NOVA BCU

Disrupción de la computación cuántica en el sistema financiero y de pagos:

Principales conceptos, impacto esperado y propuesta de abordaje para autoridades financieras.

BANCO CENTRAL DEL URUGUAY

BANCO CENTRAL DEL URUGUAY

Contenido

BANCO CENTRAL DEL URUGUAY

Introducción

La computación cuántica es un campo emergente de la informática que aprovecha los principios de la mecánica cuántica para realizar cálculos de manera radicalmente distinta a la computación clásica. Su potencial para resolver problemas complejos en tiempos significativamente menores ha generado un creciente interés en sectores académicos, industriales y gubernamentales. Prototipos construidos permiten resolver en pocos minutos problemas que una computadora clásica tardaría cientos de años, o más. Su poder de cálculo es 160 millones de veces más poderoso que el de supercomputadoras actuales, dependiendo del problema a resolver.

A diferencia de las computadoras clásicas, que utilizan bits clásicos para representar información en forma binaria, las computadoras cuánticas emplean cúbits. Estos pueden existir en un estado de 0, 1, o en una superposición de ambos simultáneamente, lo que permite el procesamiento paralelo de múltiples cálculos a la vez. Además, los cúbits pueden estar entrelazados, una propiedad conocida como entrelazamiento cuántico, que permite correlaciones entre cúbits a grandes distancias y contribuye a la aceleración del procesamiento de información, sobre todo en problemas de alta complejidad computacional.

Otra característica clave es la coherencia cuántica, que permite mantener los estados superpuestos y los cúbits entrelazados durante cierto tiempo antes de que se produzca la decoherencia, un fenómeno que afecta la estabilidad del sistema. Este desafío técnico es uno de los principales obstáculos para la escalabilidad de la computación cuántica.

El interés en la computación cuántica radica en su capacidad para resolver problemas que son computacionalmente intratables para los sistemas clásicos. Algunas de sus aplicaciones más relevantes incluyen:

- **Optimización:** en sectores como la logística, las finanzas y la investigación operativa, la computación cuántica puede encontrar soluciones óptimas a problemas complejos de manera más eficiente.
- **Simulación de sistemas cuánticos:** la capacidad de modelar moléculas y materiales a nivel cuántico tiene implicaciones importantes en la industria farmacéutica, en ciencias del clima y en el desarrollo de nuevos materiales.
- **Inteligencia Artificial y Aprendizaje Automático:** los algoritmos cuánticos pueden mejorar el procesamiento de datos en modelos de aprendizaje profundo, acelerando la obtención de resultados y mejorando su precisión.

Uno de los aspectos más críticos de la computación cuántica es su impacto en la ciberseguridad. Gran parte de la criptografía actual, basada en la dificultad computacional de ciertos problemas matemáticos como la factorización de números primos y el logaritmo discreto, sería vulnerable a los algoritmos cuánticos como el de Shor. Esto ha generado iniciativas globales en el desarrollo de criptografía post-cuántica (también conocida como criptografía resistente o segura a la computación cuántica), que busca diseñar sistemas resistentes a ataques cuánticos para garantizar la seguridad de las comunicaciones y transacciones digitales en el futuro.

Dado su potencial, desde el año 2019 se ha visto una explosión en la inversión en el orden de los billones destinada a la computación cuántica. Existen múltiples iniciativas en curso lideradas por empresas tecnológicas, centros de investigación y gobiernos que buscan posicionarse a la vanguardia de la computación cuántica. Programas como los desarrollados por IBM, Google, y empresas emergentes especializadas están empujando los límites tecnológicos. Además, entidades gubernamentales pertenecientes a la Unión Europea, China y Estados Unidos están invirtiendo en infraestructura cuántica, con programas de financiación y desarrollo estratégico. También la academia se está preparando para la futura demanda de profesionales en esta nueva disciplina, ofreciendo cursos y carreras de grado o posgrado.

No obstante, el avance de esta tecnología no atañe únicamente a temas técnicos, sino que también tiene implicaciones en la política internacional, ya que la supremacía cuántica podría redefinir el equilibrio de poder global. La posibilidad de romper cifrados y realizar simulaciones avanzadas tiene implicaciones tanto en el ámbito económico como en la seguridad nacional, impulsando una carrera tecnológica entre las principales potencias mundiales. La información pública sobre los avances puede constituir una versión parcial de la realidad, resguardada con los mayores estándares de confidencialidad por sus tenedores.

A pesar de sus promesas, la computación cuántica enfrenta importantes desafíos técnicos y teóricos. La corrección de errores cuánticos, la estabilidad de los cúbits y la construcción de hardware escalable son áreas críticas en investigación. Actualmente, la computación cuántica sigue en una fase predominantemente experimental, donde se ha avanzado con prototipos de computadoras cuánticas desarrollados por el sector privado, la academia y gobiernos. Sin embargo, la transición hacia un uso práctico a gran escala aún requiere avances significativos.

Como reflexión general, la computación cuántica representa una revolución en la manera en que procesamos la información. Su impacto podría transformar industrias enteras, aunque aún estamos en las primeras etapas de su desarrollo. A medida que se superen los desafíos actuales, esta tecnología podría redefinir el futuro de la computación y de la resolución de problemas complejos a nivel global. Además, su avance requerirá una estrecha colaboración entre la comunidad científica, la industria y los gobiernos para abordar los desafíos técnicos, regulatorios y de seguridad que emergen con su desarrollo.

Algunos conceptos fundamentales

La física cuántica es la rama de la física que estudia el comportamiento y las propiedades fundamentales de la materia y la energía a escalas extremadamente pequeñas, como los átomos y las partículas subatómicas, donde las reglas de la física clásica dejan de aplicarse. Es a partir de la combinación de la física cuántica y la teoría de la computación que surge una nueva generación de computadoras, llamadas computadoras cuánticas, capaces de resolver problemas que están más allá del alcance de las computadoras clásicas.

A continuación, se presentan brevemente algunos conceptos relevantes relacionados con la computación cuántica, que son desarrollados con más detalle en el documento **“Disrupción de la computación cuántica en el sistema financiero y de pagos. Documento técnico acompañante.”**

Cúbit: un cúbit (bit cuántico) es la unidad fundamental de información en computación cuántica. Aunque todo cúbit es un objeto cuántico[1], no todos los objetos cuánticos son cúbits, ya que este debe cumplir ciertas condiciones que permitan su control y manipulación para procesamiento de información. Los cúbits presentan características fundamentales como la superposición, el entrelazamiento y la inferencia cuántica.

Superposición: en la computación clásica, un bit puede tomar un único valor en un instante dado: 0 o 1. En cambio, gracias a la superposición cuántica, un cúbit puede existir en una combinación de múltiples estados simultáneamente. La superposición permite que una computadora cuántica realice cálculos en múltiples estados simultáneamente, proporcionando un potencial de aceleración exponencial en ciertos algoritmos. Este concepto puede pensarse como si hiciéramos girar rápidamente una moneda sobre una mesa. Mientras gira, la moneda parece estar en dos estados al mismo tiempo, cara y cruz, porque no se puede determinar cuál lado se mostrará hasta que la moneda deje de girar y se apoye uno de sus lados sobre la mesa.

[1] Se denomina objeto cuántico a cualquier entidad que sigue las leyes de la mecánica cuántica, como átomos, electrones, fotones, iones y cuasipartículas

Entrelazamiento: el entrelazamiento es una propiedad fundamental de la mecánica cuántica donde dos o más cúbits están correlacionados de manera no clásica. El estado de uno depende instantáneamente del otro, sin importar la distancia que los separe. Al compartir estos cúbits entrelazados propiedades cuánticas y estar medidos con una única función de onda, si se mide el primer cúbit y se obtiene 0, el segundo cúbit siempre dará un resultado correlacionado (que será siempre 0 o 1, según esté diseñado el experimento). Este concepto puede ejemplificarse de la siguiente manera: imagine que una persona tiene un par de guantes, uno derecho y otro izquierdo, y decide separarlos y poner cada uno en una caja -siendo las dos cajas idénticas entre sí- y enviar una de ellas a un amigo en otra parte del mundo. Hasta que esta persona no abra su caja, no sabrá si se tiene el guante derecho o el izquierdo. Sin embargo, en el momento exacto en que la abra y vea su que su guante es, por ejemplo, el derecho, automáticamente sabrá que el otro amigo tiene el guante izquierdo, sin importar la distancia entre ambos.

Interferencia: la interferencia cuántica es un fenómeno característico de la mecánica cuántica en el cual las probabilidades asociadas a diferentes estados cuánticos se combinan (interfieren) de manera constructiva (se incrementa la probabilidad para un resultado) o destructiva (para cancelar soluciones incorrectas), afectando los resultados de una medición.

Teorema del no-clonado: el teorema del no-clonado establece que no es posible copiar un estado cuántico desconocido de forma exacta. Mientras que en los sistemas clásicos cualquier dato puede copiarse sin modificar su estado original, en los sistemas cuánticos, cualquier intento de copiar un cúbit desconocido alterará su estado debido a la medición, lo que hace imposible la duplicación exacta.

Coherencia: la coherencia es la propiedad que permite que un sistema cuántico mantenga, por ejemplo, su superposición y entrelazamiento a lo largo del tiempo. Ésta mide cuánto tiempo un sistema de cúbits puede permanecer en un estado cuántico sin ser perturbado por su entorno. Es un factor de suma relevancia, ya que la computación cuántica requiere mantener la coherencia el tiempo suficiente para completar las operaciones lógicas de los algoritmos antes de que los cúbits pierdan la integridad de su información cuántica.

Decoherencia: como concepto inverso a la coherencia, la decoherencia es el proceso por el cual un sistema cuántico pierde su estado cuántico debido a interacciones con el entorno. Esto lleva a que la información cuántica se degrade y los cálculos se vuelvan inexactos, y es una barrera clave para la escalabilidad de las computadoras cuánticas. Los fenómenos de coherencia y decoherencia pueden ser pensados como un cuerpo de baile sincronizado (sistema de cúbits), que durante una presentación sobre el escenario ven su concentración perturbada al prenderse una alarma de incendio en el lugar de la presentación (ruido externo). Esto hará que la coreografía (coherencia) sufra alteraciones o pérdida de calidad (decoherencia) y que incluso la misma culmine de manera prematura (colapso de onda).

Programación cuántica: es el desarrollo de software específicamente diseñado para ejecutarse en computadoras cuánticas. Dado que estas máquinas operan bajo principios radicalmente distintos a los sistemas clásicos, los lenguajes y paradigmas de programación cuántica pueden y deben aprovechar fenómenos como la interferencia cuántica, superposición y entrelazamiento. La programación cuántica es lo que genera a los algoritmos cuánticos.

Algoritmos cuánticos: un algoritmo cuántico es un procedimiento computacional optimizado para computadoras cuánticas, diseñado para explotar las propiedades fundamentales de la mecánica cuántica. En ese sentido, a diferencia de los algoritmos clásicos, los algoritmos cuánticos pueden procesar múltiples soluciones simultáneamente y pueden emplear la interferencia cuántica para reforzar los resultados correctos y cancelar los incorrectos. Si bien todo algoritmo clásico puede ser expresado en términos de un algoritmo

cuántico, la verdadera ventaja de la computación cuántica radica en su capacidad para resolver problemas de manera exponencialmente más rápida en comparación con las computadoras tradicionales.

Tipos de algoritmos cuánticos: estos pueden clasificarse en distintas categorías en función de sus principios matemáticos y su aplicabilidad a problemas específicos: algoritmos cuánticos basados en transformadas de Fourier cuánticas, algoritmos de búsqueda y optimización cuántica, algoritmos basados en simulación cuántica y algoritmos cuánticos de aprendizaje automático.

Dentro de los algoritmos cuánticos basados en transformadas de Fourier cuánticas se encuentra el Algoritmo de Factoreo de Shor, que tiene especial relevancia ya que representa una amenaza seria para la criptografía de clave pública, al permitir la factorización de números primos (Shor, 1994). Por otro lado, el Algoritmo de Búsqueda de Grover –que se clasifica dentro de los algoritmos de búsqueda y optimización cuántica- también es relevante en la criptografía (especialmente en la simétrica), ya que reduce el número de combinaciones que deben probarse en un ataque de fuerza bruta clásico (Grover, 1996).

Unidad de Procesamiento Cuántico (QPU): son el equivalente cuántico de una Unidad de Procesamiento Central clásica, conocidas por su sigla CPU. Contiene cúbits, circuitos cuánticos y el soporte necesario para realizar cálculos cuánticos. Las QPUs aprovechan los fenómenos cuánticos antes mencionados para realizar cálculos de manera más eficiente en ciertas tareas específicas.

Evolución de la Computación Cuántica

A modo de resumen, la historia de la computación cuántica ha estado marcada por avances teóricos y experimentales clave, tanto en las ramas de la física, electrónica y mecánica, como en las ciencias de la computación, la informática y la teoría de la información, lo cual se detalla a continuación:

- **1920-1930:** Desarrollo de los fundamentos de la mecánica cuántica, con trabajos de Schrödinger, Heisenberg y Dirac, que sentaron las bases del comportamiento de partículas subatómicas.
- **1981:** Richard Feynman sugiere que las computadoras cuánticas podrían simular sistemas físicos de manera más eficiente que las computadoras clásicas.
- **1994:** Peter Shor desarrolla un algoritmo cuántico para la factorización de números primos, mostrando el potencial de la computación cuántica para desafiar los sistemas de criptografía actuales.
- **1998:** Se logra el primer bit cuántico (cúbit) funcional en un entorno experimental.
- **2001:** IBM y Stanford demuestran experimentalmente el algoritmo de Shor con éxito en un sistema cuántico de 7 cúbits.
- **2011:** Se presentan los primeros procesadores cuánticos comerciales, con empresas como D-Wave iniciando la comercialización de tecnología basada en computación cuántica adiabática.
- **2016:** IBM Quantum Experience permite el acceso en la nube a un procesador cuántico, democratizando la investigación y experimentación.
- **2019:** Google anuncia haber alcanzado la supremacía cuántica al demostrar que su procesador cuántico Sycamore puede resolver en minutos un problema que tomaría miles de años a una supercomputadora clásica.

- **2020-2022:** Se lanzan iniciativas de criptografía post-cuántica para abordar la amenaza que supone la computación cuántica a la seguridad digital.
- **2023-presente:** Se incrementan las inversiones y avances en computadoras cuánticas con más de 100 cúbits, mejorando la estabilidad y reduciendo la tasa de error.
- **Fines del 2024:** Google presenta Willow, capaz de realizar en menos de cinco minutos cálculos que a las supercomputadoras más avanzadas les llevarían aproximadamente 10 septillones de años. Adicionalmente, permite reducir exponencialmente los errores cuánticos a medida que se incrementa el número de cúbits.
- **Principios del 2025:** Se presenta el chip Majorana[2] de Microsoft, basado en la teoría de los fermiones de Majorana, que poseen propiedades exóticas ideales para la creación de cúbits topológicos.

Beneficios de la Computación Cuántica

Los sistemas de cómputo clásicos basados en bits (0 y 1) tienen limitaciones estructurales cuando se trata de resolver ciertos problemas que requieren una cantidad exponencial de recursos computacionales. Por otro lado, la computación cuántica es una tecnología emergente que promete superar muchas de las limitaciones de estos sistemas clásicos, permitiendo resolver problemas complejos de manera más eficiente. Como se comentó anteriormente, su potencial radica en la capacidad de los cúbits para representar múltiples estados simultáneamente mediante la superposición cuántica y en la posibilidad de realizar cálculos en paralelo a través del entrelazamiento. A continuación, se destacan aportes que ofrece esta tecnología.

Principales problemas que permite abordar la computación cuántica

Resolución de problemas matemáticos avanzados

Los algoritmos cuánticos pueden abordar problemas matemáticos complejos que resultan intratables para las computadoras clásicas. Algunos ejemplos incluyen:

- Factorización de números enteros grandes, lo que tiene implicaciones directas en la criptografía. Algoritmos como el de Rivest–Shamir–Adleman (RSA) y los basados en criptografía de curva elíptica (Elliptic Curve Cryptography, ECC) pueden verse directamente afectados por estos desarrollos.
- Cálculo de logaritmos y exponenciales con mayor eficiencia.
- Optimización de funciones matemáticas en espacios de alta dimensión.

Algoritmos de búsqueda y optimización

Los algoritmos cuánticos pueden realizar búsquedas y optimizaciones de manera mucho más eficiente que los algoritmos clásicos. Algunos ejemplos incluyen:

- Realizar búsquedas en bases de datos desordenadas con una aceleración cuadrática.

[2] https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/

- Optimización combinatoria como el problema del viajante de comercio3, la asignación de recursos y la planificación logística.
- Métodos adiabáticos y de recocido cuántico para optimizaciones complejas como el modelado financiero, la bioinformática y el diseño de materiales.

Caminata cuántica

Las caminatas cuánticas son la versión cuántica de los procesos aleatorios utilizados en la estadística y en la teoría de cadenas de Markov. Estas permiten:

- Modelar procesos de toma de decisiones en inteligencia artificial.
- Mejorar la eficiencia en el muestreo y la simulación de sistemas físicos.
- Desarrollar nuevas herramientas en finanzas cuantitativas y análisis de riesgos.

Resolución de ecuaciones lineales

El algoritmo de Harrow-Hassidim-Lloyd (HHL) es un algoritmo cuántico que permite resolver sistemas de ecuaciones lineales de manera exponencialmente más eficiente que los métodos clásicos. Sus aplicaciones incluyen:

- Modelado financiero en mercados complejos.
- Análisis de grandes volúmenes de datos en machine learning.
- Solución de ecuaciones diferenciales en ingeniería y ciencias aplicadas.

Simulación cuántica

Uno de los usos más prometedores de la computación cuántica es la simulación de sistemas cuánticos. Dado que la mecánica cuántica no puede ser simulada eficientemente en computadoras clásicas, las cuánticas permiten:

- Modelar reacciones químicas y diseñar nuevos materiales con aplicaciones en la industria farmacéutica y energética.
- Desarrollar nuevos fármacos mediante la simulación de interacciones moleculares.
- Optimizar procesos en la industria química y de materiales avanzados.

Aplicaciones destacadas para la industria

La computación cuántica tiene el potencial de ser aplicada a una multiplicidad de problemas, como los detallados anteriormente. Por lo tanto, los sectores que se vean afectados por estos desafíos en la práctica tendrán la oportunidad de aprovechar los beneficios en el procesamiento que la computación cuántica promete. A continuación, se plantean algunas aplicaciones posibles, destacando aquellas directamente aplicables al sistema financiero.

[3] A grandes rasgos, este problema de optimización plantea encontrar la ruta más conveniente para que un comerciante visite ciertas ciudades una vez y regrese al lugar de origen.

Mercados financieros

El sector financiero es un área que depende de la seguridad, velocidad y precisión de los cálculos. La computación cuántica permitiría ofrecer ventajas en:

Análisis de riesgos

- Modelado de riesgos más preciso: los bancos y aseguradoras podrán evaluar riesgos con mayor exactitud utilizando simulaciones cuánticas.
- Mejoras en la valoración de derivados: los cálculos relacionados con la valoración de derivados financieros podrán realizarse más rápidamente, reduciendo el riesgo de inversión.
- Riesgos financieros relacionados al clima: la evaluación del riesgo de transición climática puede beneficiarse de la capacidad de la computación cuántica para analizar interdependencias complejas entre múltiples variables económicas y ambientales.
- Vigilancia de estabilidad financiera: los reguladores podrían aprovechar la computación cuántica para analizar vastos volúmenes de datos en tiempo real, identificando patrones anómalos y señales tempranas de inestabilidad. Esto permitiría una respuesta preventiva más ágil, fortaleciendo la coordinación interinstitucional y minimizando el riesgo sistémico en los mercados.

Gestión de carteras

- Optimización de portafolios: los inversores y asesores podrán mejorar la selección de activos y la asignación de capital mediante algoritmos cuánticos de optimización.
- Predicción de tendencias de mercado: modelos cuánticos pueden identificar patrones en grandes volúmenes de datos financieros.
- Personalización de productos y servicios: la optimización cuántica permitirá ofrecer a los usuarios financieros productos y servicios adaptados a sus características y necesidades.

Prevención de fraudes

- Detección de patrones anómalos: los algoritmos cuánticos pueden contribuir para analizar transacciones y detectar posibles fraudes con mayor precisión.
- Seguridad en transacciones financieras: con el uso de algoritmos cuánticos, las instituciones financieras pueden prevenir ataques cibernéticos.

Seguridad y criptografía[4]

Más allá de la criptografía resistente a la computación cuántica (que en la actualidad está basada en la complejidad matemática y se desarrolla para ser ejecutada en computadoras clásicas), esta tecnología emergente brindaría nuevas oportunidades para la innovación criptográfica a partir de factores elementales de la física y mecánica cuántica.

A continuación, se presentan algunos ejemplos de potenciales innovaciones.

[4] Más detalle puede encontrarse en documento técnico acompañante.

- **Distribución cuántica de claves (QKD):** Basada en el principio de incertidumbre[5], permite a dos partes generar una clave secreta compartida utilizando partículas cuánticas, generalmente fotones. Cualquiera que intente espiar, dejará un rastro detectable al realizar una medición. El protocolo más conocido es el BB84 y varias compañías ya venden sistemas de QKD.
- **Generación de números aleatorios cuánticos (QRNG):** Utiliza fenómenos cuánticos, como el principio de incertidumbre, para generar números verdaderamente aleatorios, lo que mejora la calidad y seguridad en comparación con los métodos clásicos pseudoaleatorios. Serviría para proveer claves seguras para sistemas criptográficos clásicos y cuánticos.
- **Firma digital cuántica:** Similar a las firmas digitales clásicas, pero utiliza principios cuánticos como el entrelazamiento para garantizar la autenticidad y el no repudio de mensajes.
- **Criptografía cuántica multipartita:** Extiende los principios de QKD y otros protocolos a escenarios con múltiples partes, permitiendo el intercambio seguro de información entre más de dos usuarios.
- **Redes cuánticas:** se están diseñando redes de comunicación cuántica basada en la teletransportación que podrían ofrecer una seguridad, en teoría, inquebrantable.

Inteligencia artificial

La inteligencia artificial (IA) es un área que requiere un alto poder de cómputo dado el volumen de datos que es necesario procesar. Actuando como catalizador clave, la computación cuántica permitirá:

- Mejoras en modelos de aprendizaje automático: la capacidad de los algoritmos cuánticos para procesar grandes volúmenes de datos en paralelo permitirá desarrollar modelos más eficientes.
- Reducción del tiempo de entrenamiento: los modelos de IA que requieren meses de entrenamiento podrán optimizarse en menos tiempo gracias a la computación cuántica.
- Procesamiento de grandes bases de datos: la combinación de IA y computación cuántica será clave en sectores como análisis financiero, medicina personalizada y logística.

Otros casos de uso de interés

Optimización

Uno de los problemas más difíciles de resolver en la computación clásica es la optimización de procesos con múltiples variables y restricciones. Los algoritmos cuánticos pueden abordar estos problemas con una eficiencia sin precedentes, lo que los hace ideales para aplicaciones como la optimización del transporte público, tráfico, logística y rutas.

Investigación científica

La computación cuántica permitirá abordar problemas científicos que hoy son intratables debido a la complejidad de sus cálculos. Su impacto se verá, entre otros, en la física con la simulación de sistemas

[5] El principio de incertidumbre asegura que cualquier intento de medir los cúbits altera sus estados, revelando así la presencia de un intruso.

cuánticos, la química con el descubrimiento de nuevos materiales y reacciones químicas, las matemáticas para la resolución ecuaciones complejas, y la industria farmacéutica con el desarrollo de nuevos fármacos.

Riesgos y amenazas a considerar[6]

Como contraposición a los beneficios directos que brindaría la computación cuántica, y tomando como factor común el disruptivo poder de procesamiento que ofrece, ésta también tiene el potencial de disminuir la efectividad o quebrar muchos de los sistemas criptográficos ampliamente utilizados en la actualidad, lo que pone en riesgo la seguridad de la información en diversos sectores.

¿Cómo impacta en la ciberseguridad actual?

Dentro de los algoritmos de búsqueda y optimización cuántica, el **Algoritmo de Búsqueda de Grover** es relevante en la criptografía simétrica, ya que reduce el número de combinaciones que deben probarse en un ataque de fuerza bruta clásico. Este algoritmo permite que, en lugar de probar todas las combinaciones posibles (un esfuerzo de orden $O(2^n)$), una computadora cuántica pueda resolver el problema de búsqueda en aproximadamente $O(2^{n/2})$ pasos, lo que debilita la seguridad de algoritmos criptográficos como AES y SHA. Esto obliga a las organizaciones a considerar claves más largas para resistir posibles ataques cuánticos. En este caso, la solución al problema es sencillo, ya que lo que se necesitaría sería simplemente duplicar la longitud de las claves, garantizando así un nivel de seguridad adecuado frente a ataques potenciados por algoritmos cuánticos como el de Grover.

Sin embargo, hay otros algoritmos que presentan amenazas para la ciberseguridad que no se mitigan simplemente aumentando el largo de las claves criptográficas. Los algoritmos criptográficos de clave pública más utilizados hoy en día, como RSA, ECC y Diffie-Hellman (DH), se basan en la dificultad computacional de problemas matemáticos como la factorización de números primos o el logaritmo discreto. Sin embargo, el **Algoritmo de Shor**, presentado en 1994, establece que una computadora cuántica con suficiente capacidad puede resolver estos problemas en un tiempo exponencialmente menor en comparación con una computadora clásica. Esto implica que cualquier información cifrada con estos algoritmos podría ser descifrada, perdiéndose la confidencialidad y, en algunos casos, también la integridad de los datos, afectando de esa manera a las firmas digitales de igual manera. Por lo tanto, la criptografía asimétrica se vería completamente comprometida ante la computación cuántica, que permite romper sus claves en tiempos razonables. Esto afecta directamente los estándares actuales establecidos por NIST, como el SP 800-56A/B/C para infraestructuras de clave pública y el FIPS 186 para firmas digitales.

Además, uno de los problemas más graves es la posibilidad de que los atacantes almacenen datos cifrados hoy para descifrarlos en el futuro. Este modelo de ataque se conoce como **"Harvest Now, Decrypt Later" ("Almacenar Ahora, Descifrar Después")**. El concepto radica en que actores podrían estar recopilando grandes cantidades de datos cifrados con algoritmos vulnerables, sobre todo, con criptografía asimétrica. Cuando una computadora cuántica suficientemente avanzada les esté disponible, todos estos datos podrán ser descifrados rápidamente.

Dada la dificultad inherente a los cambios en infraestructuras tecnológicas, sobre todo en grandes organizaciones o en el sector público, y la dependencia de los sistemas actuales en criptografía vulnerable, la transición a algoritmos resistentes a la computación cuántica debe iniciarse de inmediato. En este sentido, el

[6] Mayor desarrollo de estas temáticas se encuentra en documento técnico acompañante.

Teorema de Mosca (2015) plantea que la seguridad de los datos cifrados depende tanto del tiempo necesario para implantar una infraestructura resistente y del tiempo que deben mantenerse seguros estos datos, como del tiempo que tomará desarrollar una computadora cuántica capaz de romper la criptografía actual. Si la suma del tiempo que los datos deben ser protegidos y el tiempo requerido para implementar tecnologías post-cuánticas es mayor que el tiempo estimado para que los atacantes dispongan de computadoras cuánticas avanzadas, los datos estarán en riesgo.

Esto puede observarse fácilmente pensándose como una triple desigualdad temporal, que evalúa la seguridad de la información en función de tres variables clave: $X + Y > Z$, donde:

- X: tiempo que la información cifrada debe permanecer segura. Ejemplo: datos gubernamentales, registros financieros o secretos industriales que deben mantenerse seguros durante 10, 20 o incluso 50 años.
- Y: tiempo necesario para migrar los sistemas criptográficos a soluciones resistentes a la computación cuántica. En grandes organizaciones y gobiernos, este proceso puede tomar entre 5 y 10 años (o más inclusive).
- Z: tiempo estimado hasta que una computadora cuántica suficientemente poderosa pueda romper la criptografía actual.

Si la suma del tiempo que los datos deben mantenerse seguros (X) y el tiempo requerido para la migración (Y) es mayor que el tiempo estimado para que las computadoras cuánticas rompan los sistemas criptográficos (Z), entonces existe un riesgo de exposición de datos sensibles antes de que los sistemas puedan ser protegidos.

Por otra parte, muchas organizaciones, especialmente gobiernos e instituciones financieras, tienen tiempos de actualización de sistemas que pueden tardar varios años en completarse. Si la computación cuántica se desarrolla antes de completar esta migración tecnológica, existiría un período donde los datos podrían quedar expuestos a ataques. Las organizaciones deberán realizar un mapeo exhaustivo de todos sus sistemas para identificar en qué puntos se usa criptografía y qué partes de la infraestructura podrían verse comprometidas para asegurar una transición sin brechas de seguridad. Es posible que algunos sistemas puedan actualizarse con criptografía resistente a la computación cuántica mediante software, mientras que otros requerirán cambios más radicales, llegando a la necesidad de desarrollar nuevas aplicaciones y sistemas, o remplazar hardware. Para ello es necesario que los nuevos algoritmos estén estandarizados e implementados para poder usarse en componentes de tecnología. Por otro lado, la transición hacia la criptografía post-cuántica requerirá profesionales capacitados en los nuevos estándares criptográficos, ciberseguridad y arquitectura de sistemas. Actualmente, hay una escasez global de expertos en ciberseguridad, lo que podría agravar la problemática si no se toman medidas de capacitación tempranas.

La falta de planificación puede generar una crisis tecnológica, con sistemas colapsando debido a la incapacidad de adaptarse a las nuevas amenazas cuánticas. Se necesita un esfuerzo coordinado entre gobiernos, empresas y academia para establecer estrategias de mitigación y preparar una transición ordenada hacia criptografía post-cuántica.

¿Riesgos fuera del ámbito de la ciberseguridad?

Un punto a destacar es que, como se detalló previamente, la computación cuántica también tiene el potencial de transformar otras áreas como la inteligencia artificial, simulaciones científicas, desarrollo de nuevos materiales y optimización de procesos industriales.

Esta disrupción tecnológica podría generar una ventaja competitiva para los países o empresas que lideren el desarrollo de la computación cuántica, creando desigualdades tecnológicas muy significativas entre naciones, regiones y sectores económicos, lo que podría contribuir a profundizar brechas socioeconómicas existentes.

Trabajos relevantes relacionados

Dada su creciente importancia en el sistema financiero y de pagos, en los últimos años la computación cuántica ha sido sujeto de varios trabajos realizados por bancos centrales y otros reguladores de distintos países y organismos bilaterales e internacionales, así como otros actores públicos y privados.

Por ejemplo, la consultora estadounidense McKinsey & Company realizó un informe en 2020 en el que exploró el posible impacto de la computación cuántica en el mercado financiero (Dietz et al., 2020). Este trabajo planteaba que las aplicaciones más prometedoras de esta tecnología se encontrarán en las industrias que requieren modelos de alta complejidad y rapidez. En este sentido, la computación cuántica ofrece la posibilidad de optimizar composiciones de portafolios con rapidez y estimar más precisamente la exposición a riesgo de crédito. Al mismo tiempo, los pagos y transferencias se verían fortalecidos mediante una mejor encriptación. Las operaciones de trading de acciones y divisas también ofrecen grandes oportunidades, dado el aumento en la demanda de cálculos más precisos de riesgos de mercado. Por último, las áreas de ventas, marketing y distribución se beneficiarían de una toma de decisiones más precisa, especialmente en la asignación de recursos y servicios personalizados. Otras corporaciones dedicadas a la consultoría han publicado documentos de similares características.

Autoridades financieras

En los últimos años, varias autoridades financieras han abordado temas de computación cuántica y las oportunidades y riesgos que estos presentan al sistema financiero.

El Banco de Japón realizó un trabajo en el que analizó cómo la computación cuántica podría comprometer la seguridad de los algoritmos criptográficos de clave pública actualmente utilizados, amenaza muy relevante dado el uso generalizado de dichos algoritmos, en particular en la industria financiera (Kan y Une, 2021). El documento revisaba las tendencias a esas fechas en la investigación y desarrollo de computadoras cuánticas, los riesgos de seguridad asociados con los algoritmos criptográficos actuales y el progreso del NIST en la estandarización de criptografía post-cuántica. Además, se discutieron las respuestas de otras organizaciones que apoyan la transición hacia esta nueva criptografía y los desafíos futuros para su implementación.

Por otro lado, el trabajo de Vesely (2023) para el Banco Central de República Checa exploró las aplicaciones de los algoritmos cuánticos a la optimización dinámica de portafolios, basándose en el modelo de Markowitz. Se compararon varios tipos de algoritmos cuánticos que se corrieron en las plataformas en la nube de computación cuántica ofrecidas por IBM y D-Wave (en este último caso utilizando tecnología de quantum annealing[7]). Se demuestra la optimización de portafolios mediante la búsqueda de la composición óptima de

[7] Un Quantum Annealer es un tipo de computadora cuántica no universal, diseñada específicamente para resolver problemas de optimización. Más detalle en documento técnico acompañante.

divisas en las reservas del Banco Central de República Checa. El artículo también tiene como objetivo proporcionar a bancos centrales y otros reguladores del sistema financiero una revisión de la literatura sobre algoritmos de optimización cuántica, dado que las empresas financieras están en la búsqueda de posibles aplicaciones de la computación cuántica.

Asimismo, en el trabajo realizado por López Chamorro (2024) para el Banco de España se plantea una explicación simplificada del funcionamiento de la computación cuántica en contraposición a la computación clásica, que luego se desarrolla más detalladamente en un apartado técnico. Además, se establecen los usos y ventajas de la computación cuántica, particularmente dentro del ámbito financiero en la modelización estocástica, la optimización y el aprendizaje automático. Por otro lado, se plantea que la computación cuántica enfrenta limitaciones, notablemente la creación de una computadora cuántica de propósito universal, capaz de resolver todo tipo de operaciones y cálculos. Otro punto sobre el que se hace hincapié es el de la seguridad de la información, ante la posibilidad de que se utilicen algoritmos cuánticos para romper los sistemas de encriptación tradicionales. Se señala que, aún si el software necesario para esto todavía no existe, resulta posible almacenar los datos hoy para desencriptarlos una vez que la tecnología lo permita ("Harvest Now, Decrypt Later"), algo que se desarrolla también tanto en el presente reporte como en el documento técnico acompañante.

Adicionalmente, una reciente publicación del Banco de Italia (Andriani et al., 2024) analizó el impacto de la computación cuántica en el sistema financiero, centrándose en sus riesgos y desafíos, particularmente en el ámbito de la ciberseguridad. Se destaca que, si bien la tecnología cuántica aún no ha alcanzado su madurez, su capacidad para romper los sistemas criptográficos actuales representa una amenaza significativa para la seguridad de la información financiera. Ante este riesgo, el informe subraya la necesidad de adoptar estrategias regulatorias y de ciberseguridad a nivel nacional e internacional, promoviendo la transición hacia esquemas criptográficos resistentes a la computación cuántica. También subraya la importancia de la cooperación internacional para definir estándares comunes que faciliten la integración de estas soluciones en las infraestructuras financieras existentes. Finalmente, el documento identifica los principales foros de cooperación global que podrían desempeñar un papel clave en la coordinación de esta transición y en el diseño de estrategias que permitan mitigar los riesgos sin frenar la innovación en el sector.

La Financial Industry Regulatory Authority de EE. UU., por su parte, realizó un informe sobre las implicancias de la computación cuántica para el mercado de valores, incluyendo las aplicaciones más probables dentro de la industria financiera y las posibles amenazas a la ciberseguridad (FINRA, 2023). Para esta investigación se interactuó con más de 20 partes interesadas, incluyendo instituciones financieras, proveedores de hardware y software de computación cuántica, académicos, observadores de la industria, entidades gubernamentales, especialistas en seguridad y organizaciones comerciales. El documento ofrece una visión general breve de la computación cuántica, destacando ciertos principios básicos; identifica y analiza las posibles aplicaciones de la computación cuántica que la industria de valores está explorando; aborda las amenazas potenciales a la ciberseguridad que podría plantear la computación cuántica; y realiza algunas potenciales consideraciones regulatorias.

Organismos internacionales

Además, varios organismos internacionales han abordado el tema de la computación cuántica, dando cuenta de su relevancia venidera en el sistema financiero. A continuación, se presentan algunas de las iniciativas más

relevantes del Bank for International Settlements (BIS), el World Economic Forum (WEF) y el Cyber Expert Group (CEG) del G7.

BIS Innovation Hub's Eurosystem Centre – Project Leap

El "Project Leap" es una iniciativa del BIS (2024) que aborda la amenaza que las futuras computadoras cuánticas representan para la estabilidad financiera. Su objetivo principal es preparar a los bancos centrales y al sistema financiero global para una transición hacia la criptografía resistente a la computación cuántica. En la primera fase del proyecto, se probaron protocolos criptográficos post-cuánticos entre dos bancos centrales: el Banco de Francia y el Deutsche Bundesbank. Se implementaron algoritmos de clave pública tradicionales junto con varios algoritmos resistentes a la computación cuántica en un modo de cifrado híbrido, con el objetivo de mantener la confidencialidad de los mensajes intercambiados entre los sistemas informáticos de ambas instituciones. El éxito logrado en esta fase inicial demostró la viabilidad de aplicar nuevos esquemas de cifrados resistentes a la computación cuántica y subrayó la importancia de que los bancos centrales incorporen fases de transición en sus planes de ciberseguridad.

World Economic Forum (WEF)

El WEF se ha mostrado muy activo, con varias publicaciones en los últimos años sobre computación cuántica, donde se destacan las siguientes:

- Quantum computing governance principles (WEF, 2022a).
- State of quantum computing: Building a quantum economy (WEF, 2022b).
- Transitioning to a quantum-secure economy (WEF, 2022c).
- Quantum readiness toolkit: Building a quantum-secure economy (WEF, 2023)
- Quantum economy blueprint (WEF, 2024a).
- Quantum security for the financial sector: Informing global regulatory approaches (WEF, 2024b).

Estas publicaciones ofrecen una revisión profunda de la computación cuántica y su impacto potencial en diversos sectores, así como en fomentar la colaboración internacional para su desarrollo responsable y equitativo. En particular, en WEF (2024b) se ofrece una hoja de ruta para la transición hacia una economía segura en un contexto cuántico. De forma muy resumida, se detallan las cuatro fases descritas con sus respectivas consideraciones claves:

1. **Preparar**
    a. Concientizar.
    b. Entender estado actual.
    c. Construir capacidades internas.
2. **Clarificar**
    a. Acordar intercambios y colaboración.
    b. Identificar regulación existente.
    c. Entender costos y complejidades de la transición.
3. **Guiar**
    a. Resolver vacíos regulatorios.
    b. Redactar estándares técnicos.

4. **Transitar y Monitorear**
    a. Modernizar y agilizar la administración de la criptografía.
    b. Desarrollo iterativo de la regulación.

G7 Cyber Expert Group (CEG)

El CEG del G7 publicó en setiembre de 2024 un comunicado sobre las oportunidades y riesgos de la computación cuántica para el sistema financiero (U.S. Department of Treasury, 2024). Allí se describió como, si bien esta tecnología promete beneficios como la optimización de operaciones financieras y una mayor eficiencia en el procesamiento de pagos, también introduce riesgos significativos, especialmente en relación con la criptografía de clave pública que protege las comunicaciones digitales y los sistemas de TI.

Para mitigar estos riesgos, el CEG recomendó en dicho comunicado que las entidades financieras:

1. Desarrollen una comprensión profunda de la computación cuántica, los riesgos asociados y las estrategias para mitigarlos. Esto incluye colaborar con proveedores, terceros y expertos en la materia para mantenerse actualizados sobre los avances tecnológicos y las amenazas emergentes.
2. Evalúen los riesgos específicos que la computación cuántica representa para sus áreas de responsabilidad, identificando datos críticos y tecnologías criptográficas en uso que podrían ser vulnerables.
3. Elaboren un plan para mitigar estos riesgos, estableciendo procesos de gobernanza, identificando a los principales actores involucrados y definiendo hitos clave para la implementación de tecnologías resistentes a la computación cuántica.

Asimismo, el CEG enfatizó la importancia de la coordinación internacional para evitar brechas regulatorias y asimetrías entre las jurisdicciones del G7.

Discusión

Como se expuso en los capítulos anteriores, el impacto de la computación cuántica en la ciberseguridad varía según el tipo de criptografía utilizada.

Si bien la criptografía simétrica se ve afectada, su impacto puede ser mitigado de manera eficaz mediante el incremento del tamaño de las claves. En particular, duplicar la longitud de las claves permite mantener un nivel de seguridad robusto frente a ataques basados en algoritmos cuánticos, como el de Grover. En contraste, la criptografía asimétrica se ve gravemente comprometida ante el avance de la computación cuántica, debido a la capacidad del Algoritmo de Shor para factorizar números enteros y calcular logaritmos discretos en tiempos razonables. Esto implica la vulnerabilidad de sistemas criptográficos ampliamente utilizados en la actualidad.

Para enfrentar los desafíos planteados, es imprescindible diseñar nuevos estándares criptográficos resistentes a la computación cuántica, implementar estas soluciones en sistemas tecnológicos, garantizando compatibilidad con las infraestructuras existentes, y realizar una migración integral hacia estos nuevos estándares, asegurando que los recursos tecnológicos y los sistemas críticos adopten estas medidas de seguridad antes de que la computación cuántica sea lo suficientemente avanzada como para constituir una amenaza real. Este enfoque permite garantizar la continuidad de la seguridad cibernética en un escenario post-cuántico.

Impacto de la computación cuántica en el mercado financiero y de pagos

La criptografía no solo protege la seguridad de los usuarios en internet, sino que también es utilizada en sectores críticos como finanzas, salud, telecomunicaciones, comercio electrónico, sistemas gubernamentales y educación, entre otros.

Un ejemplo de afectación pueden ser las comunicaciones cifradas de gobiernos y fuerzas de seguridad, las cuales podrían ser interceptadas, lo que comprometería información clasificada y podría afectar la seguridad nacional. Por otro lado, los datos de salud, protegidos por estrictas normativas en cada país, podrían quedar expuestos, afectando la privacidad de los pacientes y la integridad de los sistemas hospitalarios. A su vez, universidades y centros de investigación nacionales podrían ver comprometidos datos críticos, como estudios científicos o patentes en proceso. Además, infraestructuras críticas como la red eléctrica, sistemas de distribución de agua y redes de telecomunicaciones dependen de la ciberseguridad para operar de manera confiable, y ya han sido blanco de ataques cibernéticos de relevancia en el pasado, por lo que la computación cuántica podría poner en jaque a estos servicios.

En lo que respecta al sistema financiero y de pagos, los sistemas de autenticación y cifrado que protegen las transacciones digitales podrían volverse inseguros, lo que expondría a las instituciones financieras y sus clientes a robos masivos y fraudes. Adicionalmente, sistemas como las tarjetas de crédito, pasarelas de pago y los activos virtuales financieros dependen de criptografía para asegurar las transacciones. La computación cuántica podría hacer vulnerables estos mecanismos, generando pérdidas económicas significativas.

A continuación, se desarrolla en mayor detalle el impacto en las actividades financieras de los mercados.

Activos virtuales

Los activos virtuales, también conocidos como criptoactivos, son representaciones digitales de valor o derechos contractuales que pueden almacenarse, transferirse y negociarse electrónicamente mediante tecnologías de registros distribuidos o similares.

Cuando estos derechos tienen naturaleza financiera, como en el caso de derechos de crédito o inversión, el activo virtual se considera un instrumento financiero que emplea una nueva tecnología subyacente para su registro. Un ejemplo de ello son los valores negociables. A nivel internacional, existen numerosos casos de emisión de bonos utilizando redes públicas como Ethereum para su registro y gestión.

Por otro lado, los activos virtuales más extendidos, como Bitcoin o Ethereum, han experimentado un crecimiento significativo en los mercados y suelen utilizarse como instrumentos de inversión especulativa, aunque no representan derechos de naturaleza financiera.

La mayoría de los activos virtuales, en especial los basados en redes públicas Bitcoin y Ethereum, utilizan criptografía basada en algoritmos de clave pública como RSA y ECDSA, y hashing como SHA-256 (Aggarwal et al., 2018). Estos algoritmos son considerados seguros contra los ataques de las computadoras clásicas, pero podrían ser vulnerables ante computadoras cuánticas como fue mencionado previamente.

Algoritmos cuánticos como el de Shor podrían comprometer la seguridad de las claves privadas, lo que permitiría a un atacante derivar claves privadas a partir de claves públicas y robar fondos. Esto afectaría tanto

a las transacciones actuales como a las futuras, dado que muchas direcciones públicas en cadenas de bloques (blockchain) están expuestas debido al diseño de las transacciones.

Por lo tanto, para garantizar la resistencia cuántica, las redes blockchain necesitarían cambios sustanciales, por ejemplo, migrar a sistemas de clave pública post-cuántica (donde ya existe investigación académica, ver Allende et al. (2023)). Esto requiere hard forks[8], que implican coordinación y aceptación de la comunidad (Holmes y Chen, 2021).

En lo que respecta a la creación de nuevos bitcoins, el proceso de minería implica la búsqueda iterativa de un valor que, al ser procesado mediante una función hash aplicada a la información del bloque, cumpla con los requisitos de dificultad definidos por el protocolo de Bitcoin. Los mineros llevan a cabo numerosos intentos, probando diferentes valores (conocidos como "nonces") hasta encontrar uno que genere un hash con la cantidad necesaria de ceros iniciales. Una vez hallado dicho valor, el bloque se valida y se añade a la cadena, recompensando al minero con nuevos bitcoins y las tarifas de transacción correspondientes.

El algoritmo de Grover permite una aceleración cuadrática para realizar ataques de pre-imagen en SHA-2 y SHA-3. No obstante, existen dudas sobre su efectividad para vulnerar el proceso de minería de bitcoins (Amy et al., 2016; Kearney y Pérez-Delgado, 2021), dado que el conjunto de preimágenes posibles es extremadamente amplio (aunque finito, resulta prácticamente inabarcable en la práctica), lo que limita el impacto real de la aceleración cuántica.

Cabe destacar, que además de lo inherente a la tecnología de blockchain, los restantes componentes de la infraestructura tecnológica necesaria para operar con criptomonedas, desde los servidores de exchanges hasta las aplicaciones de usuario, deberán también migrar su criptografía a una resistente a la computación cuántica.

Infraestructura de pagos

La computación cuántica tendrá un impacto significativo en la infraestructura de pagos, tanto a escala nacional como internacional. Como será detallado a continuación, surgen riesgos en torno a los dispositivos utilizados, la generación fidedigna de información sobre los pagos, y para la comunicación de esta información entre los agentes. Sin embargo, es importante destacar que una migración a la criptografía resistente a la computación cuántica no quita que se deba continuar reforzando el sistema de pagos con controles relacionados a la autenticación reforzada, la notificación a las partes sobre transacciones realizadas, el monitoreo de pagos para detectar actividad sospechosa, entre otros. La criptografía resistente a la computación cuántica es sólo un elemento más utilizado para proteger a todas las partes en las actividades de pagos.

Comunicaciones seguras cliente-servidor

Un punto relevante a destacar es el hecho de que la seguridad en internet a nivel general viene dada de la mano de criptografía asimétrica con el uso de la infraestructura de clave pública (PKI), con los certificados digitales (para poder establecer sesiones https), los emisores de certificados digitales, y demás participantes. Toda esta infraestructura deberá ser actualizada a una criptografía post-cuántica para que utilizar internet sea seguro, más allá del uso que se le pueda dar en el sistema financiero y de pagos, por ejemplo, para la

[8] Un hard fork es una bifurcación de la blockchain que introduce cambios irreversibles en el protocolo, creando una nueva cadena incompatible con la anterior.

interacción entre clientes y entidades financieras. Varios proveedores de estos servicios se encuentran avanzados en las implementaciones[9].

Tarjetas de crédito y débito

Las especificaciones EMV[10] (a cargo del cuerpo técnico internacional EMVCo) son un estándar global para el funcionamiento seguro de las tarjetas de crédito y débito en transacciones presenciales, tanto en terminales de punto de venta (POS) como en cajeros automáticos (ATM). Este protocolo es utilizado por las principales redes de pago (Visa, Mastercard, American Express, entre otras) y ha sido adoptado en la mayoría de los países para mejorar la seguridad en los pagos electrónicos.

Sin embargo, dado que la seguridad de las transacciones con tarjetas de crédito y débito allí establecida se basa en una combinación de criptografía simétrica y asimétrica que, como fue detallado previamente, pasaría a ser vulnerable y en algunos casos quedaría hasta obsoleta, serán necesarias actualizaciones al protocolo.

Por ejemplo, tanto en modalidad de pago con chip como en pagos sin contacto, se utiliza criptografía asimétrica en el proceso de autenticación de la tarjeta, en los certificados EMV, y en la firma digital de los datos transaccionales, entre otros, la cual se considera totalmente insegura una vez que se masifique la computación cuántica. También esta criptografía es utilizada al momento en que los POS se autentican en las redes mediante certificados digitales (lo cual podría terminar en ataques de suplantación de identidad de estos dispositivos).

Por otro lado, la comunicación entre la tarjeta, el POS y la red de pagos se realiza de manera segura en la actualidad a través de criptografía simétrica, la cual fue comentado que es vulnerable pero fácilmente robustecida para mitigar la amenaza cuántica. De todos modos, cabe destacar que muchos dispositivos aun utilizan versiones menos robustas del algoritmo AES o utilizan el algoritmo 3DES dado el bajo poder de cómputo que tienen, por lo que, en esos casos, sí sería necesaria una transición más compleja a dispositivos e instrumentos con mayor capacidad de procesamiento y funcionalidades más robustas.

Por último, el uso de tarjetas a través de billeteras digitales como Google Pay y Apple Pay también se vería afectado, dado que para los procesos de tokenización de tarjetas, la identificación y autenticación de dispositivos y usuarios, y el procesamiento de las transacciones, se utiliza criptografía tanto simétrica como asimétrica, dependiendo el caso, por lo que será necesario que los proveedores de estas billeteras digitales actualicen sus sistemas y aplicaciones incorporando criptografía post-cuántica en cuanto esté disponible.

Pagos con códigos QR

Los pagos con códigos QR se encontrarían afectados por los mismos riesgos comentados previamente para las tarjetas, dado que comparten en buena medida su infraestructura, por ejemplo, los POS si los QR se generan de manera dinámica, y la manera en que la información se transmite entre participantes, a través de redes de comunicación que utilizan criptografía vulnerable a la computación cuántica.

El proceso en sí de generación de un código QR, codificando ciertos datos en una matriz de puntos binaria, no se vería afectado. No obstante, si el dispositivo con el cuál se generasen dichos QR fuese vulnerable, por ejemplo, un POS que no ha sido actualizado, estos códigos dejarían de ser confiables dado que su autenticidad e integridad se verían afectados.

[9] https://pkic.org/pqccm/
[10] www.emvco.com

Asimismo, como se menciona previamente, la comunicación de estos pagos entre dispositivos -ya sea el celular con el cual se escanea el código, el servidor al cual se comunica la aplicación, y todo otro servidor y dispositivo involucrado en el flujo del pago entre agentes participantes establecido para la jurisdicción- deberá ser actualizada para que utilice los nuevos estándares criptográficos en desarrollo resistentes a la computación cuántica. De lo contrario, esta comunicación de información podría ser accedida por terceros, develándole la información de los pagos efectuados.

En la misma línea, toda información relacionada a pagos que se almacene por algún participante que contenga datos sensibles de los compradores o los comercios, deberá ser llevada a cabo a través de criptografía resistente para que, en caso de que dicha información sea accedida por actores no autorizados, no pueda ser desencriptada y utilizada por estos con fines fraudulentos.

Transferencias

En relación a las transferencias, ya sean persona a persona, persona a comercio, persona a gobierno, o cualquiera otra combinación, en su modalidad inmediata o no, se deberán tomar recaudos en la misma línea que lo comentado previamente en lo que respecta a la actualización criptográfica para las actividades de comunicación de estas operaciones entre los participantes involucrados, desde el ordenante al destinatario de estas transferencias, hasta los agentes del sistema que hacen posible la operativa, al igual que para su almacenamiento. Esto incluye a quienes hagan de cámaras compensadoras y a los liquidadores finales, además de los reguladores que participen de esta infraestructura.

Pagos transfronterizos

Los pagos transfronterizos pueden verse afectados por la computación cuántica con un grado mayor de complejidad que los pagos nacionales.

Las transferencias bancarias internacionales se efectúan a través de plataformas de mensajería, como SWIFT, que deberán actualizar sus protocolos criptográficos para hacer frente a las nuevas amenazas. Este proceso involucrará tanto a bancos comerciales como a bancos centrales, quienes serán responsables de actualizar sus versiones de estas plataformas una vez que el proveedor ofrezca soluciones adecuadas. Asimismo, estas plataformas suelen requerir un entorno tecnológico y físico seguro para la operativa de pagos, en particular SWIFT con su CSP Programme, por lo que las actualizaciones y robustecimientos tecnológicos que deberán hacer los participantes pueden involucrar cambios que van mucho más allá de simplemente actualizar la versión de estas plataformas para mensajería de pagos.

Por otro lado, en distintas jurisdicciones pueden existir desarrollos para pagos transfronterizos de menor valor, los que requerirán la estandarización tecnológica entre países participantes, por lo que la actualización tecnológica que se dé al realizar la transición a una criptografía resistente a la computación cuántica deberá ser un esfuerzo coordinado y acordado entre estos países.

Por último, los pilotos y proyectos para pagos llevados a cabo utilizando tecnologías de blockchain, deberán ser revisados para actualizar los componentes que pasarían a ser vulnerables, como se menciona previamente en el apartado de activos virtuales.

Finanzas abiertas

Las iniciativas de banca y finanzas abiertas han venido desplegándose ampliamente en todo el mundo. Básicamente, se trata de que terceras partes puedan acceder o actualizar información bancaria o financiera de los consumidores a través de mecanismos automatizados, seguros y estandarizados, con los debidos consentimientos y autorizaciones.

La manera más utilizada para implementar esta operativa desde el punto de vista tecnológico es a través del uso de interfaces de programación de aplicaciones (APIs). Este soporte tecnológico también se verá afectado por la computación cuántica, como se comenta a continuación.

Por un lado, la identificación, autenticación y autorización frente a las APIs se hace mediante protocolos como OpenID y OAuth 2.0, estándares como JWT, la utilización de API Keys, y recursos como las firmas digitales y tokens. Toda esta tecnología que permite el intercambio seguro de información mediante APIs deberá ser actualizada para pasar a utilizar criptografía post-cuántica.

El acceso a estas APIs se realiza mediante conexiones https sobre internet, las cuales, como fue comentado previamente, requerirán utilizar nuevos algoritmos criptográficos resistentes a la computación cuántica.

Por otro lado, la integridad de los mensajes que fluyen hacia y desde las APIs, suelen incluir criptografía para validar la integridad de estos, la cual necesitará ser actualizada también.

Todo este panorama agrega complejidades a la estandarización tecnológica que es necesaria llevar a cabo entre los participantes, dado que requiere que todos estos estén en el mismo nivel de madurez en el uso de criptografía post-cuántica y que puedan coordinarse de manera efectiva las agendas de implementación.

Monedas digitales de Bancos Centrales (Central Bank Digital Currencies, CBDC)

El impacto futuro de la computación cuántica en las CBDC aún es incierto, ya que la mayoría de los proyectos están en fase de desarrollo y el diseño final diferirá según cada país. Sin embargo, dado que las CBDC dependerán de infraestructuras digitales seguras, la posible vulnerabilidad de los sistemas criptográficos actuales ante ataques cuánticos representa un desafío. Si se basan en tecnología de blockchain, podrían verse afectadas por la vulnerabilidad de las claves privadas y los modelos de consenso. En sistemas centralizados, el riesgo recaería en la seguridad de la autenticación y el cifrado de las transacciones. Más allá de estas alternativas, cabe destacar que, si se implementan esquemas basados en criptografía tradicional, podrían requerir futuras actualizaciones a algoritmos post-cuánticos para garantizar su seguridad y resiliencia a largo plazo. No obstante, hasta que se establezca un modelo específico de CBDC, no pueden hacerse afirmaciones concretas sobre el riesgo exacto que la computación cuántica podría representar.

Autenticación reforzada de clientes

La autenticación reforzada y los sistemas de autenticación multifactor (MFA, por sus siglas en inglés) son pilares fundamentales en la seguridad digital. Estos sistemas combinan múltiples capas de autenticación para verificar la identidad de los usuarios y proteger el acceso a recursos sensibles. Estos sistemas MFA se basan en la combinación de tres categorías de factores de autenticación:

- Algo que el usuario sabe (conocimiento): contraseñas, PINs, preguntas de seguridad.
- Algo que el usuario tiene (posesión): tokens físicos, dispositivos móviles, tarjetas inteligentes.

- Algo que el usuario es (biometría): huellas dactilares, reconocimiento facial, escaneo de iris.

Las contraseñas siguen siendo el factor de autenticación más común, pero también el más vulnerable. Actualmente, su seguridad se basa en la dificultad computacional de adivinar o descifrar contraseñas en ataques de fuerza bruta o por diccionario. Sin embargo, el Algoritmo de Grover podría ser usado para reducir a la mitad el orden de complejidad de un ataque de fuerza. Por lo tanto, se recomienda utilizar contraseñas más largas, usar funciones de hash más robustas frente a la computación cuántica, y fomentar la autenticación sin contraseñas (passwordless).

Por su parte, los sistemas que utilizan tokens físicos, tarjetas inteligentes y claves criptográficas dependen de algoritmos de cifrado para generar y validar credenciales, los cuales están basados en criptografía asimétrica vulnerable. Consecuentemente, para proteger la autenticación basada en posesión, es necesario migrar a tokens físicos resistentes a la computación cuántica, como aquellos basados en esquemas post-cuánticos, y usar métodos de autenticación con múltiples dispositivos, combinando factores físicos con otros mecanismos resistentes a ataques cuánticos.

Asimismo, la autenticación biométrica es ampliamente utilizada en dispositivos móviles y sistemas de seguridad de alto nivel. Sin embargo, su seguridad depende de la integridad de los datos biométricos almacenados y de los algoritmos utilizados para su procesamiento. La computación cuántica podría acelerar los ataques de reconstrucción de datos biométricos a partir de huellas parciales o imágenes capturadas. Además, si los datos biométricos están protegidos por cifrado basado en criptografía asimétrica, se vuelven vulnerables al Algoritmo de Shor, por ejemplo. Por lo tanto, también se vuelve necesario actualizar los algoritmos de cifrado utilizados.

Finalmente, cabe mencionar la criticidad de la seguridad en los datos biométricos almacenados, ya que, a diferencia de las contraseñas y los restantes factores, estos no pueden ser modificados por el usuario en caso de una vulneración. Si terceros acceden a esta información, el compromiso de seguridad es irreversible.

El caso de las contraseñas de un solo uso

Los One-Time Passwords (OTPs) son una medida de seguridad ampliamente utilizada en autenticación multifactor, acceso seguro a sistemas y transacciones bancarias en línea. Generalmente, los OTPs se generan mediante algoritmos criptográficos basados en secretos compartidos, sincronización temporal o generación aleatoria.

Los OTPs basados en hash, como los Time-Based One-Time Passwords (TOTP) y los HMAC-Based One-Time Passwords (HOTP), dependen de funciones hash criptográficas como SHA-1, SHA-256 o SHA-512, por lo que verían su robustez reducida por el Algoritmo de Grover. Por lo tanto, para mantener niveles de seguridad equivalentes, la longitud de las funciones hash utilizadas en OTPs debería duplicarse.

Por otro lado, algunos sistemas de autenticación utilizan OTPs generados mediante firmas digitales o esquemas criptográficos asimétricos, como RSA o ECC, para la verificación de identidad. Dado que la criptografía asimétrica se vuelve vulnerable con la irrupción de la computación cuántica, para contrarrestar este riesgo, los sistemas que dependen de esquemas asimétricos para la autenticación con OTPs deberán migrar hacia algoritmos post-cuánticos, como los propuestos por el NIST que se detallarán más adelante.

Finalmente, la mayoría de OTPs dependen en gran medida de la aleatoriedad en su generación. Si un atacante puede predecir el valor del OTP antes de su uso (por ejemplo, gracias a la computación cuántica), la seguridad del sistema colapsa. Por lo tanto, se recomienda el uso de generadores de números cuánticos verdaderamente

aleatorios que aprovechan principios de mecánica cuántica para garantizar una aleatoriedad genuina e impredecible[11].

También es importante destacar que la computación cuántica podría afectar la seguridad de los canales de transmisión de OTPs. En particular, los sistemas que dependen de canales inseguros (como SMS o correo electrónico) podrían verse expuestos a ataques más sofisticados de suplantación de identidad. Por lo tanto, se recomienda el uso de canales cifrados con criptografía post-cuántica, autenticación basada en hardware seguro (tokens físicos resistentes a ataques cuánticos) y autenticación multifactor con, por ejemplo, biometría avanzada.

Estándares Utilizados en el Sistema Financiero y de Pagos

El impacto de la computación cuántica en los estándares de tecnología y ciberseguridad está siendo objeto de revisión por varias organizaciones internacionales. Por ejemplo, la versión 4.0 de PCI DSS, publicada en marzo de 2022, introduce el requisito 12.3.3, que establece la necesidad de implementar procesos mejorados de gestión de criptografía para principios de 2025.

Por su parte, SWIFT y su Customer Security Programme[12] exigido a entidades financieras y reguladores podría pasar a contener requerimientos referidos a la criptografía post-cuántica, como fue mencionado previamente cuando se elaboró sobre los pagos transfronterizos.

Por otro lado, otros estándares como la familia ISO 27.000 podrían llegar a actualizarse de igual manera. Como fue mencionado previamente, el NIST está trabajando fuertemente en líneas de acción referidas a la computación cuántica, por lo que su Cybersecurity Framework (CSF) es de esperar que vea cambios.

Por lo tanto, se recomienda seguir de cerca el avance y cambios en estos estándares de uso en los participantes del mercado, incluyendo al regulador, con el fin de poder estar alineados y preparados al momento de implementarlos en la gestión.

Basilea III

Basilea III, establecido por el Comité de Supervisión Bancaria de Basilea (BCBS), busca fortalecer la regulación, supervisión y gestión de riesgos en el sector bancario global. Sus principios fundamentales están orientados a mejorar la capacidad de los bancos para absorber shocks derivados de crisis financieras y económicas, reducir el riesgo de contagio entre instituciones financieras y mejorar la transparencia del sistema financiero. Sin embargo, la llegada de la computación cuántica plantea desafíos significativos para la resiliencia y seguridad de los sistemas bancarios que operan bajo este marco.

Desde el punto de vista del Riesgo Operativo, las herramientas actuales de monitoreo y prevención de fraudes podrían quedar obsoletas frente a la capacidad de una computadora cuántica, además de la potencial afectación de sistemas financieros críticos o interrupciones masivas en las operaciones bancarias.

[11] Mayor detalle en documento técnico acompañante.

[12] www.swift.com/myswift/customer-security-programme-csp

Por lo tanto, podría ser factible que se requiera una actualización de los estándares de resiliencia operacional para incluir pruebas de resistencia frente a amenazas cuánticas, y requerimientos de planes de migración hacia tecnologías cuántico-resistentes en los sistemas centrales de los bancos.

Otras tecnologías utilizadas en el sistema financiero

Computación en la nube

La computación cuántica también representa una amenaza significativa para la computación en la nube, ya que ésta depende en gran medida de la criptografía para la protección de datos durante su almacenamiento, transmisión y procesamiento.

Por lo tanto, los reguladores financieros deberán exigir a sus supervisados que, cuanto antes, empiecen a utilizar proveedores de servicios en la nube que cuenten con criptografía post-cuántica, según estos vayan migrando su infraestructura y ofreciendo estas nuevas capacidades.

Identidad Digital y Firma Electrónica Avanzada

Ya que estas tecnologías dependen en gran medida de la criptografía asimétrica y los algoritmos de hashing para garantizar la seguridad, autenticidad e integridad de los datos y las transacciones, la computación cuántica también plantea riesgos en este ecosistema.

Tal y como se ha comentado, el algoritmo de Shor permitiría a un atacante descifrar las claves privadas vinculadas a los certificados digitales, comprometiendo así la integridad de las firmas electrónicas avanzadas. Esto facilitaría la falsificación de una firma electrónica en un documento; sin embargo, modificar inadvertidamente un documento firmado seguiría siendo inviable, ya que cualquier alteración alteraría su hash y lo haría detectable.

Dado que en nuestra jurisdicción se aceptan las firmas electrónicas avanzadas como equivalentes legales a las firmas manuscritas certificadas por un escribano público, la falsificación de éstas podría tener consecuencias legales y financieras significativas.

Pero más allá de eso, toda la infraestructura de clave pública (PKI) sería vulnerable, donde certificados digitales falsificados podrían permitir la suplantación de identidades en sistemas de identificación digital y transacciones electrónicas, y la confianza en las autoridades certificadoras se vería perdida.

Finalmente, dado que en la regulación bancocentralista se acepta esta infraestructura para el contacto no presencial de clientes y respectivos acuerdos entre las partes, se entiende necesario plantear la actualización urgente de esta infraestructura nacional cuando los algoritmos criptográficos resistentes se encuentren disponibles.

Iniciativas destacadas a nivel global

Es importante destacar que distintas jurisdicciones y organizaciones internacionales han incluido a la computación cuántica en sus agendas, muchas veces buscando ponerse a la vanguardia, y proponiendo varias iniciativas para aprovechar las oportunidades que la tecnología ofrece y mitigar los riesgos inminentes asociados. A continuación, se presentan algunas de estas iniciativas destacadas.

Internacionales

IYQ - Quantum 2025

A nivel global, la iniciativa IYQ[13] (International Year of Quantum Science & Technology) promovida por la UNESCO para el año 2025 busca aprovechar los 100 años de la mecánica cuántica para generar concientización sobre las ciencias y tecnologías cuánticas y su impacto en la sociedad.

En ese sentido, entre sus fines principales tiene servir de vitrina para eventos relacionados a la cuántica que se organicen en este año. Al momento de realizar este reporte, se concentraban cerca de 200 instancias de difusión sobre la temática.

Organización del Tratado del Atlántico Norte

La OTAN reconoce la relevancia estratégica de las tecnologías cuánticas, incluyendo la computación cuántica, y ha emprendido diversas iniciativas para explorar y aprovechar su potencial en el ámbito de la defensa y la seguridad.

Entre otras iniciativas, ha lanzado el Acelerador para la Innovación en Defensa del Norte (DIANA, por sus siglas en inglés) en el 2021, cuyo objetivo es acelerar la adopción de tecnologías emergentes y disruptivas, entre las cuales se incluyen la inteligencia artificial, la biotecnología y la computación cuántica. En el marco de DIANA, se ha establecido un nuevo centro dedicado a la tecnología cuántica en Copenhague, Dinamarca[14]. Este centro se enfocará en la investigación y desarrollo de tecnologías cuánticas, incluyendo la computación cuántica, con aplicaciones potenciales en defensa y seguridad.

Estados Unidos

Casa Blanca

El Memorando de Seguridad Nacional sobre la "Promoción del Liderazgo de Estados Unidos en Computación Cuántica mientras se Mitigan los Riesgos para los Sistemas Criptográficos Vulnerables" (NSM-10), emitido el 4 de mayo de 2022, establece la política para equilibrar las oportunidades y riesgos asociados con la computación cuántica (The White House, 2022). Sus objetivos principales son mantener el liderazgo en ciencias de la información cuántica, y mitigar los riesgos de las computadoras cuánticas para la seguridad cibernética.

Las acciones establecidas en el memorando incluían que las agencias identificasen y catalogasen los sistemas que utilizaran criptografía susceptible a ataques de computadoras cuánticas, y que se desarrollasen planes para migrar a algoritmos criptográficos seguros frente a las capacidades de futuras computadoras cuánticas.

Departamento de Seguridad Nacional

En octubre del 2021, el Departamento de Seguridad Nacional de los Estados Unidos (DHS, por sus siglas en inglés) estableció una hoja de ruta con el fin de apoyar a las organizaciones en su preparación de la transición hacia la criptografía post-cuántica (Department of Homeland Security, 2021).

[13] https://quantum2025.org/
[14] https://dianaq.ku.dk/

Esta hoja de ruta planteaba los siguientes siete pasos:

1. Interactuar con los organismos encargados de generar estándares para estar al tanto de las nuevas publicaciones.
2. Crear un inventario de datos críticos, que podrían verse vulnerados al estar disponible la computación cuántica.
3. Crear un inventario de tecnologías criptográficas utilizadas en sus sistemas, para facilitar la transición a criptografía resistente.
4. Identificar todo estándar interno relacionado a ciberseguridad, datos y adquisiciones, que requiera ser actualizado.
5. Identificar todo uso de criptografía de clave pública en la organización y marcarla como vulnerable.
6. Priorizar los sistemas informáticos utilizados en la organización para llevar a cabo la transición criptográfica, tomando en cuenta la criticidad y sensibilidad de cada sistema y la información tratada.
7. En base a los insumos creados en los pasos previos, generar un plan para la transición de sus sistemas en cuanto los estándares de criptografía post-cuántica estén disponibles.

Asimismo, se planteaban los siguientes hitos en su agenda:

- 2021-2023: Inventario y priorización de sistemas.
- 2024: Publicación de estándares de criptografía post-cuántica.
- 2024-2030: Transición hacia sistemas resistentes a la computación cuántica.
- 2030: Computación cuántica con posibilidades de quebrar la criptografía actual potencialmente disponible.

Agencia de Seguridad de Infraestructura y Ciberseguridad

La Iniciativa de Criptografía Post-Cuántica de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de Estados Unidos se estableció para abordar las amenazas emergentes que la computación cuántica representa para los sistemas criptográficos actuales (CISA, 2022).

Esta iniciativa cuenta con los siguientes objetivos principales:

- **Evaluación de Riesgos:**
  - Analizar la vulnerabilidad de las infraestructuras críticas de EE. UU. frente a las capacidades futuras de la computación cuántica.
  - Identificar funciones críticas nacionales que podrían verse afectadas y priorizar acciones de mitigación.
- **Planificación Estratégica:**
  - Desarrollar planes para enfocar recursos y colaboraciones con operadores de infraestructuras críticas en los sectores público y privado.
  - Establecer hojas de ruta para la transición a estándares criptográficos resistentes a la computación cuántica.
- **Políticas y Estándares:**
  - Colaborar con socios para fomentar la adopción de políticas y estándares que mejoren la seguridad de las redes gubernamentales y de infraestructuras críticas.
  - Apoyar los esfuerzos del Instituto Nacional de Estándares y Tecnología (NIST) en la estandarización de algoritmos post-cuánticos.

- **Compromiso y Concientización:**
  - Involucrar a las partes interesadas para desarrollar planes de mitigación y promover la implementación de nuevos estándares una vez disponibles.
  - Elaborar productos técnicos y guías para facilitar la transición a la criptografía post-cuántica.

Asimismo, se sugieren las siguientes actividades en su hoja de ruta, las cuales tienen bastante en común con las detalladas previamente por parte del DHS:

- **Inventario de tecnología:**
  - Identificar aplicaciones, hardware, dispositivos, etc., que utilizan criptografía de clave pública susceptible a ataques cuánticos.
- **Planificación de la transición:**
  - Desarrollar planes para migrar a algoritmos criptográficos resistentes a la computación cuántica, incluyendo períodos de prueba y considerando la interdependencia de sistemas y la eliminación de tecnologías obsoletas.
- **Políticas de adquisición:**
  - Establecer políticas que aseguren la incorporación de estándares post-cuánticos en futuras adquisiciones tecnológicas, poniendo en conocimiento a proveedores sobre nueva postura.
- **Educación y concientización:**
  - Informar y capacitar al personal sobre la importancia de la transición a la criptografía post-cuántica y los pasos necesarios para su implementación.

Instituto Nacional de Estándares y Tecnología

El Instituto Nacional de Estándares y Tecnología (NIST) ha desarrollado una serie de publicaciones para guiar la transición hacia la criptografía post-cuántica con el objetivo de proteger la información digital frente a las amenazas emergentes que representan las futuras computadoras cuánticas.

Por ejemplo, ya en el 2021 publicó el documento “Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms”, el cual describe riesgos y medidas a adoptar como las ya detalladas en este informe (Barker et al., 2021).

Algo más reciente, de fines del 2024, es el documento “Transition to Post-Quantum Cryptography Standards”, el cual detalla el enfoque del NIST para la transición hacia la criptografía post-cuántica, abordando riesgos, estrategias de implementación y estándares emergentes (Moody et al., 2024). Explica la necesidad de migrar desde algoritmos vulnerables, destaca la adopción de firmas digitales post-cuánticas, el enfoque híbrido, y discute desafíos técnicos en la implementación. Además, proporciona recomendaciones para organizaciones sobre planificación y pruebas de interoperabilidad.

Proyecto “Migration to Post-Quantum Cryptography”

A través del Centro Nacional de Excelencia en Ciberseguridad (NCCoE), NIST ha venido desarrollando este proyecto[15]. Este esfuerzo complementa las actividades de estandarización de criptografía post-cuántica del

[15] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

instituto, con el fin de facilitar la transición desde los algoritmos criptográficos de clave pública actuales a aquellos resistentes a ataques basados en computadoras cuánticas

El objetivo del proyecto consiste en desarrollar prácticas sistemáticas que faciliten la migración a algoritmos criptográficos resistentes a ataques cuánticos, materializadas en forma de documentos técnicos, guías e implementaciones. Todo esto, realizado de manera colaborativa junto a referentes de la industria.

Estandarización de algoritmos de criptografía post-cuántica

El NIST ha estandarizado recientemente varios algoritmos de criptografía post-cuántica. El llamado a postulaciones de algoritmos para ser estandarizados comenzó en 2016, con el fin de que las propuestas pudieran ser evaluadas y vulneradas, de ser posible, por expertos. El objetivo primordial es suplantar los algoritmos vulnerables de la criptografía asimétrica. Han sido seleccionado cuatro algoritmos de 69 inicialmente postulados. A continuación, se detallan los estandarizados:

- **ML-KEM (Módulo-Lattice-Based Key-Encapsulation Mechanism) (NIST, 2024a):**
  - Basado en el algoritmo CRYSTALS-Kyber[16].
  - Proporciona un mecanismo de encapsulación de claves seguro, esencial para el cifrado de datos y el establecimiento de claves compartidas entre partes.
- **ML-DSA (Módulo-Lattice-Based Digital Signature Algorithm) (NIST, 2024b):**
  - Derivado del algoritmo CRYSTALS-Dilithium[17].
  - Ofrece un esquema de firma digital que garantiza la autenticidad e integridad de los mensajes y documentos digitales.
- **SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) (NIST, 2024c):**
  - Basado en el algoritmo SPHINCS+[18].
  - Proporciona un esquema de firma digital sin estado, utilizando funciones hash para garantizar la seguridad. Ofrece una alternativa basada en hash, diversificando las bases matemáticas utilizadas.
- **FN-DSA (FFT over NTRU-Lattice-Based Digital Signature Algorithm)[19]:**
  - Basado en el algoritmo FALCON[20].
  - Proporciona un esquema de firma digital eficiente utilizando transformadas rápidas de Fourier sobre estructuras de retículos.

Agencia de Seguridad Nacional

La Agencia de Seguridad Nacional (NSA) de Estados Unidos ha desarrollado la Suite de Algoritmos de Seguridad Nacional Comercial 2.0 (CNSA 2.0). Los objetivos de la CNSA 2.0 incluyen, implementar algoritmos criptográficos capaces de resistir ataques tanto de computadoras clásicas como cuánticas, y asegurar que los sistemas de seguridad nacional, que manejan información clasificada y son críticos para actividades militares e inteligencia, mantengan su integridad y confidencialidad. Con su adopción, se planea descontinuar el uso de algoritmos como RSA, DH y ECC en los sistemas de seguridad nacional.

[16] https://pq-crystals.org/kyber/index.shtml
[17] https://pq-crystals.org/dilithium/index.shtml
[18] https://sphincs.org/
[19] Estándar no publicado aún, pero que lo será a la brevedad bajo el identificador FIPS 206.
[20] https://falcon-sign.info

Los algoritmos allí establecidos, que incluyen los recientemente estandarizados ML-KEM y ML-DSA, son los siguientes:

- **Cifrado Simétrico:**
  - AES-256: Utiliza claves de 256 bits para cifrado de información.
- **Intercambio de Claves:**
  - ML-KEM: Basado en CRYSTALS-Kyber, con parámetros ML-KEM-1024.
- **Firmas Digitales:**
  - ML-DSA: Basado en CRYSTALS-Dilithium, con parámetros ML-DSA-87.
  - LMS: Para la firma de firmware y software, con SHA256/192 recomendado.
  - XMSS: Otra opción para la firma de firmware y software.
- **Funciones Hash:**
  - SHA-384 y SHA-512: Para la generación de resúmenes criptográficos.

NSA – CISA – NIST

La NSA, la CISA y el NIST han colaborado en la publicación del documento conjunto titulado "Quantum-Readiness: Migration to Post-Quantum Cryptography" del 2023 (CISA et al., 2023).

Este documento tiene como propósito informar a las organizaciones, especialmente aquellas que forman parte de infraestructuras críticas, sobre los impactos potenciales de las capacidades cuánticas emergentes. Además, proporciona recomendaciones para prepararse y planificar la migración hacia estándares de criptografía post-cuántica.

Las recomendaciones establecidas, también en línea con lo previamente detallado en este reporte, son:

- Desarrollar un plan estratégico que guíe la transición hacia la adopción de algoritmos criptográficos resistentes a ataques cuánticos.
- Identificar y documentar todos los sistemas y aplicaciones que dependen de la criptografía de clave pública vulnerable a futuros ataques cuánticos.
- Analizar la dependencia de proveedores y tecnologías que podrían verse afectadas por la transición a los nuevos algoritmos criptográficos, asegurando que estén preparados para soportar algoritmos post-cuánticos.
- Iniciar conversaciones con proveedores para comprender sus planes y capacidades en relación con la implementación de sus nuevas soluciones.
- Realizar evaluaciones de riesgo para priorizar los esfuerzos de migración, enfocándose en los sistemas más críticos y vulnerables.

Europa

Reino Unido

La National Cyber Security Centre (NCSC) del Reino Unido ha adoptado una postura proactiva frente a los desafíos y oportunidades que presenta la computación cuántica en el ámbito de la ciberseguridad.

En relación con los preparativos para la era post-cuántica, al igual que otros organismos, la NCSC aconseja a las organizaciones realizar un inventario detallado de sus sistemas criptográficos actuales para identificar posibles vulnerabilidades frente a futuras amenazas cuánticas. Asimismo, recomienda trabajar estrechamente con especialistas en criptografía y seguridad cuántica para asegurar una transición efectiva. Finalmente, la NCSC sugiere mantenerse al tanto de las actualizaciones en hardware y software que incorporen algoritmos.

Respecto a los algoritmos resistentes a utilizar, esta recomienda ML-KEM-768 y ML-DSA-65 dado sus niveles apropiados de seguridad y eficiencia.

Unión Europea

La Comisión Europea ha emitido una recomendación en abril de 2024, en la cual establece la necesidad de una transición coordinada hacia la criptografía post-cuántica en la Unión Europea (European Commission, 2024). Esta iniciativa responde a los riesgos que la computación cuántica representa para los actuales estándares criptográficos. El documento se fundamenta en el artículo 292 del Tratado de Funcionamiento de la Unión Europea y en la Directiva NIS 2 (2022/2555), que regula la ciberseguridad en la UE.

La recomendación busca alcanzar tres grandes objetivos:

- Definir una hoja de ruta coordinada para la Implementación de la criptografía post-cuántica que permita sincronizar los esfuerzos de los Estados miembros.
- Apoyar la evaluación y selección de algoritmos de criptografía post-cuántica adecuados para la UE.
- Establecer medidas proporcionales y apropiadas para preparar la transición.

Por otro lado, la Declaración Europea sobre Tecnologías Cuánticas, también conocida como "Quantum Declaration[21]", es una iniciativa estratégica de la UE que busca posicionar a Europa como líder mundial en el ámbito de las tecnologías cuánticas. El objetivo último de esta declaración es convertir a Europa en el "valle cuántico" del mundo, es decir, la región líder en excelencia e innovación cuántica. Para lograrlo, se promueve la coordinación de esfuerzos en áreas clave como la investigación, el desarrollo de infraestructuras cuánticas paneuropeas y la aceleración de la transición de los descubrimientos científicos desde el laboratorio al mercado.

De manera paralela, la Quantum Technologies Flagship[22] de la UE es un programa de investigación e innovación a gran escala lanzado en 2018. Con una duración prevista de diez años y un presupuesto de 1.000 millones de euros, esta iniciativa busca consolidar y expandir el liderazgo científico europeo en tecnologías cuánticas, facilitando la transformación de la investigación en aplicaciones comerciales que aprovechen plenamente el potencial disruptivo de estas tecnologías. Tiene cuatro puntos focales, siendo estos la computación cuántica, la simulación cuántica, la comunicación cuántica, y la metrología (sensores) cuántica, los cuales han venido siendo abordados en más de 100 proyectos.

Agencia de la Unión Europea para la Ciberseguridad (ENISA)

ENISA ha publicado dos documentos relevantes sobre criptografía post-cuántica.

El primero de ellos, titulado "Criptografía Post-Cuántica: Estado Actual y Mitigación Cuántica", publicado en mayo de 2021, ofrece un análisis exhaustivo sobre el avance de la estandarización de la criptografía post-

[21] https://digital-strategy.ec.europa.eu/en/policies/quantum
[22] https://qt.eu/

cuántica y las estrategias de mitigación ante las amenazas que plantea la computación cuántica (Beullens et al., 2021). Allí se enfatiza la importancia de que Europa comience a considerar estrategias de mitigación ante las amenazas cuánticas, destacando la necesidad de una transición coordinada hacia la criptografía post-cuántica para salvaguardar la seguridad de las infraestructuras digitales.

El otro documento de interés, titulado "Estudio de Integración de la Criptografía Post-Cuántica" y publicado en octubre de 2022, es una continuación del documento anterior y profundiza en los desafíos y consideraciones para integrar sistemas criptográficos post-cuánticos en los protocolos existentes, así como en el diseño de nuevos protocolos adaptados a estas tecnologías emergentes (ENISA, 2022).

Las recomendaciones clave, que van en líneas a las realizadas por otros organismos, son las siguientes:

- Evaluación de infraestructuras criptográficas en uso.
- Desarrollo de protocolos híbridos, que combinen algoritmos tradicionales con criptografía post-cuántica para ofrecer una transición más segura.
- Participar activamente en iniciativas de estandarización para asegurar que los protocolos desarrollados sean aceptados y compatibles a nivel internacional.
- Formar a los profesionales de la ciberseguridad en las nuevas tecnologías post-cuánticas y en las mejores prácticas para su implementación.

Instituto Europeo de Normas de Telecomunicaciones

El Instituto Europeo de Normas de Telecomunicaciones (ETSI) ha desempeñado un papel fundamental en la promoción y estandarización de tecnologías relacionadas con la computación cuántica y la criptografía le en Europa.

Por ejemplo, estableció un grupo dedicado a la criptografía segura cuántica, enfocado en desarrollar estándares. También ha venido llevando a cabo talleres, conferencias y proyectos sobre la temática. Finalmente, ha publicado normas y documentos técnicos que faciliten la adopción de la computación cuántica en el sector de las telecomunicaciones.

Asia

China

Como fue mencionado previamente, China ha logrado hitos con el desarrollo de computadoras cuánticas como Jiuzhang, basada en fotones, y Zuchongzhi, basada en superconductores, con capacidades que superan a las computadoras clásicas en cálculos específicos. Adicionalmente, ha implementado una de las redes de comunicación cuántica más avanzadas del mundo, con la conexión entre Beijing y Shanghái y el lanzamiento del satélite Micius en 2016, que permitió realizar la primera transmisión de claves cuánticas a nivel global. También el gobierno chino ha invertido miles de millones de dólares en su centro nacional de computación cuántica en Hefei.

En lo que refiere a criptografía post-cuántica, China está siguiendo su propia estandarización de algoritmos[23], independizándose de iniciativas como la del NIST. Intereses de confianza y seguridad nacional pueden entrar

[23] https://www.niccs.org.cn/en/

en juego en estos puntos también, lo cual explica que otros países además hayan elegido el camino de su propia estandarización.

Japón

En Japón, se han dado varios avances a partir de alianzas en la industria. Fujitsu y RIKEN han desarrollado procesadores cuánticos y trabajan en la integración de tecnología cuántica con inteligencia artificial y supercomputación. Por otro lado, NTT y NEC están investigando en redes cuánticas y sistemas de criptografía cuántica para seguridad en las telecomunicaciones. Adicionalmente, Japón es parte del consorcio IBM Quantum Network, el cual busca colaborar en la adopción de sistemas cuánticos en la industria y la academia.

India

En 2020, el gobierno indio lanzó la Misión Nacional de Tecnologías Cuánticas y Aplicaciones, con una inversión millonaria para impulsar la investigación en computación cuántica, criptografía y sensores cuánticos. Por su parte, en la academia, instituciones como el Instituto Tata de Investigación Fundamental y el Instituto Indio de Ciencia están liderando investigaciones en algoritmos cuánticos y seguridad de la información. Además, India está fortaleciendo su ecosistema cuántico con asociaciones estratégicas con gigantes tecnológicos.

Corea del Sur

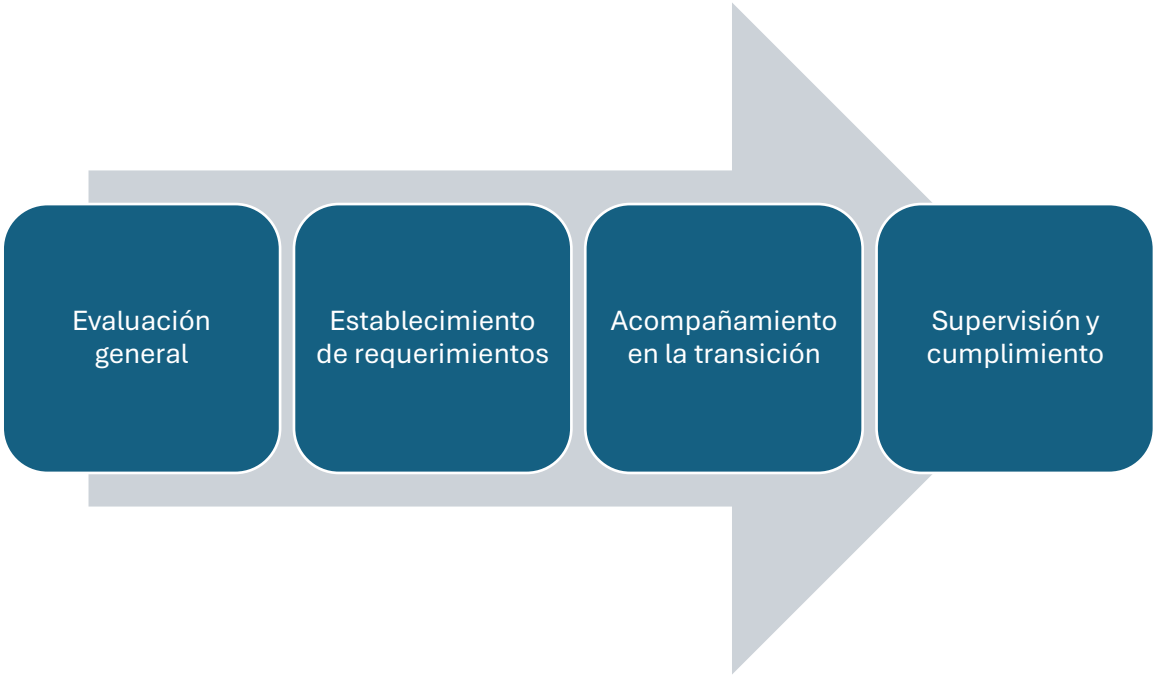
Al igual que otros países, el gobierno surcoreano ha impulsado la creación del Centro Nacional de Computación Cuántica, con una inversión inicial de varios millones para desarrollar tecnología cuántica de hardware y software. Pero también la industria ha incursionado en la computación cuántica. Por ejemplo, empresas como Samsung están investigando el uso de materiales cuánticos para mejorar la eficiencia en dispositivos electrónicos. Por otro lado, SK Telecom ha desarrollado redes de telecomunicaciones basadas en criptografía cuántica, mejorando la seguridad de las infraestructuras de comunicación.

Singapur

Por último, en Singapur se han seguido iniciativas similares a las de otros países de la región. El Quantum Engineering Programme, con una gran inversión, busca desarrollar aplicaciones prácticas de la computación cuántica en ciberseguridad y optimización logística. Del lado de la academia, el Centre for Quantum Technologies, con apoyo de la Universidad Nacional de Singapur, lidera investigaciones en computación y criptografía cuántica. Desde el lado de la industria, el país ha establecido programas de colaboración con tecnológicas internacionales para desarrollar algoritmos cuánticos aplicados a problemas industriales y financieros.

Propuestas de abordaje para una autoridad financiera

A partir del análisis de las implicaciones y riesgos planteados por el desarrollo de la computación cuántica, así como la experiencia y agendas definidas en otras jurisdicciones para su abordaje, a continuación, se propone un enfoque basado en cuatro etapas para una autoridad financiera con el fin de que pueda adaptar el mercado dentro de su perímetro de la manera más efectiva posible.



Evaluación general

En esta etapa, corresponde analizar el posible impacto de la computación cuántica en los sistemas financieros y de pagos, y establecer ámbitos de coordinación con las partes interesadas relevantes. Para ello, se sugieren las siguientes actividades para las autoridades financieras:

- Entender la temática a fondo y su impacto en la operativa financiera de su jurisdicción.
- Identificar estado actual tecnológico y el futuro deseado, es decir, con criptografía resistente a la computación cuántica.
- Identificar el perímetro de acción para dicha autoridad financiera, sus responsabilidades, regulados, y toda otra autoridad que corresponda, parte interesada en general o potencial aliado (como otras agencias o universidades).
- Comunicar claramente a la industria y otras partes interesadas toda información que contribuya a la acción por parte de los actores del mercado, ya sea a través de marcos conceptuales, recomendaciones, etc.
- Promover cambios en la infraestructura digital de su jurisdicción, como la de identificación digital y firma electrónica avanzada.
- Crear ámbitos de trabajo colaborativos con otras autoridades a nivel regional e internacional.

Establecimiento de requerimientos

Una vez comprendido de forma cabal el riesgo al que se está expuesto se recomienda que la autoridad financiera identifique el camino óptimo para la transición a criptografía segura en su jurisdicción, y comience a establecer los requerimientos necesarios, lo cual incluiría las siguientes actividades:

- Concientización del mercado y otras partes interesadas, sobre los riesgos y la transición que es necesaria para asegurar la implantación de mecanismos de control.
- Valoración específica de los riesgos e identificación de áreas prioritarias de actualización en términos, de mercados, infraestructuras, participantes, así como otras variables que se consideren relevantes.
- Requerir a los participantes del mercado una hoja de ruta para la transición a una criptografía segura, la cual deberá incluir los siguientes pasos:
    - Identificar y poner en marcha equipo responsable de la migración, indicando persona responsable de la misma.
    - Evaluar costos y requerimientos para la transición.
    - Generar capacidades para todos los involucrados en la migración.
    - Crear registro luego de un proceso de identificación de datos y tecnologías vulnerables, ya sea software, hardware, base de datos, dispositivos de red, entre otros.
    - Desarrollar un plan de migración con una adecuada priorización de tecnologías e información.
    - Crear un mapa de proveedores críticos tecnológicos, indicando la factibilidad de que estos puedan actualizar los componentes criptográficos de sus productos.
    - Seleccionar algoritmos de criptografía resistente a la computación cuántica y criptografía híbrida a ser utilizados luego de la migración, y actualizar políticas, estándares y protocolos internos con estos nuevos elementos.
    - Llevar a cabo pruebas formales.
- Fijar una fecha límite factible para la finalización de las actividades de transición por parte de la industria.
- Redactar toda normativa y comunicación que se entienda necesaria.

Acompañamiento en la transición

Una vez que la industria se encuentre en el proceso de transición a una criptografía segura, sería beneficioso que la autoridad financiera pueda realizar ciertas actividades en paralelo para aumentar la probabilidad de una migración en tiempo y forma. Para ello, algunas actividades a realizar son las siguientes:

- Seguir de manera continua los avances internacionales en la temática, por ejemplo, el despliegue de nuevos estándares internacionales de algoritmos, la redacción de estándares de ciberseguridad, o actualizaciones en suites de algoritmos como la CNSA 2.0.
- Emitir guías, redacciones, publicaciones, marcos conceptuales o similares que contribuyan al conocimiento y accionar de los agentes del mercado.
- Supervisar y monitorear los progresos en las hojas de ruta de transición de los supervisados, velando en especial por el cumplimiento de sus cadenas de proveedores, requiriendo ajustes cuando se entienda necesario.
- Mantener una postura de intercambio constante con la industria.

Supervisión y cumplimiento

Finalmente, y considerando un futuro a mediano plazo, corresponde evaluar si los participantes del mercado llevaron a cabo una transición efectiva hacia una criptografía segura. En ese sentido, se recomienda incluir las siguientes actividades para la autoridad financiera:

- Capacitar personal de supervisión, para que pueda evaluar adecuadamente el cumplimiento en su totalidad de la transición.
- Supervisar toda entidad regulada que requiera de controles de ciberseguridad respecto a la confidencialidad e integridad de los datos que trate, priorizando aquellas de mayor criticidad en el mercado.
- Generar condiciones para poder detectar el uso de criptografía vulnerable en los supervisados.
- Evaluar factibilidad ante solicitud de prórrogas para la transición.
- Revisar cambios regulatorios necesarios y redactar nueva normativa.

Conclusiones

La computación cuántica representa un cambio de paradigma en el procesamiento de la información, basado en principios fundamentales como la superposición y el entrelazamiento cuántico. A diferencia de la computación clásica, que opera con bits binarios, las computadoras cuánticas utilizan cúbits, lo que les permite realizar cálculos exponencialmente más rápidos en ciertos problemas específicos.

A lo largo de las últimas décadas, la computación cuántica ha evolucionado significativamente, desde los primeros modelos teóricos hasta la implementación de procesadores cuánticos con decenas de cúbits. Gigantes tecnológicos y organismos gubernamentales han invertido en su desarrollo, acelerando la investigación y fomentando aplicaciones prácticas en diversos sectores.

Las aplicaciones de la computación cuántica en la industria incluyen la optimización de procesos, la simulación de materiales complejos en la farmacéutica y la química, y mejoras en inteligencia artificial. En el sector financiero, su potencial abarca desde la detección de fraudes hasta la optimización de carteras de inversión y la mejora en la modelización de riesgos.

Sin embargo, la computación cuántica también plantea importantes desafíos, especialmente en el ámbito de la ciberseguridad. Algoritmos como Grover y Shor amenazan los actuales sistemas criptográficos, facilitando la ruptura de claves de cifrado utilizadas en transacciones financieras y comunicaciones seguras. El teorema de Mosca y la estrategia de "Harvest Now, Decrypt Later" subrayan la urgencia de migrar a estándares post-cuánticos, un proceso que puede requerir largos tiempos de adaptación.

Organismos internacionales como los bancos centrales, el BIS, el WEF y el G7 han realizado estudios y publicaciones para comprender el impacto de la computación cuántica en el sistema financiero. Asimismo, entidades como la UNESCO han promovido la cooperación científica y la capacitación en este ámbito.

Instituciones como el NIST, CISA y el DHS han liderado iniciativas para la transición hacia criptografía resistente a la computación cuántica. La Unión Europea y otros países han implementado estrategias de investigación y desarrollo, además de regulaciones para mitigar los riesgos asociados.

El impacto en el sistema financiero y de pagos será significativo. La computación cuántica podría transformar la autenticación de clientes, la seguridad de las transacciones con tarjetas y activos virtuales, así como

fortalecer los esquemas de firma digital y encriptación en la nube. No obstante, también puede generar vulnerabilidades en los sistemas actuales, lo que hace esencial la implementación de medidas de seguridad avanzadas.

Para las autoridades financieras, es crucial adoptar un enfoque proactivo, promoviendo la investigación y colaboración con expertos en computación cuántica y ciberseguridad. La regulación debe fomentar la migración hacia estándares post-cuánticos, estableciendo hojas de ruta claras y promoviendo la cooperación internacional para garantizar la seguridad del sistema financiero global en la era cuántica.

Referencias

Aggarwal, D., Brennen, G., Lee, T., Santha, M., y Tomamichel, M. (2018). Quantum Attacks on Bitcoin, and How to Protect Against Them. Ledger, 3. https://doi.org/10.5195/ledger.2018.127

Allende, M., León, D. L., Cerón, S., et al. (2023). *Quantum-resistance in blockchain networks*. *Scientific Reports, 13*, 5664. https://doi.org/10.1038/s41598-023-32701-6

Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., y Schanck, J. (2017). *Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3. In: Avanzi, R., Heys, H. (eds) Selected Areas in Cryptography – SAC 2016. SAC 2016.* Lecture Notes in Computer Science (), vol 10532. Springer, Cham. https://doi.org/10.1007/978-3-319-69453-5_18

Andriani, C., Bencivelli, L., Castellucci, A., De Santis, M., Marchetti, S., y Piantanida, G. (2024). *The quantum challenge: implications and strategies for a secure financial system* (Occasional Paper No. 877). Banca d'Italia. https://www.bancaditalia.it/pubblicazioni/qef/2024-0877/QEF_877_24.pdf

Bank for International Settlements. (2024). *Cybersecurity and quantum computing*. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

Barker, W., Polk, W., y Souppaya, M. (2021). *Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04282021

Beullens, W., D'Anvers, J.-P., Hülsing, A., Lange, T., Panny, L., de Saint Guilhem, C., y Smart, N. P. (2021). *Post-quantum cryptography: Current state and quantum mitigation (Version 2)*. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/92307

CISA. (2022). *Prepare for new cryptographic standards to protect against future quantum-based threats*. https://www.cisa.gov/news-events/alerts/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum-based-threats

CISA, NSA, y NIST. (2023). *Quantum-Readiness: Migration to Post-Quantum Cryptography*. https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

Department of Homeland Security. (2021). *Post-quantum cryptography infographic*. https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

Dietz, M., Henke, N., Moon, J., Backes, J., Pautasso, L., y Sadeque, Z. (2020). *How quantum computing could change financial services*. McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/how-quantum-computing-could-change-financial-services

European Union Agency for Cybersecurity (ENISA). (2022). *Post-Quantum Cryptography - Integration study*. ENISA. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

European Commission. (2024). *Recommendation on a coordinated implementation roadmap for the transition to post-quantum cryptography*. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

Financial Industry Regulatory Authority. (2023). Quantum Computing and the Implications for the Securities Industry. https://www.finra.org/rules-guidance/key-topics/fintech/report/quantum-computing

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212–219. https://doi.org/10.1145/237814.237866

Holmes, S., y Chen, L. (2021). *Assessment of quantum threat to Bitcoin and derived cryptocurrencies*. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2021/967.pdf

Kan, K., y Une, M. (2021). *Recent trends on research and development of quantum computers and standardization of post-quantum cryptography*. *Monetary and Economic Studies, 39*(6), 77-102. Institute for Monetary and Economic Studies, Bank of Japan. https://www.imes.boj.or.jp/research/papers/english/me39-6.pdf

Kearney, J. J., y Perez-Delgado, C. A. (2021). *Vulnerability of blockchain technologies to quantum attacks*. *Array, 10*, 100065. https://doi.org/10.1016/j.array.2021.100065

López Chamorro, N. (2024). *El camino hacia la supremacía cuántica: oportunidades y desafíos en el ámbito financiero, la nueva generación de criptografía resiliente*. *Documentos Ocasionales/Banco de España, 2421*. https://www.bde.es/wbe/es/publicaciones/analisis-economico-investigacion/documentos-ocasionales/el-camino-hacia-la-supremacia-cuantica--oportunidades-y-desafios-en-el-ambito-financiero--la-nueva-generacion-de-criptografia-resiliente.html

Moody, D., Perlner, R., Regenscheid, A., Robinson, A., y Cooper, D. (2024). *Transition to post-quantum cryptography standards* (NIST Internal Report 8547 ipd). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8547.ipd

Mosca, M. (2015). *Cybersecurity in an era with quantum computers: Will we be ready?* Cryptology ePrint Archive, Report 2015/1075. International Association for Cryptologic Research. Retrieved from https://eprint.iacr.org/2015/1075

National Institute of Standards and Technology (NIST). (2024a). *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (FIPS Publication 203). https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology (NIST). (2024b). *Module-Lattice-Based Digital Signature Standard* (FIPS Publication 204). https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology (NIST). (2024c). *Stateless Hash-Based Digital Signature Standard* (FIPS Publication 205). https://doi.org/10.6028/NIST.FIPS.205

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124-134. https://doi.org/10.1109/SFCS.1994.365700

The White House. (2022). *National security memorandum on promoting United States leadership in quantum computing while mitigating risks to vulnerable cryptographic systems*. https://bidenwhitehouse.archives.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/

U.S. Department of the Treasury. (2024). *G7 Cyber Expert Group statement on planning for opportunities and risks of quantum computing*. https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf

Vesely, M. (2023). *Finding the optimal currency composition of foreign exchange reserves with a quantum computer*. CNB Working Paper No. 1/2023. https://www.cnb.cz/export/sites/cnb/en/economic-research/.galleries/research_publications/cnb_wp/cnbwp_2023_01.pdf

World Economic Forum. (2022a). *Quantum computing governance principles*. https://www.weforum.org/publications/quantum-computing-governance-principles

World Economic Forum. (2022b). *State of quantum computing: Building a quantum economy*. https://www.weforum.org/publications/state-of-quantum-computing-building-a-quantum-economy

World Economic Forum. (2022c). *Transitioning to a quantum-secure economy*. https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy

World Economic Forum. (2023). *Quantum readiness toolkit: Building a quantum-secure economy*. https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy

World Economic Forum. (2024a). *Quantum economy blueprint*. https://www.weforum.org/publications/quantum-economy-blueprint

World Economic Forum. (2024b). *Quantum security for the financial sector: Informing global regulatory approaches*. https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches