

Blockchain, una mirada a la descentralización de las transacciones y de la información

Resumen

Las nuevas tecnologías de la información pueden generar valor a las empresas e industrias en una forma disruptiva y, dependiendo de su envergadura y proyección de crecimiento, también cambiar el mundo y la forma de conectarlo. *Blockchain* es una de ellas e incide en el modelo actual de negocios, en industrias como la financiera y de bienes raíces, generando una mejora en los servicios para brindar mayor valor a los clientes.

Este artículo busca explorar las bases del funcionamiento de la tecnología *blockchain*, sus principales características y las primeras aplicaciones, además de reflexionar hacia dónde se dirige y el impacto que podría generar.

Palabras claves

Blockchain, *bitcoin*, descentralización, base de datos, distribuida.

Rafael Bettín Díaz

Introducción

Dada la constante evolución de la tecnología y teniendo en cuenta que en promedio cada diez años surge el siguiente gran paradigma tecnológico, vale la pena estar a la vanguardia de los acontecimientos más recientes en

este campo. Desde los años 70 hemos pasado de las tarjetas perforadas al uso actual de la nanotecnología y los dispositivos móviles inteligentes, sumados a los desarrollos que produjo la aparición de Internet y ahora *blockchain* o bloque de cadenas.

De acuerdo con Swan (2015), *blockchain*, en su forma más precaria, “se comporta como el libro mayor en donde se almacenan todas las transacciones que se han ejecutado” [traducción del autor]. Su funcionamiento es como una base de datos que en una forma descentralizada permite almacenar transacciones e información de valor [traducción del autor] (Gates, 2017, Chapter I), todo esto bajo el concepto de libro mayor distribuido o DLT¹ por sus siglas en inglés. Cada transacción en este gran libro mayor se verifica por consenso de la mayoría de los participantes de la red y, una vez introducida la información, ésta no puede ser borrada, modificada o alterada [traducción del autor] (Crosby, Nachiappan, Pattanayak, Verma, & Kalyanaraman, 2015, p. 1).

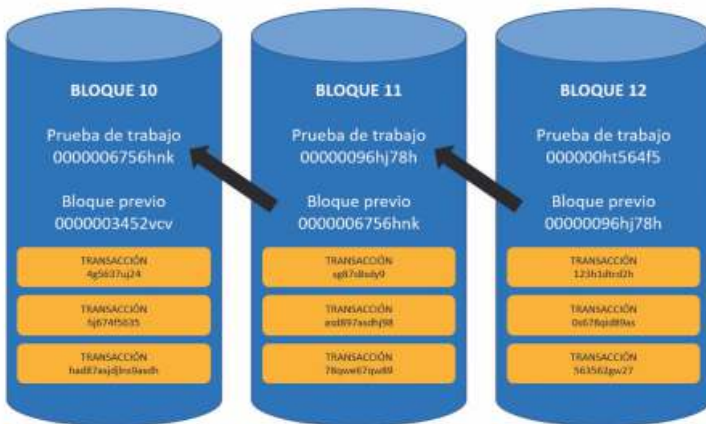
Para entender de una forma práctica los conceptos alrededor de *blockchain*, haremos referencia a una de las múltiples aplicaciones que esta tecnología puede tener, como lo es *bitcoin*, la moneda digital dada a conocer en un artículo titulado "Bitcoin: Un sistema

de efectivo electrónico Peer-to-Peer" (2008), de Satoshi Nakamoto, cuya identidad sigue siendo desconocida. *Bitcoin* permite a las personas realizar transacciones financieras directamente, sin una autoridad intermediaria y en cualquier otra moneda digital o efectivo electrónico en el mercado, fundamentadas en la tecnología *blockchain*.

Inicialmente, Satoshi describió una versión *peer-to-peer* de efectivo electrónico que permitiría los pagos en línea directamente de una parte a otra, sin tener que pasar a través del concepto de una institución financiera y cuyo almacenamiento de las transacciones se realizaría a través de cadenas de bloques; con cada bloque reciente o transacción, conectado o añadido a un bloque precedente y el bloque anterior a otro bloque precedente; en ese orden se forma una cadena de bloques o transacciones autenticadas y validadas mediante una firma digital. (Ver imagen 1)

¹ Distributed Ledger Technology

Imagen 1 : Almacenamiento de información y transacciones en *blockchain*



Fuente: Creación del autor.

Todo el sistema de *blockchain* por ser descentralizado y distribuido está construido en la confianza y la transparencia debido a que la identidad de los participantes es desconocida y la única autenticación se realiza a través de claves digitales, mediante la ejecución de varios algoritmos matemáticos [traducción del autor](Icahn, 2017, p. 10).

Actualmente, la importancia de esta tecnología recae en las diferentes aplicaciones que, gracias a las investigaciones realizadas alrededor de ella, se han podido desarrollar, ampliando de manera significativa su alcance, rompiendo paradigmas y de una forma disruptiva incursionando en diferentes procesos que funcionan de manera centralizada, entre ellos los servicios bancarios, los bienes raíces y los procesos asociados a la cadena de abastecimiento.

Blockchain: ¿cómo funciona?

Una de las formas más fáciles para explicar el funcionamiento de *blockchain* es a través de una transacción financiera, simulando una transferencia des-

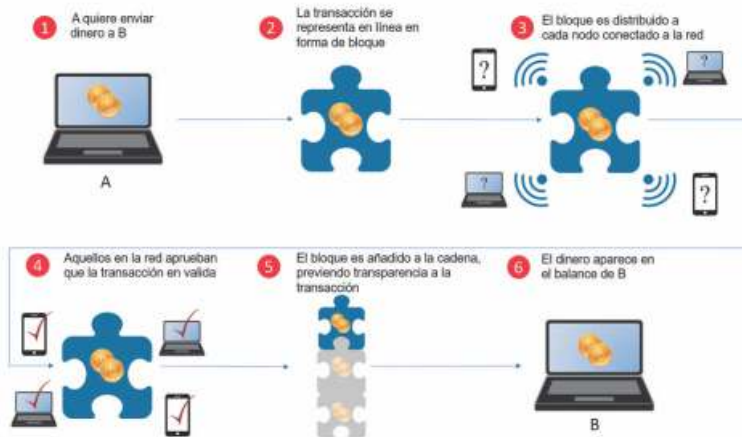
de el origen A, hasta el destino B, como se muestra en la Imagen 1.

Una vez que la transacción es creada por el sujeto A (1), se representa en línea como un bloque junto con muchas otras transacciones realizadas en el mismo período de tiempo (2); En este punto, con el fin de verificar la validez del certificado de esta transacción, se utilizan diferentes algoritmos matemáticos (funciones hash²) para cifrar la firma digital empleada para enviar la transacción. Este bloque creado, ahora se está transmitiendo a toda la red de nodos conectados (3) y todos los nodos conectados a la red *blockchain* verifican si la transacción es válida o no; este proceso se conoce como prueba de trabajo³ y puede tardar hasta 10 minutos, aproximadamente. Una vez que la transacción es validada y

² Las funciones hash: estas funciones son un algoritmo matemático que "toma algunos datos de entrada y crea algunos datos de salida" [traducción del autor] (Sean, 2016), Esto significa que una función hash se llevará a una entrada de cualquier longitud y tendrá una salida de longitud fija.

³ Prueba de trabajo: Se permite que cada nodo *blockchain* conectado a mantener transacciones segura y alcanzar un acuerdo resistente a la manipulación [traducción del autor] (Icahn, 2017, p. 18).

Imagen 2: Transacción financiera utilizando la tecnología *blockchain*



Fuente: (Crosby et al., 2015, p. 10)

aprobada por todos los nodos conectados (4), el bloque es finalmente añadido a la cadena (5); todo este proceso de 1 a 5 se conoce como minería⁴. Al final, el sujeto B puede ver la transacción reflejada en su balance (6).

Características de *blockchain*

Durante el desarrollo de este artículo hemos mencionado algunas de las características de esta tecnología, cómo funciona y algunos de sus usos potenciales. Ahora vamos a enfatizar en ciertos beneficios y oportunidades como la descentralización de la información y la trazabilidad en las transacciones, según Gates (2017) y Swan (2015). Adicionalmente, revisaremos algunos de los riesgos asociados, debido al manejo de redes públicas y otros aspectos relacionados con la seguridad.

Beneficios y oportunidades de la tecnología

- La transparencia es una de las mejoras más significativas de *blockchain*.
 - No hay intermediarios involucrados en el proceso.
 - Utiliza una red descentralizada.
 - Crea confianza entre los participantes de la red que, aunque nunca se han visto, pueden realizar transacciones entre sí.
 - La seguridad es proporcionada a través de la trazabilidad.
 - Todos los datos introducidos en *blockchain* son inmutables, inalterables o inmodificables.
 - *Blockchain* puede ser fácilmente auditable.
 - Ofrece múltiples usos, casi cualquier tipo de activos se pueden grabar en ella.
- La tecnología es bastante asequible, sin necesidad de grandes inversiones ni infraestructuras complejas. Ya hay plataformas basadas en *blockchain* como *Ethereum*⁵ que nos permiten crear aplicaciones descentralizadas (Dapps⁶).
 - *Costo reducido*, toda vez que con un solo libro es posible mantener registros de las transacciones realizadas.
 - Como es distribuida ayuda a aumentar la velocidad de la transacción. Esto se debe a que elimina los intermediarios y todo el mundo puede auditar y verificar la información registrada en ella.

Riesgos asociados a la tecnología

- Por lo general, las redes *blockchain* son públicas y están envueltas en falta de seguridad; significa que todo el mundo será capaz de ver las transacciones y el balance de todos los participantes de la red. Vale la pena resaltar que también hay *blockchains* privadas, que poco a poco han ido tomando más auge en los mercados.
- Las claves públicas y privadas⁷ en *blockchain* proporcionan al usuario la capacidad de realizar cualquier clase de transacción, dependiendo del tipo de red *blockchain* utilizada. Al perder una de las dos claves (pública o privada) se pierde todo y no hay manera de recuperar la información.

⁴ Minería: Se refiere a añadir nuevos bloques de registros (transacciones) en la contabilidad pública de *Blockchain*.

⁵ "Es una plataforma *Blockchain* que es pública y tiene una funcionalidad de transacciones programables" [traducción del autor].

⁶ "Ejemplos de las aplicaciones que se ejecutan en una red P2P de los ordenadores en lugar de un único equipo".

⁷ Es como el nombre de usuario y contraseñas que la mayoría de la gente utiliza como identificadores en cualquier otra aplicación.

A pesar de que la descentralización es algo por lo que sobresale esta tecnología, también puede ser una de las razones para que su adopción tome más tiempo, debido a que ninguna organización tiene control sobre *blockchain*.

- La red *blockchain* todavía tiene problemas de escalabilidad, debido a los tiempos empleados en minería y validación de las transacciones; el proceso puede ser más lento que con otras aplicaciones transaccionales centralizadas.
- Aún existe poca confianza por parte de la gente para utilizar este tipo de tecnologías en las que la información, dependiendo del tipo de *blockchain* implementada, puede ser pública.
- La regulación de los gobiernos y de las instituciones bancarias puede ser un problema al cual se enfrentará *blockchain* a lo largo del camino.
- La integración con los sistemas existentes y heredados es uno de los puntos críticos de esta tecnología, especialmente para las instituciones bancarias, debido al costo de la migración y la sustitución de los sistemas.

Aplicaciones en diferentes industrias

En servicios financieros

La principal área de estudio para los negocios y empresas alrededor de *blockchain*, es la combinación de los servicios financieros tradicionales con esta nueva tecnología. Para ello, la Red de Información Interbancaria (RII) de los más prestigiosos bancos a nivel mundial ha unido esfuerzos con el fin de investigar los posibles usos de esta tecnología y la forma de crear una red

global que permita realizar transacciones entre sus clientes y sus mismas entidades filiales. Ahora, los bancos con sucursales a nivel regional podrán realizar movimientos financieros entre éstas sin tener que retransmitir esos fondos a través de un intermediario” [traducción del autor] (Swan, 2015, p. 11).

En recaudación de fondos

Con el uso de tecnologías como *blockchain*, el modelo de negocios actual para los servicios de recolección de fondos de inversión (*crowdfunding*) cambiaría completamente; antes se necesitaba un servicio centralizado como *Kickstarter* o *Indiegogo* para permitir una campaña de *crowdfunding*, Ahora, con *blockchain* se elimina la necesidad de un tercero intermediario.

También se habilita la posibilidad de que los *startups* recauden fondos mediante la creación de sus propias monedas digitales y vendan "acciones criptográficas" a los inversionistas interesados. Estos últimos, en este tipo de campañas, mediante *blockchain*, reciben un *token*⁸ que representa las acciones de la empresa en la que han invertido [traducción del autor] (Swan, 2015, p. 12).

Con los contratos inteligentes⁹

Muchas de las industrias que utilizan la tecnología *blockchain* van a hacer uso

8 Unidad de valor emitida por una entidad privada (BBVA, 2017).

9 De acuerdo con los contratos de Smart Alliance - En colaboración con Deloitte, Nick Szabo describió un contrato inteligente, como un conjunto de promesas digitales, incluidos los protocolos y condiciones, que las partes estuvieron de acuerdo para llevar a cabo esas promesas [traducción del autor] (2016).

de contratos inteligentes y podrán intercambiar algo de valor en forma automática. Si se cumplen las condiciones de un contrato, los pagos o el intercambio de valor son realizados de acuerdo con sus términos. Del mismo modo, si no se cumplen las condiciones del contrato, los pagos pueden ser retenidos [traducción del autor] (Swan, 2015, Chapter VIII). Actualmente, empresas como Walmart en Estados Unidos, tienen este modelo como piloto para la compra de carne de cerdo desde Asia y gestionar la operación con sus proveedores.

Con Internet de las cosas¹⁰ (IOT)

IoT se está convirtiendo rápidamente en una tecnología popular para el consumidor y las empresas. Una gran mayoría de las plataformas de IoT se basa en un modelo centralizado, en el que como agente o *hub* controla la interacción entre los dispositivos. Sin embargo, este enfoque es poco práctico para muchos escenarios en los que los dispositivos necesitan intercambiar datos entre sí de forma autónoma.

Este requisito específico ha llevado a esfuerzos hacia IoT con plataformas descentralizadas. La tecnología *blockchain* facilita la implementación de estas plataformas descentralizadas para el intercambio de datos seguros y sobre todo para la confianza de la información, así como para el mantenimiento de registros. Este tipo de arquitectura, *blockchain* sirve como el libro mayor y mantiene un registro confiable de todos los mensajes intercambiados entre los dispositivos inteligentes en una topología IoT descentralizada [traducción del autor] (Crosby et al., 2015, p. 17).

En la cadena de suministro

En una implementación *blockchain*, un contrato inteligente puede desencadenar la transferencia de valores automáticos basados en condiciones. Basta imaginar un rastreador GPS¹¹ en un barco que desencadena un pago realizado en un instante a través de *blockchain*, una vez que la ubicación GPS de la nave demuestra que el buque ha llegado al destino del comprador [traducción del autor] (Hua & Notland, 2016, pp. 22, 23). En la industria de la cadena de suministro, las aplicaciones de *blockchain* están generando nuevos modelos para su mejora y automatización, permitiendo a los diferentes actores conocer toda la información de los diferentes productos, desde su cultivo hasta la entrega al cliente final, pasando por los diferentes procesos de transformación, lo que permite una fácil identificación y generación del certificado de origen de los mismos, sobre todo si hablamos del mercado de alimentos orgánicos.

El futuro de *blockchain*

“La tecnología más probable que cambie la próxima década de los negocios no es la web social, los grandes datos, la nube, la robótica, o incluso la inteligencia artificial. Es la blockchain ...” (Tapscott & Tapscott, 2016).

La cadena de suministro puede ser uno de los procesos que en este mo-

10 Internet de las cosas (IoT por sus siglas en inglés) “Es un término utilizado para una red de dispositivos que comprenden los frigoríficos, cámaras de seguridad, automóviles, aviones, computadoras, etc. ha existido durante un tiempo bajo diferentes formas y nombres” [traducción del autor](Guartime, 2017).

11 Sistema de Posicionamiento Global.

mento tiene más flexibilidad para adoptar esta tecnología; no obstante, su aplicación está actualmente bajo investigación por parte de las grandes compañías tecnológicas que seguramente integrarán la minuciosa de toda la cadena de valor *blockchain* del proceso, donde las empresas podrán realizar transacciones entre sí con un único “libro mayor” compartido para todas las transacciones, donde el tiempo y el papeleo que están gastando se pueden reducir considerablemente. Como parte de esta evolución vendrá sus integraciones con el sistema actual, con el fin de no hacer traumático el proceso de adopción, donde la tecnología se ejecutará en una capa de tecnología diferente a las que conocemos ahora, lo cual la hace transparente para el usuario final.

Por otro lado, esta tecnología todavía tiene un largo camino por recorrer, muchos obstáculos que superar y confianza que ganar. Las entidades y los gobiernos tienen que establecer una mayor regulación para ayudar con su adopción y las empresas empiezan a avanzar hacia nuevos modelos, servicios y propuestas tecnológicas basadas en *blockchain*. También, la infraestructura alrededor dará forma al futuro de la tecnología, para reducir su costo y rápida adopción.

Para el corto tiempo que lleva en el mercado ha avanzado ampliamente en su investigación, dando lugar a *blockchain* 1.0, para el uso en monedas digitales; posteriormente, *blockchain* 2.0, surgió para los contratos inteligentes y su aplicación con IoT; y, por último, *blockchain* 3.0, el estado actual de esta tecnología para diferentes industrias, a través del desarrollo de *Dapps*. Entre los sectores que en

un futuro próximo adoptarán *blockchain* como base para sus procesos figuran: el seguimiento de los impuestos, las entidades reguladoras, las cuales tendrán la oportunidad de conocer en tiempo real los movimientos financieros de todo el mundo y con antelación su patrimonio; la votación en línea y el almacenamiento en la nube. La información se distribuye en muchos servidores conectados a la red que todavía mantiene la privacidad de la información; la identidad digital será posible mediante el seguimiento de una persona desde su nacimiento, por cada documento relacionado con ella (Icahn, 2017).

Referencias

- BBVA. (2017, July 7). BBVA | Qué es un “token” y para qué sirve. Retrieved November 15, 2017, from <https://www.bbva.com/es/que-es-un-token-y-para-que-sirve/>
- blockchainhub.net. (n.d.). What is a dApp? Decentralized Application on the Blockchain. Retrieved October 10, 2017, from <https://blockchainhub.net/decentralized-applications-dapps/>
- Bresett, M. (2017). Ethereum: What You Need to Know about the Block Chain Based Platform.
- Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2015). Blockchain Technology Beyond Bitcoin. Sutardja Center for Entrepreneurship & Technology Technical Report, Berkeley University of California, 35.
- Gates, M. (2017). Blockchain: Ultimate guide to understanding blockchain,

- bitcoin, cryptocurrencies, smart contracts and the future of money. (First Edition).
- Guartime. (2017). Internet of Things Authentication: A Blockchain solution using SRAM Physical Unclonable Functions, 16.
- Gupta, M. (2017). Blockchain For Dummies®, IBM Limited Edition. John Wiley & Sons, Inc. Retrieved from www.wiley.com
- Hua, A. V., & Notland, J. S. (2016, December 19). Blockchain enabled Trust & Transparency in supply chains. NTNU School of Entrepreneurship, Norway. Retrieved from <http://www.the-blockchain.com/docs/Blockchain%20enabled%20Trust%20&%20Transparency%20in%20supply%20chains.pdf>
- Icahn, G. (2017). BLOCKCHAIN: The Complete Guide To Understanding Blockchain Technology. Amazon Digital Services LLC.
- Satoshi Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, 9.
- Sean. (2016, November 29). If you understand Hash Functions, youll understand Blockchains. Retrieved October 5, 2017, from <https://decentralize.today/if-you-understand-hash-functions-youll-understand-blockchains-9088307b745d>
- Smart Contracts Alliance, & Deloitte. (2016). Smart Contracts: 12 Use Cases for Business & Beyond A Technology, Legal & Regulatory Introduction. Chamber of Digital Commerce, 55.
- Swan, M. (2015). Blockchain: Blueprint for a new economy (First Edition). California, United States: OReilly Media, Inc.
- Tapscott, D., & Tapscott, A. (2016, May 10). The Impact of the Blockchain Goes Beyond Financial Services. Retrieved October 13, 2017, from <https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services> 🌐

Rafael Bettín Díaz. Ingeniero de Sistemas de Información, Especialista en Gerencia de Proyectos, Est. Maestría en Ingeniería de Procesos. Actualmente y por lo últimos 3 años me he desempeñado como Gerente de Proyectos de implementación y desarrollo de software de gestión empresarial.