Recibido: 03.02.2022 • **Aceptado:** 01.03.2023

Palabras clave: Blockchain, ciberseguridad, criptomonedas, sistemas descentralizados, transacciones seguras.

Seguridad en transacciones electrónicas utilizando ***blockchain***

RICARDO ROMERO MÉNDEZ
rromerom@uaslp.mx
ALEJANDRA GUADALUPE SILVA TRUJILLO
asilva@uaslp.mx
ALBERTO RAMOS BLANCO
beto@uaslp.mx
FACULTAD DE INGENIERÍA, UASLP

En los últimos 30 años, la sociedad ha experimentado un notorio progreso en la manera en que se comparte información. Con la aparición del internet, en la última década del siglo XX, se logró que mucha información digital estuviera a disposición de todos aquellos que contaran con una computadora y conectividad de red. Desde entonces se han desarrollado varias plataformas de navegación en internet como Netscape, Yahoo Search, Google, entre otras; plataformas para compartir videos como YouTube, Netflix, Prime Video, Disney Plus; y también plataformas de redes sociales como MySpace, MetroFlog, con mayor popularidad Facebook, Twitter e Instagram; plataformas de compras *online* como Amazon, eBay, Alibaba, Mercado Libre. Con el adviento de las mencionadas plataformas, los consumidores de las mismas se volvieron generadores de contenidos, pues todas tienen una característica en común: requieren de un intermediario que administra el sistema de forma centralizada y se beneficia de la información que los usuarios proporcionan, al comercializar con los datos para que estos mismos se conviertan en clientes potenciales de empresas orientadas alas preferencias de búsqueda de los consumidores.

Seguridad, almacenamiento de datos y servicios bancarios

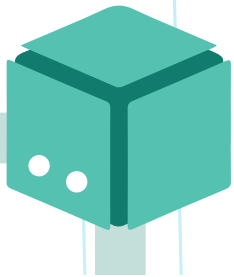
Con el internet se desarrollaron servicios web de almacenamiento de datos, con ellos los bancos crearon plataformas para sus transacciones y servicios. Aunque no se ha logrado dotar a los usuarios de un medio cien por ciento seguro para realizar transacciones de información bancaria, lo cual ha provocado que de manera simultánea al desarrollo de estos servicios, hayan crecido los delitos cibernéticos que han logrado, en ocasiones, violar la secrecía de la información y realizar operaciones fraudulentas a clientes de bancos o chantajear a famosos con información robada de servicios de almacenamiento de datos. Como ejemplos recientes de delitos cibernéticos de este tipo puede mencionarse el ataque sufrido por J. P. Morgan, compañía de servicios bancarios, víctima en 2014 de robo de información de 76 millones de usuarios. Otro caso es el ataque sufrido por el banco Capital One, en 2019, en cuyo caso se robó información de 100 millones de clientes, con un costo para la compañía de al menos 680 millones de dólares. Finalmente, el ataque al oleoducto Colonial Pipeline, en mayo de 2021, donde los piratas cibernéticos tomaron control de las contraseñas necesarias para operar el sistema del oleoducto y solicitaron un rescate millonario, dejando sin servicio a millones de usuarios de la costa este de Estados Unidos de América.

La ciberseguridad es considerada en la actualidad la mayor amenaza al desarrollo de los sistemas bancarios electrónicos. Esto es así, ya que las organizaciones sufren amenazas de diversas fuentes y es difícil determinar qué es importante cuidar; ello ha encarecido los servicios que requieren las empresas. En consecuencia, están abiertas a nuevas tecnologías que brinden mayor ciberseguridad para sus operaciones, algo que hace algunos años era impensable, pues las empresas financieras habían optado por sistemas centralizados de almacenamiento de información de usuarios y servicios, los cuales son fácilmente ubicables y en caso de un ataque exitoso, ponen en riesgo la información de un número masivo de usuarios o de organizaciones completas.

El *blockchain*

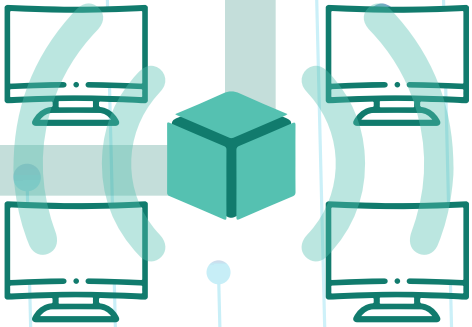
Una alternativa para los sistemas de información centralizados de bancos y organizaciones es la tecnología de *blockchain* o cadena de bloques, la cual proporciona una alternativa de ciberseguridad robusta; a pesar de ser una alternativa esperanzadora aún tiene muchas limitaciones, las cuales, en conjunto con sus ventajas serán exploradas a continuación.

Nueva transacción
Se solicita una nueva transacción a Blockchain, una base de datos descentralizada

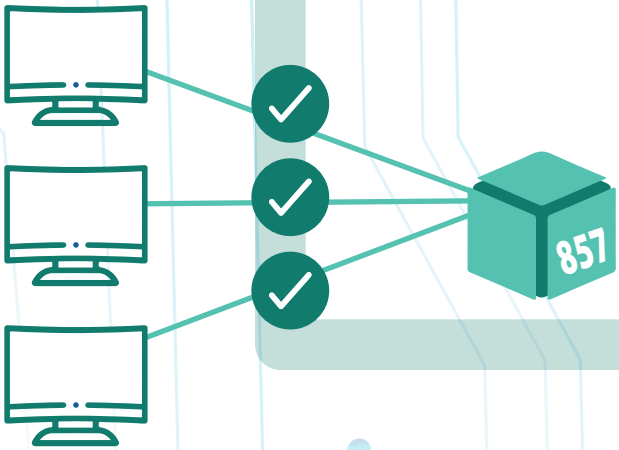


Creación del bloque
La transacción es representada por un bloque

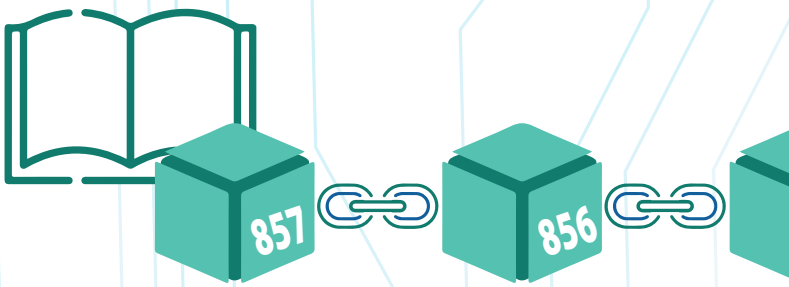
Minar
Los nodos mineros verifican esta transacción y la ponen en un bloque con otras transacciones



Transmisión
La transacción es transmitida a todos los nodos de la red



Confirmación
Los demás nodos confirman el trabajo del minero



Blockchain
El bloque es agregado al blockchain junto a los démas bloques y se realiza la transacción

Transacciones por *blockchain*

Vale la pena mencionar que *blockchain* no es una compañía o un producto, sino una plataforma tecnológica descentralizada, un software o protocolo para realizar transacciones sin intermediarios. El primero en sentar las bases para esta plataforma fue Satoshi Nakamoto, de quien se desconoce su identidad y se cree que es un seudónimo usado por la persona o grupo de personas que crearon el protocolo Bitcoin, quien o quienes en un artículo publicado en 2008 sentaron las bases de un sistema de red entre pares (P2P o *peer-to-peer*) de transacciones digitales, el cual funciona gracias a una serie de nodos que se comportan como iguales entre sí.

La plataforma *blockchain* es por naturaleza una red en la cual no existe una autoridad o ente que la opere ni centralice la información de las transacciones, sino que a través de un gran número de nodos, que son equipos de cómputo y servidores de voluntarios, distribuye de manera instantánea los libros o carpetas electrónicas de las transacciones financieras u otra información. De este modo, se distribuye la toma de decisiones respecto a la operación financiera y resulta casi imposible para los delincuentes cibernéticos tomar control de las operaciones, pues ello implicaría la infección simultánea de un gran número de equipos de cómputo, algo que requiere una acción concertada prácticamente imposible de lograr (Gupta, 2020).

Una vez que se distribuye la información de una operación financiera o de otro tipo en la red de blockchain, es prácticamente inasequible modificar las condiciones de la operación. La plataforma blockchain basa la toma de decisiones en un mecanismo de consenso, el cual requiere que de los miles de nodos entre los que se distribuye la misma información de una operación tengan un consenso, es decir, que al menos un 51 por cierto de los nodos coincidan en la información que comparten de forma electrónica (Gupta, 2020). Por lo tanto, es casi imposible para los delincuentes cibernéticos modificar la operación, pues para ello deberían infectar más del 51 por ciento de las computadoras donde está depositada la información. Ello implica una labor titánica, primeramente para ubicar los diferentes nodos que comparten la información, luego para tomar control de cada una de estas computadoras; esta misma dificultad es la principal fortaleza de una plataforma de transacciones como *blockchain*.

Una descripción figurativa de lo que ocurre en una transacción de *blockchain* es el problema de los generales de Bizancio (Lamport, Shostak y Pease, 2019), la cual es una analogía en donde se presenta a cuatro generales que planean atacar una ciudad, pero en dicha estrategia al menos tres de ellos deben atacar al mismo tiempo para derrotar al ejército de la ciudad. La única forma de comunicación posible entre ellos es a través de mensajes, y no saben si alguno de los generales es un traidor. Si uno de ellos es traidor, puede modificar el mensaje y ocasionar que los otros fracasen y la única forma de reconocer a un general traidor es compartir entre todos ellos el historial de mensajes para así comprobar que no han sido alterados. Si la mayoría de los generales evidencian que uno de ellos ha enviado un mensaje diferente, reconocerán al traidor e ignorarán su mensaje porque no habrá consenso con los demás mensajes enviados. Si la mayoría de los generales son leales, sólo prevalecerá el mensaje correcto.

¿Cómo funciona?

El mecanismo por el cual se logra que una red de *blockchain* sea segura es

Las organizaciones y empresas están abiertas a nuevas tecnologías que brinden mayor ciberseguridad, blockchain es una alternativa

conocido como *proof of work*, es de consenso descentralizado y solicita a los miembros de una red de bloques realizar una operación matemática. Cuando se efectúa una operación se genera un libro (*ledger*) que contiene un registro de todas las operaciones realizadas, organizadas en bloques secuenciales, de modo que es imposible efectuar operaciones repetidas con un mismo recurso. Para evitar la alteración de ese registro, el libro se hace público y se distribuye. Se asigna a esta operación una cadena de números que sirve como prueba de unanimidad entre bloques, lo cual al sustituirlo en una función de consenso (*hash function*), producirá un solo número de consenso (*hash number*) (Di Pierro, 2017). Cualquier versión alterada de ese dato es rechazada por el resto de los bloques. Dicha función es de un solo sentido, por lo que implica que no puede ser utilizada para obtener el dato original, sino solo para asegurar que los datos que originaron el número de consenso concuerdan con los datos originales. Los bloques de una transacción se actualizan cada cierto tiempo y esta acción es realizada por un minero (*miner*) que obtiene el derecho de actualizar un libro si es capaz de proporcionar la respuesta o número de consenso. El minero continuamente propone números aleatorios hasta que obtiene aquel que es el número de consenso. Es imposible calcular ese número, pero los mineros utilizan prueba y error hasta que lo obtienen. El minero presenta este número a la red y si concuerda con el de consenso, se acuerda que su bloque será el siguiente de la cadena de bloques (*blockchain*). Este mecanismo asegura que sólo quien ha invertido suficiente poder computacional (*proof of work*) en proponer números hasta atinar el correcto, ganará el derecho de actualizar el libro de esta operación, con una consiguiente ganancia para él. Este es un incentivo para que todos los participantes de la red actúen de manera honesta y sólo registren operaciones verdaderas, además de que, al ser *proof of work* un método que requiere de un gran esfuerzo de cómputo para tratar de controlar la red, es casi imposible realizar operaciones maliciosas debido a la necesidad de consenso.

En resumen, las transacciones inicialmente son agrupadas en bloques. Los usuarios o nodos compiten por resolver un acertijo matemático complicado, que requiere un gran esfuerzo computacional, para designar quién añadirá un nuevo bloque de transacciones a la cadena de bloques previos. Después de que se ha añadido un nuevo bloque, una mayoría de los usuarios debe comprobar la autenticidad de la información y añadir otros bloques a la cadena. Debido a que todos están interconectados y dependen de bloques previos, es imposible alterar o borrar operaciones anteriores. Por ello, *blockchain* es prácticamente inmutable. La única manera de corromper una operación en *blockchain* es poseer más del 51 por ciento de los nodos, pero como éstos deben estar realizando operaciones matemáticas para ganar la posibilidad de proponer el siguiente bloque, resulta prácticamente incosteable tratar de hackear transacciones en blockchain. Hasta la fecha nadie ha sido capaz de conducir un ataque con dicho porcentaje de nodos para alterar una transacción.

Retos

El uso computacional que *blockchain* requiere para "minar" es extensivo, lo que conlleva un gran uso de energía eléctrica, razón por la cual la mayoría de los mineros buscan instalar sus servidores en regiones de electricidad barata. Otra desventaja es el tiempo que conlleva realizar una operación; mientras que *blockchain* puede realizar entre 55 y 120 operaciones por segundo, Visa, la empresa dedicada a facilitar transferencias electrónicas de fondos a través del uso de tarjetas de crédito y débito, puede realizar hasta 70 000 transacciones por segundo. Estas dos limitaciones hacen difícil el ascenso de la tecnología Blockchain para que pueda competir con intermediarios de servicios financieros.

Con el fin de buscar alternativas que permitan el crecimiento de la tecnología *blockchain*, se han propuesto otros mecanismos de consenso. Uno de ellos es el conocido como *proof of stake*, el cual en lugar de mineros tiene validadores.

RICARDO ROMERO MÉNDEZ

Es doctor en Ingeniería Mecánica por el Departamento de Ingeniería Aeroespacial y Mecánica de la Universidad de Notre Dame en South Bend, Indiana, EUA. Actualmente es secretario general de la Facultad de Ingeniería de la UASLP y desarrolla el proyecto "Modelado de transferencia de calor en calentadores solares de placas y tubos".

Para ser seleccionado como validador, se debe apostar una cierta cantidad de moneda corriente. A mayor sea la oferta es más probable ser elegido de manera aleatoria como el siguiente validador. Si es elegido y se modifica maliciosamente la operación a través de operaciones fraudulentas, los demás nodos no aprobarán ese consenso y el validador perderá la moneda corriente que apostó; de lo contrario, si actúa honestamente y sigue las reglas, será premiado con una recompensa. Este mecanismo de *proof of stake* salva las desventajas de excesivo consumo energético y lentitud de *proof of work*; sin embargo, tiene otras desventajas, ya que favorece injustamente a los nodos de actores más ricos, además de no ser considerado tan robusto como *proof of work*.

A pesar de las desventajas mencionadas, *blockchain* es una tecnología que al paso de sus apenas trece años de creación, ha ido ganando adeptos. La industria financiera es vista como una de las usuarias primarias del concepto y las organizaciones financieras han reconocido sus ventajas en cuanto a robustez y seguridad (Nofer *et al*., 2017). Otro ejemplo de la implementación de una red *blockchain*, son las criptomonedas, consideradas un instrumento virtual que cumple las funciones de una divisa (Lozano, 2022), de hecho, una criptomoneda es una de las formas más conocidas de implementar una red *blockchain*. Los bancos centrales de una buena cantidad de países han incluido criptomonedas como parte de sus posibilidades para las transacciones mercantiles. Apenas el 29 de diciembre de 2021, el Banco Central de México anunció la creación de su criptomoneda Central Bank Digital Currencies (CBDC), controlada por el Estado para la realización de transacciones en plataformas de bitcoin: "por considerar de suma importancia estas nuevas tecnologías y la infraestructura de pagos de última generación como opciones de gran valor para avanzar en la inclusión financiera en el país" (Darinka Rodríguez, 2021), y también para competir con criptomonedas tales como bitcoin, ethereum. Lo mismo ha hecho la mayoría de los países de economías desarrolladas.

A manera de cierre, podemos decir que la tecnología *blockchain* ofrece ventajas importantes en la seguridad en transacciones de todo tipo. A pesar de las desventajas aquí mencionadas, ha ganado aceptación, pero aún se siguen buscando opciones de consenso que la vuelvan más competitiva con las plataformas mercantiles a través de intermediarios financieros como Visa y PayPal.

Vale la pena mencionar que, a pesar de que *blockchain* tiene una relación mayor con las criptomonedas, tales como bitcoin y ethereum, su uso potencial es mucho más extenso. La tecnología *blockchain* puede utilizarse para todo aquello que requiera una contabilidad auditable y 100 por ciento confiable sin necesidad de intermediarios, como por ejemplo: para cadena de suministros, expedientes médicos, registros notariales, declaración y pago de impuestos, comercio de arte, entre otros. Puede ser que aún no necesites usar *blockchain*, pero se prevé que en un futuro no muy lejano, no podrémos vivir sin él y que ni siquiera nos daremos cuenta de que lo estamos utilizando. UP

Referencias bibliográficas:

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260. Recuperado de: https://bitcoin.org/bitcoin.pdf

Aishwary Gupta (productor). (junio, 2020). *Blockchain Geeks* [Podcast Series]. Recuperado de: https://open.spotify.com/show/6icfSDbLAwU2Lbj0bO0VGS?si=_YdaSnc0Ru2udIlD_ETQ4g

Lamport, L., Shostak, R. y Pease, M. (2019). The Byzantine generals problem. En Dahlia Malkhi (Ed.), *Concurrency: the Works of Leslie Lamport* (pp. 203-226). Nueva York, EUA: Association for Computing Machinery.

Nofer, M., Gomber, P., Hinz, O. y Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), pp. 183-187.

M. Di Pierro (2017). What Is the Blockchain? *Computing in Science & Engineering*, 19(5), pp. 92-95. DOI: 10.1109/MCSE.2017.3421554.

Lozano, D.P. (2022). Criptomonedas y Blockchain en el ámbito financiero: un análisis de correlación. *Revista de Métodos Cuantitativos para la Economía y la Empresa*, 34, pp. 328-358. DOI: 10.46661/revmetodoscuanteconempresa.6650

Darinka Rodríguez (30 de diciembre de 2021). México prepara una nueva moneda digital para 2024, *El País*. Recuperado de: https://elpais.com/mexico/2021-12-31/mexico-prepara-una-nueva-moneda-digital-para-2024.html