrained hierarchical risk parity algorithm with cluster-based capital allocation.* Stellenbosch University, Department of Economics. Handle: RePEc:sza:wpaper:wpapers328

Poincaré, M. H. (1904). "Cinquième complément à l'analysis situs". *Rendiconti del Circolo Matematico di Palermo* (1884-1940), 18, no. 1, pp. 45-110. https://doi.org/10.1007/BF03014091

Popov, Aleksey, Evgeny Kiktenko, Aleksey Fedorov y Vladimir I. Man'ko. (2016). "Information processing using three-qubit and qubit-qutrit encodings of noncomposite quantum systems". *Journal of Russian Laser Research,* 37, no. 6, pp. 581-590. https://doi.org/10.1007/s10946-016-9610-8

Preskill, John. (2012). *Quantum computing and the entanglement frontier.* https://doi.org/10.48550/arXiv.1203.5813

Preskill, John. (2018). "Quantum computing in the NISQ era and beyond". *Quantum,* 2, p. 79. https://doi.org/10.22331/q-2018-08-06-79

Rattew, Arthur G., y Bálint Koczor. (2022). *Preparing Arbitrary Continuous Functions in Quantum Registers With Logarithmic Complexity.* https://doi.org/10.48550/arXiv.2205.00519

Rattew, Arthur G., y Patrick Rebentrost. (2023). *Non-Linear Transformations of Quantum Amplitudes: Exponential Improvement, Generalization, and Applications.* https://doi.org/10.48550/arXiv.2309.09839

Research and Markets. (2022). *Report on Quantum Computing Applications in the Financial Services Industry: End-User Cases and Market Forecasts.* https://www.researchandmarkets.com/reports/4600701/quantum-computing-technologies-and-global#rela0-5521656

Riebe, Mark, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James y R. Blatt. (2004). "Deterministic quantum teleportation with atoms". *Nature,* 429, no. 6993, pp. 734-737. https://doi.org/10.1038/nature02570

Rivest, Ronald L., Adi Shamir y Leonard Adleman. (1978). "A method for obtaining digital signatures and public-key cryptosystems". *Communications of the ACM,* 21, no. 2, pp. 120-126. https://doi.org/10.1145/359340.359342

Sangskriti, Sristy, Protik Nag y Summit Haque. (2021). *Fundamental Machine Learning Routines as Quantum Algorithms on a Superconducting Quantum Computer.* https://doi.org/10.48550/arXiv.2109.09522

Sanz-Fernández, Cristina, Rodrigo Hernández, Christian D. Marciniak, Ivan Pogorelov, Thomas Monz, Francesco Benfenati, Samuel Mugel y Román Orús. (2021). *Quantum portfolio value forecasting.* https://doi.org/10.48550/arXiv.2111.14970

Schrödinger, Erwin. (1935). "Die gegenwärtige Situation in der Quantenmechanik". *Naturwissenschaften,* 23, no. 50, pp. 844-849. https://doi.org/10.1007/BF01491891

Sevilla, Jaime, y C. Jess Riedel. (2020). *Forecasting timelines of quantum computing.* https://doi.org/10.48550/arXiv.2009.05045

Shor, Peter W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". *Proceedings 35th annual symposium on foundations of computer science,* pp. 124-134. Ieee. https://doi.org/10.1109/SFCS.1994.365700

Sirignano, Justin A. (2019). "Deep learning for limit order books". *Quantitative Finance,* 19(4), pp. 549-570. https://doi.org/10.48550/arXiv.1601.01987

Sorensen, Bob. (2021). *Broad Interest in Quantum Computing as a driver of Commercial Success.* Hyperion Research. https://www.dwavesys.com/media/an1helvq/hyperion_report_v2.pdf

Turing, Alan Mathison. (1938). "On computable numbers, with an application to the Entscheidungs problem. A correction". *Proceedings of the London Mathematical Society,* 2, no. 1, pp. 544-546. https://doi.org/10.2307/2268808

White House. (2022). *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.* https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Woerner, Stefan, y Daniel J. Egger. (2019). "Quantum risk analysis". *Quantum Information,* 5(1), pp. 1-8. https://doi.org/10.1109/TQE.2021.3063635

Wootters, W. K., y W. H. Zurek. (1982). "A single quantum cannot be cloned". *Nature.* 299, pp. 802-803. https://doi.org/10.1038/299802a0

World Economic Forum. (2022). *Quantum Computing Governance Principles.* https://www.weforum.org/reports/quantum-computing-governance-principles/

PUBLICACIONES DEL BANCO DE ESPAÑA

DOCUMENTOS OCASIONALES

2220 LUIS ÁNGEL MAZA: Una estimación de la huella de carbono en la cartera de préstamos a empresas de las entidades de crédito en España. (Existe una versión en inglés con el mismo número).

2221 SUSANA MORENO SÁNCHEZ: The EU-UK relationship: regulatory divergence and the level playing field.

2222 ANDRÉS ALONSO-ROBISCO y JOSÉ MANUEL CARBÓ: Inteligencia artificial y finanzas: una alianza estratégica.

2223 LUIS FERNÁNDEZ LAFUERZA, MATÍAS LAMAS, JAVIER MENCÍA, IRENE PABLOS y RAQUEL VEGAS: Análisis de la capacidad de uso de los colchones de capital durante la crisis generada por el COVID-19. (Existe una versión en inglés con el mismo número).

2224 SONSOLES GALLEGO, ISABEL GARRIDO e IGNACIO HERNANDO: Las líneas del FMI para aseguramiento y prevención de crisis y su uso en Latinoamérica (Existe una versión en inglés con el mismo número).

2301 LAURA HOSPIDO, CARLOS SANZ y ERNESTO VILLANUEVA: Air pollution: a review of its economic effects and policies to mitigate them.

2302 IRENE MONASTEROLO , MARÍA J. NIETO y EDO SCHETS: The good, the bad and the hot house world: conceptual underpinnings of the NGFS scenarios and suggestions for improvement.

2303 IADRIÁN LÓPEZ GONZÁLEZ: Inteligencia artificial aplicada al control de calidad en la producción de billetes.

2304 BELÉN AROCA MOYA: Conceptos, fundamentos y herramientas de neurociencia, y su aplicación al billete.

2305 MARÍA ALONSO, EDUARDO GUTIÉRREZ, ENRIQUE MORAL-BENITO, DIANA POSADA y PATROCINIO TELLO-CASAS: Un repaso de las diversas iniciativas desplegadas a nivel nacional e internacional para hacer frente a los riesgos de exclusión financiera.

2306 JOSÉ LUIS ROMERO UGARTE, ABEL SÁNCHEZ MARTÍN y CARLOS MARTÍN RODRÍGUEZ: Alternativas a la evolución de la operativa bancaria mayorista en el Eurosistema. (Existe una versión en inglés con el mismo número).

2307 HENRIQUE S. BASSO, OURANIA DIMAKOU and MYROSLAV PIDKUYKO: How inflation varies across Spanish households.

2308 LAURA CRESPO, NAJIBA EL AMRANI, CARLOS GENTO y ERNESTO VILLANUEVA: Heterogeneidad en el uso de los medios de pago y la banca *online:* un análisis a partir de la Encuesta Financiera de las Familias (2002-2020).

2309 HENRIQUE S. BASSO, OURANIA DIMAKOU y MYROSLAV PIDKUYKO: How consumption carbon emission intensity varies across Spanish households.

2310 IVÁN AUCIELLO-ESTÉVEZ, JOSEP PIJOAN-MAS, PAU ROLDAN-BLANCO y FEDERICO TAGLIATI: Dual labor markets in Spain: a firm-side perspective.

2311 CARLOS PÉREZ MONTES, JORGE E. GALÁN, MARÍA BRU, JULIO GÁLVEZ, ALBERTO GARCÍA, CARLOS GONZÁLEZ, SAMUEL HURTADO, NADIA LAVÍN, EDUARDO PÉREZ ASENJO e IRENE ROIBÁS: Marco de análisis sistémico del impacto de los riesgos económicos y financieros. (Existe una versión en inglés con el mismo número).

2312 SERGIO MAYORDOMO e IRENE ROIBÁS: La traslación de los tipos de interés de mercado a los tipos de interés bancarios. (Existe una versión en inglés con el mismo número).

2313 CARLOS PÉREZ MONTES, ALEJANDRO FERRER, LAURA ÁLVAREZ ROMÁN, HENRIQUE BASSO, BEATRIZ GONZÁLEZ LÓPEZ, GABRIEL JIMÉNEZ, PEDRO JAVIER MARTÍNEZ-VALERO, SERGIO MAYORDOMO, ÁLVARO MENÉNDEZ PUJADAS, LOLA MORALES, MYROSLAV PIDKUYKO y ÁNGEL VALENTÍN: Marco de análisis individual y sectorial del impacto de los riesgos económicos y financieros. (Existe una versión en inglés con el mismo número).

2314 PANA ALVES, CARMEN BROTO, MARÍA GIL y MATÍAS LAMAS: Indicadores de riesgos y vulnerabilidades en el mercado de la vivienda en España.

2215 ANDRÉS AZQUETA-GAVALDÓN, MARINA DIAKONOVA, CORINNA GHIRELLI y JAVIER J. PÉREZ: Sources of economic policy uncertainty in the euro area: a ready-to-use database.

2316 FERNANDO GARCÍA MARTÍNEZ y MATÍAS PACCE: El sector eléctrico español ante el alza del precio del gas y las medidas públicas en respuesta a dicha alza. (Existe una versión en inglés con el mismo número).

2317 ROBERTO BLANCO y SERGIO MAYORDOMO: Evidencia sobre el alcance de los programas de garantías públicas y de ayudas directas a las empresas españolas implementados durante la crisis del COVID-19. (Existe una versión en inglés con el mismo número).

2318 ISABEL GARRIDO y IRUNE SOLERA: Has the 2021 general SDR allocation been useful? For what and for whom?

2319 ROBERTO BLANCO, ELENA FERNÁNDEZ, MIGUEL GARCÍA-POSADA y SERGIO MAYORDOMO: An estimation of the default probabilities of Spanish non-financial corporations and their application to evaluate public policies.

2320 BANCO DE ESPAÑA: La accesibilidad presencial a los servicios bancarios en España: Informe de seguimiento 2023. (Existe una versión en inglés con el mismo número).

2321 EDUARDO AGUILAR GARCÍA, MARIO ALLOZA FRUTOS, TAMARA DE LA MATA, ENRIQUE MORAL-BENITO, IÑIGO PORTILLO PAMPIN y DAVID SARASA FLORES: Una primera caracterización de las empresas receptoras de fondos NGEU en España.

2401 ALEJANDRO MORALES, MANUEL ORTEGA, JOAQUÍN RIVERO y SUSANA SALA: ¿Cómo identificar a todas las sociedades del mundo? La experiencia del código LEI (Legal Entity Identifier).

2402 XAVIER SERRA y SONSOLES GALLEGO: Un primer balance del *Resilience and Sustainability Trust* del FMI como canal de utilización de los derechos especiales de giro. (Existe una versión en inglés con el mismo número).

2403 PABLO HERNÁNDEZ DE COS: El papel de la política macroprudencial en la estabilización de las fluctuaciones macrofinancieras. Conferencia de Estabilidad Financiera/Banco de Portugal, Lisboa (Portugal), 2 de octubre de 2023.

2404 MORTEZA GHOMI, SAMUEL HURTADO y JOSÉ MANUEL MONTERO: Análisis de la dinámica reciente de la inflación en España. Un enfoque basado en el modelo de Blanchard y Bernanke (2023).

2405 PILUCA ALVARGONZÁLEZ, MARINA ASENSIO, CRISTINA BARCELÓ, OLYMPIA BOVER, LUCÍA COBREROS, LAURA CRESPO, NAJIBA EL AMRANI, SANDRA GARCÍA-URIBE, CARLOS GENTO, MARINA GÓMEZ, PALOMA URCELAY, ERNESTO VILLANUEVA and ELENA VOZMEDIANO: The Spanish Survey of Household Finances (EFF): description and methods of the 2020 wave.

2406 ANA GÓMEZ LOSCOS, MIGUEL ÁNGEL GONZÁLEZ SIMÓN y MATÍAS JOSÉ PACCE: Modelo para la previsión del PIB de la economía española a corto plazo en tiempo real (Spain-STING): nueva especificación y reevaluación de su capacidad predictiva. (Existe una versión en inglés con el mismo número).

2407 OLYMPIA BOVER, LAURA CRESPO, SANDRA GARCÍA-URIBE, MARINA GÓMEZ-GARCÍA, PALOMA URCELAY y PILAR VELILLA: Micro and macro data on household wealth, income and expenditure: comparing the Spanish Survey of Household Finances (EFF) to other statistical sources.

2408 ÁNGEL ESTRADA y CARLOS PÉREZ MONTES: Un análisis de la evolución de la actividad bancaria en España tras el establecimiento del gravamen temporal de la ley 38/2022.

2409 PABLO A. AGUILAR, MARIO ALLOZA, JAMES COSTAIN, SAMUEL HURTADO y JAIME MARTÍNEZ-MARTÍN: El efecto de los programas de compras de activos del Banco Central Europeo en las cuentas públicas de España. (Existe una versión en inglés con el mismo número).

2410 RICARDO BARAHONA y MARÍA RODRÍGUEZ-MORENO: Estimating the OIS term premium with analyst expectation surveys.

2411 JOSÉ MANUEL CARBÓ, HOSSEIN JAHANSHAHLOO y JOSÉ CARLOS PIQUERAS: Análisis de fuentes de datos para seguir la evolución de *Bitcoin*.

2412 IVÁN KATARYNIUK, RAQUEL LORENZO ALONSO, ENRIQUE MARTÍNEZ CASILLAS y JACOPO TIMINI: An extended Debt Sustainability Analysis framework for Latin American economies.

2413 Encuesta Financiera de las Familias (EFF) 2022: métodos, resultados y cambios desde 2020.

2414 ÁNGEL ESTRADA, CARLOS PÉREZ MONTES, JORGE ABAD, CARMEN BROTO, ESTHER CÁCERES, ALEJANDRO FERRER, JORGE GALÁN, GERGELY GANICS, JAVIER GARCÍA VILLASUR, SAMUEL HURTADO, NADIA LAVÍN, JOËL MARBET, ENRIC MARTORELL, DAVID MARTÍNEZ-MIERA, ANA MOLINA, IRENE PABLOS y GABRIEL PÉREZ-QUIRÓS: Análisis de los riesgos sistémicos cíclicos en España y de su mitigación mediante requerimientos de capital bancario contracíclicos. (Existe una versión en inglés con el mismo número).

2415 CONCEPCIÓN FERNÁNDEZ ZAMANILLO y LUNA AZAHARA ROMO GONZÁLEZ: Facilitadores de la innovación 2.0: impulsando la innovación financiera en la era *fintech*.

2416 JAMES COSTAIN y ANTON NAKOV: Models of price setting and inflation dynamics.

2417 ARTURO PABLO MACÍAS FERNÁNDEZ e IGNACIO DE LA PEÑA LEAL: Sensibilidad a los tipos de interés soberanos de la cartera de colateral elegible para los préstamos de política monetaria.

2418 ANTONIO F. AMORES, HENRIQUE BASSO, JOHANNES SIMEON BISCHL, PAOLA DE AGOSTINI, SILVIA DE POLI, EMANUELE DICARLO, MARIA FLEVOTOMOU, MAXIMILIAN FREIER, SOFIA MAIER, ESTEBAN GARCÍA-MIRALLES, MYROSLAV PIDKUYKO, MATTIA RICCI and SARA RISCADO: Inflation, fiscal policy and inequality. The distributional impact of fiscal measures to compensate for consumer inflation.

2419 LUIS ÁNGEL MAZA: Una reflexión sobre los umbrales cuantitativos en los modelos de depósito de las cuentas anuales y su posible impacto en el tamaño empresarial en España.

2420 MARIO ALLOZA, JORGE MARTÍNEZ, JUAN ROJAS y IACOPO VAROTTO: La dinámica de la deuda pública: una perspectiva estocástica aplicada al caso español. (Existe una versión en inglés con el mismo número).

2421 NOEMÍ LÓPEZ CHAMORRO: El camino hacia la supremacía cuántica: oportunidades y desafíos en el ámbito financiero, la nueva generación de criptografía resiliente.