LITORALPRESS

Fecha: 06-01-2025
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Noticia general
Título: Una amenaza inminente para el bitcóin: el riesgo de un hackeo cuántico

Pág. : 6
Cm2: 813,5

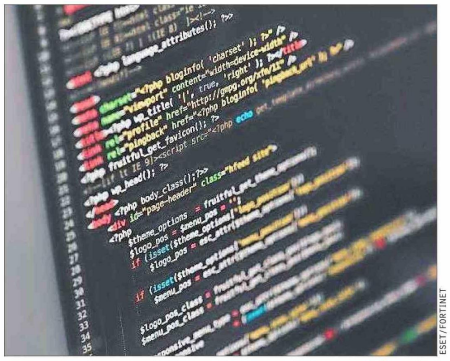
Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

WSJ

Preocupa que nueva tecnología vulnere codificación de la ciptomoneda

Una amenaza inminente para el bitcóin: el riesgo de un hackeo cuántico

Investigadores advierten que un ataque computacional cuántico contra la criptomoneda provocaría billones de dólares en pérdidas.



ESET/FORTINET

Los computadores cuánticos hacen tareas en mucho menor tiempo que los estándar.

JOE RAEDLE/AFP

Un estudio del Hudson Institute de 2022 estimó que un hackeo cuántico del bitcóin causaría más de US$ 3 billones en pérdidas.

ALEXANDER OSIPOVICH
The Wall Street Journal

La recuperación del bitcóin enfrenta un riesgo que no está en el radar de una mayoría de inversionistas en criptomonedas: la computación cuántica.

La naciente tecnología, la que atrajo la atención después de que Google anunciara un avance importante con su nuevo chip de computación cuántica Willow, podría algún día permitir que los *hackers* descifren la codificación que mantiene seguro al bitcóin. Ese hackeo podría afectar el precio del bitcóin, al permitir que los ladrones roben monedas de billeteras digitales supuestamente seguras.

Los investigadores señalan que es probable que un dispositivo cuántico lo suficientemente potente como para descifrar el bitcóin esté a una década o más de distancia. Con todo, los avances en la tecnología plantean un riesgo a largo plazo, a menos que la comunidad díscola de aquellos que desarrollan el bitcóin refuercen su tecnología en una actualización que requiere mucho tiempo.

Un ataque cuántico contra el bitcóin podría tener efectos secundarios perjudiciales en los mercados financieros tradicionales, advierten analistas.

"Lo que tiene aquí es una bomba de tiempo a punto de explotar, si es que alguien tiene esa habilidad para desarrollar el hackeo de computación cuántica y decide utilizarla para apuntarles a las criptomonedas", comentó Arthur Herman, antiguo miembro del Hudson Institute, un centro de estudios con sede en Washington, D.C.

Un estudio del Hudson Institute de 2022 estimaba que un hackeo cuántico del bitcóin causaría más de US$ 3 billones en pérdidas en los mercados de criptomonedas y de otro tipo, y desencadenaría una profunda recesión. Herman indicó que los costos probables de un hackeo cuántico han aumentado desde que el estudio se dio a conocer, puesto que el bitcóin está cerca de los US$ 100 mil y se ha convertido en un activo de inversión cada vez más popular.

El Presidente electo Donald Trump ha prometido crear una reserva estratégica para las tenencias de bitcoines del gobierno, una especie de Fort Knox digital.

La computación cuántica podría permitir que los ladrones invadan ese Fort Knox. A diferencia de los computadores estándar, en los que todos los datos se representan fundamentalmente en ceros o unos, los computadores cuánticos utilizan las propiedades singulares de las partículas subatómicas para representar datos en "qubits", los que pueden existir en un medio continuo de estados que son mezclas de ceros y unos.

Eso permite que los computadores cuánticos hagan de prisa tareas que a los computadores estándar les tomaría mucho más tiempo resolver que toda una vida humana. Esas tareas podrían incluir el descubrimiento de nuevos medicamentos, el pronóstico del tiempo; o el descifrado de la codificación que se utiliza para proteger datos sensibles.

Por ejemplo, un método de codificación común involucra números muy grandes llamados claves públicas, que son múltiplos de dos números primos grandes. Los dos números primos se pueden combinar para generar lo que se conoce como la clave privada. Los datos se pueden codificar con la clave pública, y decodificar con la clave privada. Como lo sugieren los nombres, los usuarios mantienen sus claves privadas en secreto, pero las públicas se podrían compartir.

La fortaleza de este método es que un computador estándar requiere una enorme cantidad de tiempo para derivar la clave privada de la pública, debido a la dificultad de factorizar; deducir los números primos que se pueden multiplicar para obtener la clave pública.

RESERVA
Donald Trump prometió crear una reserva para las tenencias de bitcóin del Gobierno.

La computación cuántica hace que la factorización sea mucho más fácil. Un algoritmo que creó un matemático estadounidense en 1994 posibilita dividir en factores números enormes en cosa de minutos; siempre que tenga un computador cuántico lo suficientemente potente.

Un avance como este amenazaría no solo al bitcóin, sino a las finanzas tradicionales, porque muchos sistemas bancarios en línea utilizan variantes de criptografía de clave pública. Pero el bitcóin podría ser un objetivo especialmente atractivo para los ladrones cuánticos, advierten expertos en seguridad.

"El bitcóin va a ser el blanco de todos los ataques", afirmó Skip Sanzeri, cofundador de QuSecure, una nueva empresa que se especializa en ciberseguridad cuántica. "Los bancos tienen cierta regulación, algunos mecanismos de defensa y la capacidad de cubrir a sus clientes, mientras que el bitcóin es el Salvaje Oeste. Su billetera digital no le va a reembolsar si le roban sus bitcoines".

Aunque los *hackers* han robado bitcoines antes, sus ataques por lo general implicaban obtener acceso no autorizado a las bolsas de criptomonedas. Un ataque cuántico sería más insidioso, porque pondría en duda la seguridad de toda la red de bitcóin, no solo de unas pocas bolsas de criptomonedas con una seguridad deficiente.

Algunas reservas de bitcoines son especialmente susceptibles al robo cuántico. En los primeros días del bitcóin, se mantenía en direcciones con claves públicas expuestas, lo que incluía el millón de monedas aproximadamente que se cree que pertenecen a Satoshi Nakamoto, el misterioso creador del bitcóin. Alrededor de 1,72 millones de bitcoines —valorados en más de US$ 160 mil millones al precio actual— se mantienen en esas direcciones, las que más tarde se eliminaron gradualmente, según Galaxy Digital.

Finalmente, todos los bitcoines corren peligro una vez que los computadores cuánticos lleguen a ser lo suficientemente potentes. Esto es porque los *hackers* podrían robar las monedas que se transfieren de una dirección a otra durante un espacio de 10 minutos que requiere la red de bitcóin para confirmar esas transferencias.

Algunos criptoveteranos dicen que aún hay mucho tiempo para que el bitcóin solucione sus vulnerabilidades.

"Definitivamente hay un apocalipsis cuántico en el horizonte que va a tener lugar en algún momento en el futuro, pero ese momento está a una distancia lo suficientemente larga como para que no cunda el pánico", manifestó Emin Gün Sirer, fundador de la criptomoneda Avalanche.

El bitcóin se podría asegurar si se adoptan formas más nuevas de codificación que no puedan ser descifradas fácilmente por computadores cuánticos; pero ese reacondicionamiento podría tardar años, precisan ejecutivos de criptomonedas. Debido a la naturaleza descentralizada del bitcóin, cambiar su tecnología requiere de un consenso amplio entre personas de todo el mundo que mantienen su red. Las actualizaciones anteriores han sido lentas y contenciosas.

Incluso después de que la comunidad llegue a un acuerdo sobre cómo lograr que el bitcóin sea a prueba de computadores cuánticos, hay otro obstáculo: los bitcoines existentes tendrían que ser transferidos a direcciones resistentes a un ataque cuántico. Cada persona o empresa que mantenga bitcoines tendría que ejecutar esa transferencia, o correr el riesgo de perder monedas a manos de ladrones cuánticos.

Traducido del inglés por "El Mercurio"