El físico Nicolas Pulido junto a un prototipo de computadora cuántica en Brunswick, Alemania.

LAS POSIBILIDADES Y LOS RIESGOS de la informática cuántica

Las computadoras cuánticas podrían descifrar la criptografía que sostiene la estabilidad financiera

José Deodoro, Michael Gorbanyov, Majid Malaika y Tahsin Saadi Sedik

Los soldados de la antigua Grecia enviaban comunicaciones secretas envolviendo una vara en una tira de pergamino y escribiendo sobre él en sentido horizontal. De esa manera, solo quien tuviera una vara del mismo grosor podría descifrar el mensaje. Ese es uno de los ejemplos más antiguos de criptografía. Los secretos de hoy, como las comunicaciones de Internet, las operaciones de la banca digital y el comercio electrónico, se protegen de los ojos de los curiosos por medio de potentes algoritmos informáticos. Sin embargo, estos códigos criptográficos, hasta ahora impenetrables, pronto podrían ser historia.

Las computadoras cuánticas pueden alcanzar un nivel de optimización capaz de descubrir muchos de los códigos de encriptación actuales en menos tiempo del que lleva generarlos usando computadoras convencionales. Las instituciones financieras deben reforzar sus sistemas de ciberseguridad sin demoras. De lo contrario, la estabilidad financiera estará en peligro.

Una revolución cuántica

La informática cuántica es el uso de fenómenos cuánticos, como la *superposición* y el *entrelazamiento* para realizar cálculos. La unidad elemental de una computadora cuántica es el bit cuántico (o *cúbit*, para abreviar). Por lo general, se constituye con las propiedades cuánticas de partículas subatómicas, como el espín de los electrones o la polarización de los fotones. Mientras que cada bit binario que se usa en las computadoras digitales de la actualidad representa un valor de cero o

Las computadoras cuánticas tienen el potencial de superar con creces a las computadoras digitales, que siguen las leyes de la física clásica.

uno, los cúbits representan cero y uno (o una combinación de ambos) a la vez. Este fenómeno se denomina superposición. El entrelazamiento cuántico es una conexión especial entre pares o grupos de elementos cuánticos. El cambio de estado de un elemento afecta al instante a los demás elementos entrelazados, sin importar qué distancia haya entre ellos.

Al aumentar la cantidad de cúbits, crece exponencialmente la velocidad de procesamiento de los cálculos. Se necesitan dos bits binarios tradicionales para igualar la potencia de un cúbit; cuatro bits para igualar dos cúbits; ocho bits para igualar tres cúbits, y así sucesivamente. Se necesitarían alrededor de 18.000 billones de bits de memoria tradicional para modelar una computadora cuántica con apenas 54 cúbits. Una computadora de 100 cúbits requeriría más bits que los átomos que hay en nuestro planeta, y una de 280 cúbits exigiría más bits que los átomos que hay en el universo conocido.

Las computadoras cuánticas tienen el potencial de superar con creces a las computadoras digitales, que siguen las leyes de la física clásica. William Phillips, premio Nobel de Física, comparó el salto de la tecnología actual a la cuántica con el del ábaco a la computadora digital. Hasta hace poco, esta supuesta *ventaja* o "*supremacía*" *cuántica* era puramente teórica. Pero en 2019 Google usó una computadora cuántica para llevar a cabo un cálculo determinado en apenas 200 segundos. Según la empresa, el mismo cálculo le habría llevado 10.000 años a la supercomputadora digital más potente.

Las posibilidades

Los cómputos complejos son como la búsqueda de la salida de un laberinto. Una computadora tradicional la abordaría siguiendo todos los caminos posibles en secuencia hasta encontrar la salida. La superposición, en cambio, les permite a las computadoras cuánticas probar todos los caminos a la vez, lo que reduce drásticamente el tiempo necesario para dar con la solución.

Gracias a su capacidad de resolver problemas con más precisión y velocidad que las computadoras digitales, las computadoras cuánticas pueden acelerar los descubrimientos y la innovación científicos, revolucionar las proyecciones y simulaciones del mercado financiero, y potenciar el aprendizaje automático y la inteligencia artificial. También podrían usarse para modelar partículas subatómicas, interacciones moleculares y reacciones químicas, lo que revolucionaría la ingeniería química y las ciencias materiales, y permitiría diseñar materiales nuevos, como baterías de estado sólido. Además, las computadoras cuánticas podrían ayudarnos a entender el cambio climático.

Y, por último, podrían transformar el sistema financiero. Podrían llevar a cabo simulaciones de Monte Carlo —que se utilizan para predecir el comportamiento de los mercados mediante simulaciones del cálculo de precios y riesgos— con más exactitud y casi en tiempo real, y ya no sería necesario simplificar estos modelos con supuestos que se alejan de la realidad. Las computadoras cuánticas también podrían resolver tareas de optimización —como asignar capital, definir carteras de inversión o gestionar el efectivo en redes de cajeros automáticos— en una fracción minúscula del tiempo que tomarían las computadoras digitales. Además, podrían acelerar el entrenamiento de los algoritmos de aprendizaje automático. El tiempo que esto les lleva a las computadoras digitales aumenta exponencialmente con cada dimensión que se agrega. Lo que no ocurre con las computadoras cuánticas.

Y los riesgos

Pero todo esto tiene sus peligros. La capacidad de cómputo de estas poderosas máquinas cuánticas podría amenazar la criptografía moderna, lo cual repercutiría gravemente en la estabilidad financiera y la privacidad. La criptografía actual se basa en tres grandes tipos de algoritmos: *claves simétricas, claves asimétricas* (también conocidas como *claves públicas*) y funciones *hash*. Con las claves simétricas, se utiliza una misma clave para encriptar y desencriptar un mensaje. La criptografía asimétrica usa un par de claves relacionadas (una privada y la otra pública). Un mensaje que se encripta con una clave solo puede desencriptarse usando su clave par. Estos algoritmos son de uso sumamente extendido en la autenticación digital, las firmas digitales y la seguridad de datos. Las funciones *hash* convierten una entrada digital en un conjunto único de bytes de un tamaño fijo. Se usan para almacenar contraseñas de forma segura y para identidades digitales.

En casi todos los casos, estos algoritmos criptográficos son eficaces para proteger los datos. Ni las supercomputadoras digitales ni las técnicas de criptoanálisis más avanzadas de la actualidad pueden decodificarlos con suficiente rapidez. Sin embargo, las computadoras cuánticas podrán resolver problemas matemáticos complejos exponencialmente más rápido que las supercomputadoras digitales, lo cual dejará obsoleta a la criptografía asimétrica y debilitará a las demás claves y funciones *hash*. En teoría, una computadora

FOTO: GETTY IMAGES / PICTURE ALLIANCE / JULIAN STRATENSCHULTE

Las instituciones financieras deben tomar medidas inmediatas a fin de prepararse para una transición criptográfica.

cuántica totalmente operativa podría decodificar una clave asimétrica en cuestión de minutos. Las claves públicas son particularmente vulnerables, puesto que se basan en el problema de la factorización: para las computadoras digitales es difícil encontrar dos números primos a partir de su producto. Las computadoras cuánticas, en cambio, lo harán sin esfuerzo.

Las claves asimétricas son muy utilizadas para proteger las comunicaciones en Internet. De tener éxito, los ataques sobre estos algoritmos pondrían en riesgo las conexiones que emplea el sistema financiero: la banca móvil, el comercio electrónico, las transacciones de pago, los retiros de efectivo de cajeros automáticos y las comunicaciones en redes privadas virtuales, por mencionar solo algunos. Los populares activos digitales como el bitcóin y el ethereum, son otras aplicaciones vulnerables de la criptografía con claves públicas, igual que las aplicaciones web protegidas por contraseña. El más conocido de estos protocolos, HTTPS, se usa en 97 de los 100 principales sitios web del mundo.

Para algunas aplicaciones, es posible que ya sea demasiado tarde. Toda información hoy considerada segura podría recopilarse y almacenarse para descifrarse más tarde, una vez que se hayan creado computadoras cuánticas suficientemente potentes. De hecho, casi cualquier mensaje encriptado, personal o financiero, que se envía y almacena hoy podría descifrarse retroactivamente por medio de una computadora cuántica poderosa. La mayoría de las instituciones financieras y organismos de regulación no están al tanto de estos nuevos riesgos.

Una carrera contra las máquinas

La carrera por formular nuevos estándares y algoritmos a prueba de cálculos cuánticos ya comenzó. En Estados Unidos, el Instituto Nacional de Normas y Tecnología está llevando a cabo un concurso para desarrollar algoritmos de encriptación que puedan hacer frente a las computadoras cuánticas, y prevé anunciar a un ganador de aquí a 2024. El Instituto Europeo de Normas de Telecomunicaciones también está a la delantera. Estas iniciativas alimentan las actividades de otros organismos normativos. Sin embargo, a causa de los riesgos retroactivos, las instituciones financieras no disponen más que de una estrecha ventana para implementar las nuevas normas.

Las instituciones financieras deben tomar medidas inmediatas a fin de prepararse para una transición criptográfica. Para empezar, deben evaluar los riesgos retroactivos y futuros que implican las computadoras cuánticas; por ejemplo, en lo relativo a la información que ya pudo haberse recopilado para explotarse más adelante. Luego, deben formular planes para migrar la criptografía actual a algoritmos que puedan resistir las capacidades cuánticas. Eso incluye hacer un inventario de la criptografía de claves públicas que utilicen las instituciones financieras mismas y todos sus proveedores externos. Los algoritmos vulnerables deberán cambiarse por criptografía poscuántica. Además, las instituciones financieras deben redoblar su agilidad criptográfica a fin de que los algoritmos puedan actualizarse con celeridad. La experiencia en materia de reemplazo de algoritmos, hasta ahora mucho más simple que la transición a normas poscuánticas, indica que estos procesos pueden ser extremadamente disruptivos, y es habitual que requieran años o décadas para completarse.

El FMI tiene una responsabilidad importante de generar conciencia entre sus miembros sobre los riesgos que conllevan las computadoras cuánticas para la estabilidad financiera, y de promover el diseño de normas y prácticas a prueba de cálculos cuánticos. También debe alentar a los países miembros a colaborar estrechamente en el desarrollo de normas de encriptación que puedan hacer frente a estas nuevas tecnologías a fin de garantizar la interoperabilidad y adoptar planes de migración de la encriptación para sus sectores financieros.

Las computadoras cuánticas de hoy son muy sensibles. Cualquier perturbación ambiental, como el calor, la luz o la vibración, saca a los cúbits de su estado cuántico y los convierte en bits ordinarios, lo que provoca errores de cálculo. Aun así, no falta mucho para el advenimiento de máquinas que computen con menos errores y estén en condiciones de descifrar códigos. Las instituciones financieras deben comprender los riesgos y blindar sus sistemas antes de que sea tarde. Al fin y al cabo, la historia está llena de moralejas sobre códigos supuestamente inviolables que ceden a manos de nuevas tecnologías. FD

JOSÉ DEODORO es Experto a cargo de la plataforma de gestión de datos y **MAJID MALAIKA** es Experto en transformación digital y riesgos de ciberseguridad, ambos del Departamento de Tecnología de la Información del FMI. **MICHAEL GORBANYOV** es Economista Principal del Departamento de Estrategia, Políticas y Evaluación del FMI y **TAHSIN SAADI SEDIK** es Subjefe de División del Departamento de Asia y el Pacífico del FMI.

Este artículo se basa en el documento de trabajo 21/71 del FMI "Quantum Computing and the Financial System Spooky Action at a Distance?"