Siempre se ha defendido que blockchain es una tecnología absolutamente segura que mantiene las transacciones que tienen lugar en su seno a salvo de *hackers* y ciberdelincuentes. Sin embargo, la experiencia demuestra que las cadenas de bloques no son tan inquebrantables y que pueden ser objeto de ataques y robos.

El mayo pasado la empresa de intercambio de criptomonedas Binance anunció públicamente que había sufrido un ciberataque que conllevó la pérdida de 7 000 bitcoins valoradas en 40 millones de dólares. Los hackers hicieron gala de una gran paciencia trabajando lentamente durante un largo periodo de tiempo a través de *phishing* (ciberdelito basado en la suplantación de identidad) y de virus informáticos.

A pesar de que el consejero delegado de la compañía Changpeng Zhao aseguró que los usuarios no se verán afectados por el robo, pues la cantidad será repuesta por el fondo *Secure Asset Fund for Users* (SAFU), creado por Binance el pasado año, lo cierto es que acciones como esta ponen en cuestión uno de los mayores valores de los que hace gala la tecnología blockchain: su inquebrantabilidad.

El caso de Binance no es único. Este mes se ha sabido que la plataforma de blockchain Komodo ha descubierto en su cartera un virus *backdoor*, que permite al delincuente que lo ha creado acceder a los datos de encriptación de la empresa. Los responsables han tenido que extraer los datos y el dinero de sus clientes y llevarlos a una plataforma más segura, en previsión de que tenga lugar un ataque.

La tecnología de la cadena de bloques nos es vendida como una nueva revolución tecnológica que lo cambiara todo. Don Tapscott en su libro *Blockchain Revolution* lo definía así: *"La primera generación de la revolución digital nos trajo el internet de la información. La segunda generación –alimentada por la tecnología blockchain– nos está trayendo el internet del valor: una nueva plataforma para remodelar el mundo de los negocios y transformar para bien el antiguo orden de los asuntos humanos".*

La asociación inmediata que nos llega a la mente al pensar en blockchain son las criptomonedas, como Bitcoin, aunque estas son solamente un primer ejemplo del potencial que tiene este tipo de tecnológica descentralizada. No hay sector que -en teoría- escape al influjo de los bloques. Se habla de aplicar blockchain en las cadenas de suministro de las empresas, en los servicios ofrecidos al ciudadano por las administraciones públicas, en la educación, en el periodismo, en la protección de los derechos de autor, en la seguridad del internet de las cosas...

Y, sin embargo, hay quien pone en cuestión que esta tecnología sea todo lo segura que se dice que es. Michael Orcutt del MIT es una de estas voces críticas. A su juicio, bajo determinadas condiciones la tecnología de blockchain puede presentar vulnerabilidades. Algunas veces los problemas vienen por errores no intencionados de programación; otras por cuestiones más difusas: *"el complicado resultado de interacciones entre el código, la economía de blockchain y la avaricia humana".*

El *hash* y el protocolo de consenso

A pesar de todo, las cadenas de bloques tienen una base tecnológica muy segura. Su aireada inquebrantabilidad se basa en dos elementos de peso: que cada bloque del sistema está asociado a una huella digital criptográfica única, y que existe un protocolo de consenso que consigue que todos los nodos de la red estén de acuerdo sobre la veracidad del historial que todos comparten.

Las huellas digitales se llaman *hash* y son creadas por los mineros de blockchain, unas figuras esenciales dentro del sistema. Se trata de poderosos ordenadores que trabajan a cambio de criptomonedas. Cada *hash* es una fórmula matemática única que concentra en pocos caracteres gran cantidad de información. Sirven para sellar un bloque y para unirlo con el bloque siguiente, dado que este contiene el *hash* del anterior. De esta forma, no es posible alterar la información contenida en un bloque –un pago, por ejemplo- sin cambiar toda la cadena.

Cuando se añade un nuevo bloque a la cadena, todos los nodos de la red verifican que el *hash* corresponde al bloque en cuestión, y, automáticamente, actualizan sus copias de la blockchain, pues todos guardan una de toda la cadena entera. Si alguien intentase alterar un registro de forma retroactiva, tendría que cambiar el hash de ese bloque y de todos los siguientes que van unidos, pero los bloques que intente añadir entrarían en conflicto con los existentes, y los nodos rechazarían la operación.

Parece un método altamente seguro, ¿dónde está el problema entonces? En la imaginación del ser humano. Orcutt, antes citado, nos habla del "minero egoísta", que es cuando un nodo distrae al resto de ellos con un rompecabezas criptográfico con el fin reunir el tiempo suficiente para alterar un bloque sin que perciban el cambio, y también del "ataque de eclipse", en el que un nodo se hace con el control de la información de todo el sistema y hace pasar por verdadera la información falsa acerca de las transacciones.

Criptohackeo

Uno de los principales ciberdelitos asociados a blockchain es el denominado *criptohackeo*, que consiste en secuestrar los ordenadores de terceras personas para minar criptodivisas. Cuanta más potencia computacional, mayores beneficios genera la minería.

De acuerdo con el informe *Sociedad Digital en España 2018,* este tipo de ataque se duplicó el pasado año hasta el 42 %, en comparación con el 20,5 % de crecimiento en la segunda mitad de 2017. De hecho, las tres variantes de virus más comunes detectados entre enero y junio tenían como objetivo minar monedas a escondidas en los ordenadores infectados. El principal malware relacionado con la minería de criptomonedas son los virus Coinhive, Cryptoloot y JSEcoin.

Tal y como expone el informe de ESET sobre tendencias en ciberseguridad, la minería de bitcoins es un proceso muy costoso que solamente es rentable para aquellos agentes que lo realizan a gran escala, es decir, utilizando numerosas máquinas y dispositivos para poder disponer de un inmenso poder de computación.

La minería de criptomonedas es sí no es un delito; lo que constituye una actividad ilegal es utilizar sistemas de terceros sin su conocimiento y consentimiento. Y nadie está a salvo de sufrir este tipo de ataque: la conocida empresa Tesla fue víctima del *criptohackeo* en 2018 en uno de sus servidores alojados en la nube.

Catálogo de amenazas a las cadenas de bloques

Sin embargo, el *criptojacking* no es la única amenaza que acecha al blockchain. Los usuarios de estos servicios de divisas suelen ser las víctimas preferidas de los piratas, aunque también las *startups* de criptomonedas, e incluso las grandes empresas del sector, como Ethereum.

Un estudio realizado por McAfee identifica cuatro vectores concretos de ataque: *phishing, malware*, vulnerabilidades de implementación y tecnología.

A través del *phishing*, el delincuente se hace con las claves de identidad del usuario, generalmente con la intención de obtener lucro de ello robando criptodivisas. Un claro ejemplo de esto es el robo que sufrieron de sus monederos los usuarios de la criptomoneda IOTA, a finales de 2017, que casi alcanzó globalmente la cifra de 4 millones de dólares.

Los programas malignos o *malware* también afectan de lleno a blockchain, como hemos visto anteriormente con el caso del *criptohackeo*. Igualmente, los delincuentes utilizan la modalidad de *ransomware* o secuestro de los sistemas de criptomonedas, para exigir un rescate por la liberación de la información.

Un tercer problema viene asociado con las propias vulnerabilidades técnicas de los blockchain, que han dado lugar a ataques de denegación del servicio (DoS), robo de monedas y exposición de la información confidencial.

Ataque del 51%

El último peligro que identifica el trabajo de McAfee es el relativo a los factores inherentes a la propia tecnología, es decir, a las vulnerabilidades que surgen de aprovecharse de las propias reglas de funcionamiento de blockchain.

Uno de estos riesgos es la denominada regla del 51%, algo que hasta hace poco se quedaba en el terreno de la teoría, hasta que lo ha sufrido en sus carnes a principios de este año la red Ethereum Classic. Básicamente,

consiste en alterar el funcionamiento de una criptodivisa para poder gastar el mismo dinero repetidas veces. En concreto, los delincuentes cambiaron una cantidad de moneda de Ethereum por dinero real, para después reescribir el blockchain como si la operación no hubiese tenido lugar, con lo que seguían disponiendo de las criptomonedas que habían gastado.

Para poder cometer este ciberdelito es necesario acumular el 51% de todo el poder computacional que sostiene la red. Esto es algo casi imposible de realizar con Bitcoin, dado lo extendida que está esta criptodivisa y la inmensa cantidad de nodos que tiene su estructura blockchain, pero es factible con otras que tienen redes mucho más pequeñas.

Sin entrar en excesivos tecnicismos, el minero que ha conseguido la mayoría del poder para minar criptomonedas en el sistema tiene en sus manos la posibilidad de engañar a los demás, creando rápidamente una versión alternativa de la blockchain en la que los pagos que ha realizado nunca han tenido lugar. Esta nueva versión se conoce en el argot como *fork*, y el poder computacional del delincuente la convierte en la autorizada, sin que el resto de participante se percate del fraude.

Los responsables de Ethereum Classic descubrieron que algo raro había pasado cuando vieron que alguien había hecho cambios en el blockchain. Las primeras estimaciones arrojaban una estafa de 460.000 dólares, pero más adelante esa cifra superó el millón, realizada en quince transacciones distintas.

Los ataques del 51% son quizá los más preocupantes porque, frente a otros basado en introducir códigos malignos para robar información confidencial o secuestrar ordenadores, estos se basan en utilizar las propias reglas del juego de blockchain en beneficio propio.

Importancia de la confianza

El futuro de blockchain depende en gran medida en que se pueda mantener la confianza de los usuarios en su funcionamiento. La cadena de bloques implica pasar de fiarnos en las personas con las que nos relacionamos comercial o contractualmente, y en las instituciones que respaldan esas relaciones, a depositar toda nuestra confianza en la tecnología.

La revista *The Economist* denominó a blockchain como la *“máquina de la confianza”*, pues nos permite realizar transacciones con otros participantes a los que no conocemos de nada, confiando ciegamente para ello en las herramientas criptográficas y matemáticas del sistema, y en el funcionamiento correcto del protocolo de consenso.

Solamente una certeza absoluta del público en su seguridad garantizará su expansión. Pero, como indica Vitalik Buterin, cofundador de Ethereum, esto implica una contradicción: *“se supone que la mayor ventaja de la tecnología blockchain es que es más segura, pero a la gente le cuesta confiar en nuevas tecnologías, y esta paradoja no puede ser evitada”.*

Imagen de David McBee en Pexels