FMI – Posibilidades y peligros de la computación cuántica



*Las computadoras cuánticas podrían descifrar la criptografía que sustenta la estabilidad financiera*

Los soldados en la antigua Grecia enviaban despachos secretos envolviendo una tira de pergamino alrededor de un bastón y escribiendo a través de él. Sus mensajes solo podían ser descifrados por alguien con un bastón del mismo grosor. Es uno de los primeros ejemplos de criptografía. Los secretos de hoy, como la comunicación por Internet, la banca digital y el comercio electrónico, están protegidos de miradas indiscretas por poderosos algoritmos informáticos. Sin embargo, estos códigos criptográficos hasta ahora impenetrables pronto podrían ser historia.

Las computadoras cuánticas pueden alcanzar un nivel de optimización que descifraría muchas de las claves de cifrado actuales en menos tiempo del que se tarda en generarlas utilizando computadoras digitales convencionales. Las instituciones financieras deben preparar sus sistemas de ciberseguridad para el futuro sin demora. De lo contrario, se pondrá en peligro la estabilidad financiera.

**Una revolución cuántica**

La computación cuántica es el uso de fenómenos cuánticos como *la superposición* y *el entrelazamiento* para realizar cálculos. La unidad básica de una computadora cuántica es el bit cuántico (o *qubit*, para abreviar). Por lo general, se realiza por las propiedades cuánticas de las partículas subatómicas, como el espín de los electrones o la polarización de un fotón. Mientras que cada bit binario utilizado en las computadoras digitales de hoy representa un valor de cero o uno, los qubits representan tanto cero como uno (o alguna combinación de los dos) al mismo tiempo. Este fenómeno se llama superposición. El entrelazamiento cuántico es una conexión especial entre pares o grupos de elementos cuánticos. Cambiar el estado de un elemento afecta a otros elementos entrelazados al instante, independientemente de la distancia entre ellos.

**Los códigos criptográficos impenetrables de hoy**

**pronto podrían ser historia.**

El aumento del número de qubits ofrece un aumento exponencial en la velocidad de procesamiento de cálculos. Se necesitan dos bits binarios tradicionales para igualar la potencia de un solo qubit; se requieren cuatro bits para que coincidan con dos qubits; se necesitan ocho bits para que coincidan con tres qubits; y así sucesivamente. Se necesitarían alrededor de 18 cuatrillones de bits de memoria tradicional para modelar una computadora cuántica con solo 54 qubits. Una computadora cuántica de 100 qubits requeriría más bits de los que hay átomos en nuestro planeta. Y una computadora de 280 qubits requeriría más bits de los que hay átomos en el universo conocido.

Las computadoras cuánticas tienen el potencial de superar masivamente a las computadoras digitales que siguen las leyes clásicas de la física. William Phillips, el físico ganador del Premio Nobel, ha comparado el salto de la tecnología actual a la cuántica con el del [ábaco](https://minghsiehece.usc.edu/2018/04/quantum-information-a-scientific-and-technological-revolution-for-the-21st-century/) a la computadora digital en sí. Hasta hace poco, esta llamada *ventaja cuántica* o *"supremacía" cuántica* era solo una teoría. En 2019, sin embargo, Google utilizó una computadora cuántica para realizar una tarea de cálculo específica en solo 200 segundos. La misma tarea, dijo la compañía, habría tomado la supercomputadora digital más poderosa en ese momento [10,000 años](https://www.nature.com/articles/s41586-019-1666-5).

**Las posibilidades**

Las tareas computacionales complejas son como encontrar la manera de salir de un laberinto. Una computadora tradicional trataría de escapar siguiendo cada camino en secuencia hasta llegar a la salida. La superposición, por el contrario, permite a una computadora cuántica probar todos los caminos a la vez. Esto reduce drásticamente el tiempo para encontrar una solución.

Al resolver problemas con más precisión y velocidad que las computadoras digitales, las computadoras cuánticas tienen el potencial de acelerar el descubrimiento científico y la innovación, revolucionar el modelado y las simulaciones del mercado financiero y potenciar el aprendizaje automático y la inteligencia artificial. Podrían usarse para modelar partículas subatómicas, interacciones moleculares y reacciones químicas. Esto podría revolucionar la ingeniería química y la ciencia de los materiales y permitir el diseño de nuevos materiales, como las baterías de estado sólido. Las computadoras cuánticas también podrían ayudarnos a comprender el cambio climático.

Las computadoras cuánticas también podrían transformar el sistema financiero. Podrían realizar simulaciones monte carlo más precisas, utilizadas para predecir el comportamiento de los mercados a través de simulaciones de precios y riesgos, casi en tiempo real. No habría necesidad de simplificar estos modelos con suposiciones poco realistas. Las computadoras cuánticas también podrían resolver tareas de optimización, como asignar capital, determinar inversiones de cartera o administrar el efectivo en redes de cajeros automáticos, en una fracción del tiempo que toman las computadoras digitales. Las computadoras cuánticas también podrían acelerar el entrenamiento de algoritmos de aprendizaje automático. El tiempo que tardan las computadoras digitales en hacer esto aumenta exponencialmente con cada dimensión que se agrega. No es así con las computadoras cuánticas.

**Y los peligros**

Sin embargo, existen riesgos. La potencia de cálculo de estas poderosas máquinas cuánticas podría amenazar la criptografía moderna. Esto tiene implicaciones de largo alcance para la estabilidad financiera y la privacidad. La criptografía actual se basa en tres tipos principales de algoritmos: *claves simétricas, claves* *asimétricas* (también *conocidas como claves públicas*) y *funciones hash*. Con las claves simétricas, la misma clave se utiliza para cifrar y descifrar un mensaje. La criptografía asimétrica utiliza un par de claves relacionadas (una privada y otra pública). Un mensaje cifrado por una clave solo puede ser descifrado por el par de esa clave. Estos algoritmos son ampliamente utilizados para la autenticación digital, las firmas digitales y la seguridad de los datos. Las funciones hash convierten la entrada digital en un conjunto único de bytes de tamaño fijo. Se utilizan para almacenar contraseñas de forma segura y para admitir identidades digitales.

Estos algoritmos criptográficos han tenido éxito en su mayoría en la protección de los datos. Incluso las supercomputadoras digitales y las técnicas de criptoanálisis más avanzadas de hoy en día no pueden romperlas lo suficientemente rápido. Sin embargo, las computadoras cuánticas podrán resolver problemas matemáticos difíciles exponencialmente más rápido que las supercomputadoras digitales. Esto hará que la criptografía asimétrica sea [obsoleta](https://www.etsi.org/committee/cyber?id=1805) y debilitará otras claves criptográficas y hashes. Teóricamente, una computadora cuántica en pleno funcionamiento podría romper una clave asimétrica en cuestión de minutos. Las claves públicas son especialmente vulnerables porque la mayoría de ellas se basan en el problema de la factorización: es difícil para las computadoras digitales encontrar dos números primos de su producto. Las computadoras cuánticas, por el contrario, pueden hacerlo sin esfuerzo.

Las claves asimétricas son ampliamente utilizadas para asegurar las comunicaciones a través de Internet. Los ataques exitosos contra estos algoritmos comprometerían las conexiones utilizadas por el sistema financiero, incluida la banca móvil, el comercio electrónico, las transacciones de pago, los retiros de efectivo en cajeros automáticos y las comunicaciones VPN, por nombrar solo algunos. Las aplicaciones vulnerables que dependen de la criptografía de clave pública también incluyen activos digitales populares como Bitcoin y Ethereum, así como aplicaciones web protegidas por contraseña. El más conocido de estos protocolos, [HTTPS](https://transparencyreport.google.com/https/overview?hl=en), es utilizado por 97 de los 100 mejores sitios web del mundo.

Para algunas aplicaciones, puede que ya sea demasiado tarde. Cualquier información que se asuma segura hoy en día podría ser capturada y almacenada para ser descifrada más tarde una vez que se creen computadoras cuánticas suficientemente poderosas. De hecho, casi cualquier mensaje personal o financiero cifrado enviado y almacenado hoy en día podría ser descifrado retroactivamente por una poderosa computadora cuántica. La mayoría de las instituciones financieras y los reguladores aún no están alertas a estos nuevos riesgos.

**Carrera contra la máquina**

La carrera para desarrollar nuevos estándares y algoritmos de cifrado cuánticos seguros ya ha comenzado. En los Estados Unidos, el Instituto Nacional de Estándares y Tecnología está organizando una competencia para desarrollar algoritmos de cifrado cuánticos seguros. Espera anunciar un ganador para [2024](https://csrc.nist.gov/publications/detail/nistir/8309/final). El Instituto Europeo de Normas de Telecomunicaciones también está tomando la delantera. Estos esfuerzos están contribuyendo a las actividades de otros órganos normativos. Sin embargo, debido a los riesgos retroactivos, las instituciones financieras tienen una ventana estrecha para implementar los nuevos estándares.

Las instituciones financieras deben tomar medidas inmediatas para prepararse para una [transición criptográfica](https://www.etsi.org/committee/cyber?id=1805). Deberían comenzar por evaluar los riesgos retroactivos y futuros de las computadoras cuánticas, incluida la información que ya puede haber sido capturada y puede ser explotada años después. Las instituciones financieras deberían desarrollar planes para migrar la criptografía actual a algoritmos resistentes a la cuántica. Esto incluye hacer un inventario de la criptografía de clave pública que utilizan ellos mismos, así como la utilizada por cualquier proveedor externo. Los algoritmos vulnerables deberán pasar a la criptografía postcuántica. Las instituciones financieras también deben desarrollar agilidad criptográfica para que los algoritmos puedan actualizarse sin problemas. Las experiencias de reemplazos de algoritmos, aunque mucho más simples que la transición a estándares post-cuánticos, muestran que pueden ser extremadamente disruptivos. A menudo tardan años o [décadas en lograrse](https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects).

El FMI tiene un papel importante que desempeñar en la sensibilización de sus miembros sobre los riesgos para la estabilidad financiera de las computadoras cuánticas y en la promoción de normas y prácticas de seguridad cuántica. El Fondo debería alentar a los países miembros a colaborar estrechamente en el desarrollo de estándares de cifrado cuántico seguro para garantizar la interoperabilidad y adoptar planes de migración de cifrado para sus sectores financieros.

Las computadoras cuánticas de hoy en día son muy sensibles. Cualquier perturbación ambiental, como el calor, la luz o la vibración, saca los qubits de su estado cuántico y los convierte en bits regulares. Esto produce errores de cálculo. Aun así, las máquinas que computan con menos errores y son capaces de descifrar códigos no están muy lejos. Las instituciones financieras deben reconocer los riesgos y proteger sus sistemas antes de que sea demasiado tarde. Después de todo, la historia está llena de historias de advertencia de códigos supuestamente irrompibles que son descifrados por la nueva tecnología.

*Este artículo se basa en el documento de trabajo 21/71 del FMI, "*[*Quantum Computing and the Financial System: Spooky Action at a Distance?"*](https://www.imf.org/en/Publications/WP/Issues/2021/03/12/Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-50159)



**TAHSIN SAADI SEDIK**, subjefe de división del Departamento de Asia y el Pacífico del FMI.



**MAJID MALAIKA,** experto líder en transformación digital y riesgo de ciberseguridad en el Departamento de Tecnología de la Información del FMI.



**MICHAEL GORBANYOV** es economista sénior del Departamento de Estrategia, Políticas y Examen del FMI.



**JOSÉ DEODORO** es el propietario de la plataforma de recopilación de datos en el Departamento de Tecnología de la Información del FMI.

Las opiniones expresadas en artículos y otros materiales son las de los autores; no reflejan necesariamente la política del FMI.