«Blockchain»: ¿nuevo paradigma?

Un mecanismo habilitado para gestionar, transmitir, autenticar y almacenar información compartiendo un registro distribuido, descentralizado y sincronizado entre todos los participantes, en lugar de utilizar las tradicionales bases de datos centralizadas, puede transformar el mundo tal como lo conocemos hoy. Un primer paso firme hacia el Internet del Valor.

Irene Peña @IrenePCuenca | *Consultora senior área Corporate Finance de Afi*
Verónica López Sabater @VLopezSabater | *Consultora senior área Economía Aplicada de Afi*

Blockchain (literalmente, cadena de bloques) es una tecnología de contabilidad distribuida (DLT, por sus siglas en inglés) que llegó a nuestras vidas en torno a 2009 materializado en un activo digital considerado por muchos como moneda virtual o criptomoneda –el bitcoin (฿)– que asumió el protagonismo asociado a dicha tecnología.

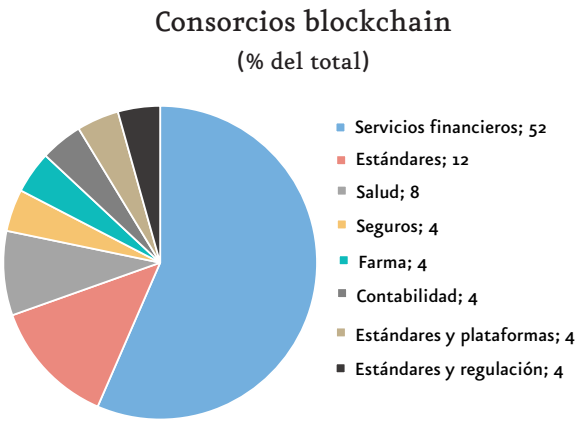
Si bien la criptomoneda ha sido hasta la fecha la aplicación más aterrizada y popular de esta tecnología sobre cuyo protocolo (Bitcoin, con mayúsculas) se han desarrollado miles de criptomonedas alternativas –algunas que compiten, otras que colaboran con bitcoin– la creación de un sistema electrónico de pago entre pares no es más que una de las múltiples aplicaciones que se están desarrollando en la actualidad, la mayoría de ellas en fase de prueba de concepto y sustentadas en contratos inteligentes o *smart contracts* (SC) y tokenización de activos.

Si originalmente la tecnología *blockchain* se podía entender como una amenaza para entidades bancarias al permitir independizar los servicios financieros de los bancos, son precisamente estos los que han liderado en los primeros años el esfuerzo inversor en proyectos para desarrollar soluciones e innovaciones basadas en *blockchain*, en su mayoría centrados en mecanismos de compensación y liquidación. En términos globales, IBM prevé que el 15% de los bancos mundiales estará utilizando *blockchain* a finales de 2017, y un 66% a finales de 2021.

[iStock]/Thinkstock.

Pero sus aplicaciones son incluso más interesantes en otras industrias tales como la energética, sanitaria y educativa, entre muchas otras. Del análisis realizado por William Mougayar, experto en *blockchain* y autor de «The Business Blockchain», a finales de 2016 existían 25 consorcios globales desarrollando diversas iniciativas *blockchain*, con más de 550 miembros de distintas industrias, siendo la financiera la más representativa.

En 2017, sin embargo, observaremos una mayor presencia de consorcios multisectoriales, como el recientemente anunciado en España –Red Lyra– primera plataforma tecnológica multisectorial del mundo, basada en *blockchain*, con todos sus nodos en territorio español para garantizar la legalidad, de la que forman parte como socios fundadores Banco Santander,



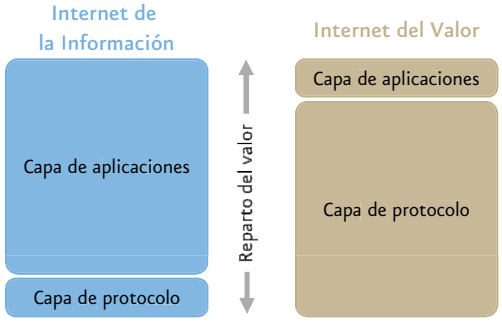
Fuente: *Mougayar W. (2016) State of Blockchain Consortia.*.

BBVA, Bankia, Banco Sabadell, BME, Caja Rural, Cajamar, Cepsa, Endesa, Gas Natural Fenosa, Iberdrola, Correos, Ejaso, Everis, Garrigues, Grant Thornton, Comillas ICADE, MásMóvil, Momopocket, Notarnet y Roca Junyent y Scytl.

La Red Lyra tiene como objetivo desarrollar de forma colaborativa un sistema de identidad digital, basado en SC sobre Ethereum (del que hablamos a continuación) sobre el que cada participante podrá desarrollar aplicaciones de forma competitiva (capa aplicaciones).

Próximamente la Red Lyra se constituirá en asociación sin ánimo de lucro y abrirá las puertas a nuevos socios participantes.

DEL INTERNET DE LA INFORMACIÓN AL INTERNET DEL VALOR



Fuente: «*Blockchain: La revolución industrial de internet*».

Respecto a Ethereum, este protocolo no fue concebido, a diferencia de Bitcoin, para servir como una red de pagos Su criptomoneda nativa –ehter (Ξ)– es la moneda de pago creada para actuar como «gasolina» para la máquina virtual de Ethereum y está destinada únicamente a premiar a los desarrolladores, permitir que los clientes paguen por las aplicaciones y las operaciones que se desarrollan dentro de la plataforma, y evitar el spam.

Creado por Vitalik Buterin[1] de la Fundación Ethereum, busca promover la I+D+i y educación para universalizar los protocolos y herramientas descentralizadas a través de la colaboración con desarrolladores y conseguir universalizar las aplicaciones descentralizadas, los contratos inteligentes (*smart contracts*) y las organizaciones autónomas descentralizadas en torno a la tecnología *blockchain*, desarrollado originalmente, eso sí, como una versión mejorada del protocolo Bitcoin.

Las dos únicas infraestructuras públicas sólidas y fiables hoy en día según los expertos son Bitcoin y Ethereum, sobre las que se pueden desarrollar otras aplicaciones (*sidechains*, cadenas de bloques que tienen otras funcionalidades). De hecho, los creadores de la red Ethereum consideran que las *blockchain* privadas tienen poco recorrido global por dos motivos fundamentales, la seguridad y la construcción de una comunidad: Ethereum cuenta con más de 70.000 desarrolladores que de forma colaborativa –a cambio

PRINCIPALES CONSORCIOS *BLOCKCHAIN* - SECTOR FINANCIERO

- **Ripple Consensus Network**. Desarrolló su protocolo *blockchain* en código abierto (Ripple Transaction Protocol, RTXP y su moneda nativa XRP) en 2012. Ripple es hoy en día la única red *blockchain* bancaria (con estándares, reglas y gobierno definidos) para pagos internacionales, esto es, un sistema de liquidación bruta en tiempo real (LBTR).
- **Ethereum Entreprise Alliance**, consorcio que busca desarrollar, sobre la red Ethereum, estándares de industria de forma colaborativa, comenzando por la mejora de la latencia en la liquidación interbancaria, la mejora de la transferencia en cadenas de suministro y la creación de mercados P2P en los que los intermediarios tradicionales sean prescindibles. Entre los socios fundadores destacan Accenture, Banco Santander, BNY Mellon, CME Group, ConsenSys, Intel, JP Morgan y Microsoft. A estos se sumaron posteriormente BBVA, Credit Suisse, ING, Thomson Reuters, UBS y Wipro.
- **R3CEV**, consorcio liderado por la Fintech R3 al que ya se han sumado más de cuarenta entidades financieras. Ha desarrollado el protocolo Corda con la expectativa de que se convierta en el estándar para el sector y base de creación de nuevos productos financieros, protocolo que se abrió recientemente al integrarse en el consorcio Hyperledger.
- **Hyperledger**, plataforma de código abierto operativa desde 2015 por Linux Foundation, enfocada a transacciones globales en la que participan, entre otros, London Stock Exchange, IBM, Wells Fargo, SWIFT, JP Morgan, CISCO y los consorcios R3CEV y Digital Assets Holdings. Como dato representativo, SWIFT –*Society for Worldwide Interbank Financial Telecommunication*– es precisamente la asociación bancaria que desde 1977 centraliza los servicios de mensajería entre entidades financieras para pagos transfronterizos, y que blockchain podría reemplazar.
- **Digital Assets Holding**, consorcio integrado por Accenture, IBM, BNP Paribas, Goldman Sachs, DTCC, ABN AMRO, Citi, CME Group, JP Morgan, Broadbridge, Innoventures y Banco Santander, entre otros.
- **B3i**, consorcio formado por las 5 principales aseguradoras europeas (Aegon, Allianz, Munich Re, Swiss Re, Zurich), para estudiar las posibilidades del *blockchain* en su sector.
- **Symbiont Distributed Ledger** fue anunciado en octubre de 2016 como la primera plataforma de emisión y *trading* de valores inteligentes (*Smart securities*).

Fuente: *Afi*.

de ether, la gasolina de Ethereum– crean nuevos protocolos en código abierto, a disposición de la sociedad para agilizar el tránsito de la Internet de la Información a la Internet del Valor.

En España, BBVA, Banco Santander y CECABANK son las entidades que –hasta el reciente anuncio de constitución de la Red Lyra– lideraban el esfuerzo inversor en esta tendencia a través numerosas iniciativas tanto propias como a través de consorcios. Así, por ejemplo, BBVA es miembro del consorcio R3CEV, Banco Santander lo es de *Digital Assests Holding* y ambas entidades son miembro de la *Enterprise Ethereum Alliance* (EEA) y de Ripple. En el marco de este último, BBVA realizó recientemente el primer piloto real de transferencias internacionales con dinero fiduciario. CECABANK, por su parte, ha creado con Grant Thornton el primer consorcio bancario de *blockchain* en España con el objeto de desarrollar las primeras aplicaciones bancarias sustentadas en la tecnología *blockchain*.

Pero, ¿qué es *blockchain* y qué lo hace tan diferencial?

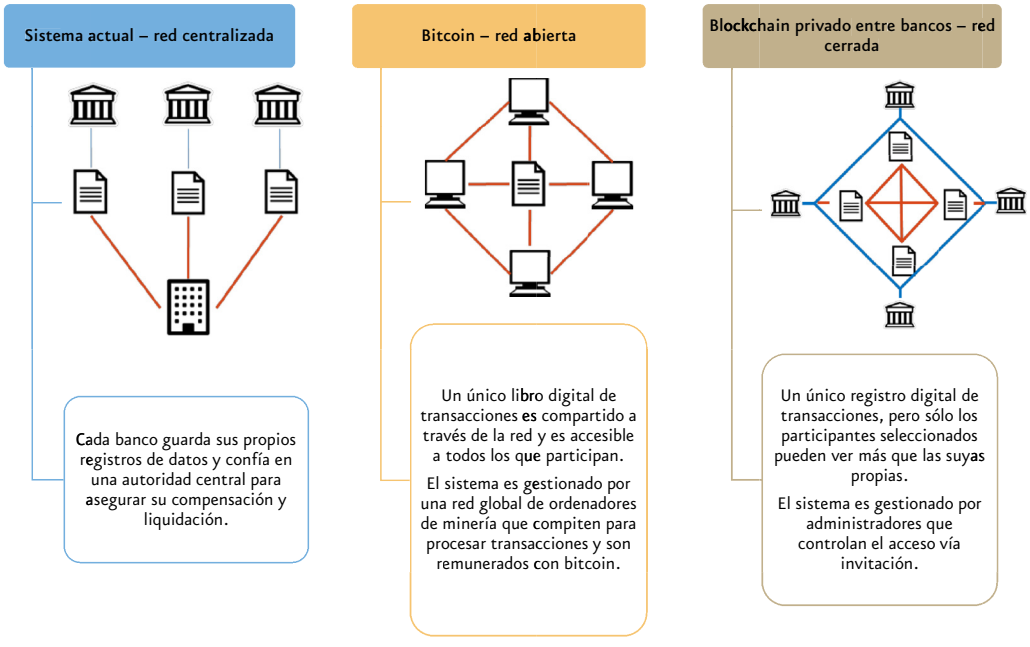
Blockchain es un protocolo de transferencia segura de datos, un libro de contabilidad en el que se crea una cadena de transacciones en bloques, cada una verificada y sellada por una tercera parte independiente que no es una autoridad central sino un conjunto de participantes (mineros), que validan transacciones por consenso. La cadena de bloques está disponible para la consulta de cualquiera, pudiéndose reconstruir la secuencia histórica de transacciones realizadas entre las partes.

Una de las principales características de la tecnología *blockchain* es el concepto de inmutabilidad. Cada cadena de bloques en la que se registra la transferencia de datos puede llegar a estar copiada en un gran número de nodos –ordenadores o servidores independientes– , copias que llevan aparejado un número de serie o *hash*, de longitud fija, que identifica la transacción y que es común en todas las copias del bloque. De este modo, para alterar los datos de la transferencia de datos, no basta con alterar un único bloque sino que es preciso alterar las múltiples copias que existen de dicho bloque, lo que en la práctica lo hace materialmente imposible. Se trata, por tanto, de un mecanismo consensuado, ya que muchos ordenadores (nodos) han de ponerse de acuerdo para decidir y validar lo que ha pasado.

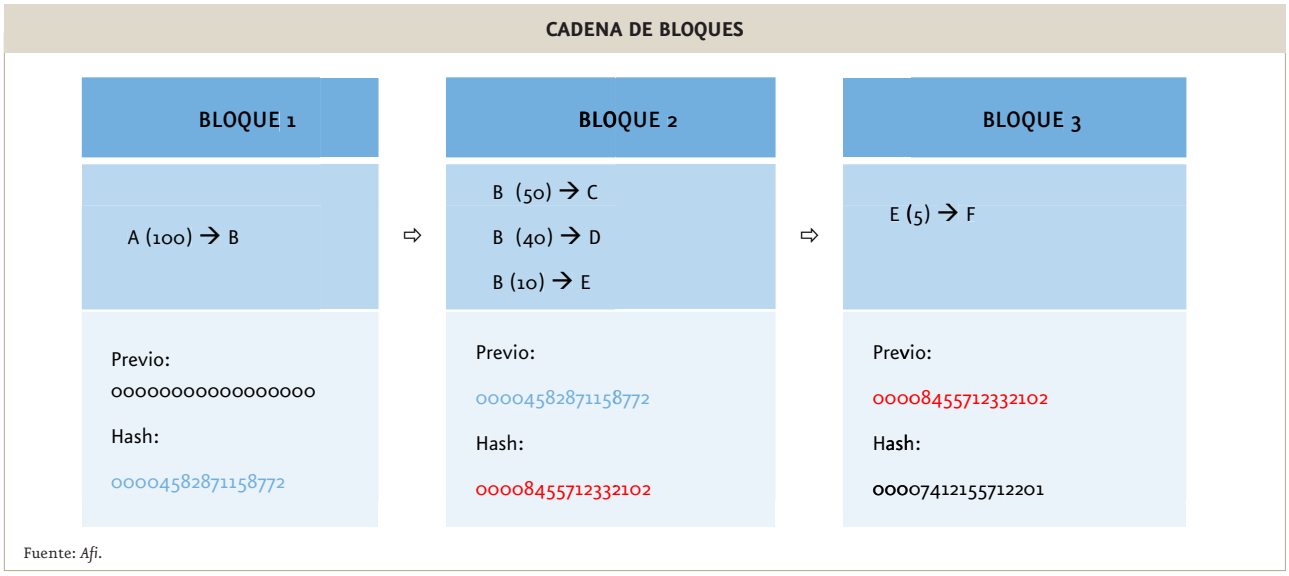
Para una serie de transacciones nos encontraremos, en lugar de con un único bloque, con una cadena de bloques. Cada nuevo bloque identificará al bloque anterior mediante su *hash*, permitiendo alcanzar consenso sobre una transacción concreta así como sobre lo que pasó en el pasado. Fijándonos, por ejemplo, en el bloque 3, podremos comprobar que E puede hacer una transferencia de 5 unidades a F ya que en el bloque 2 hemos observado que B transfirió a E 10 unidades.

La posibilidad de comprobar que la transferencia de propiedad se ha producido sin que exista duda ha sido otra de las grandes disrupciones de esta tecnología. Hasta la aparición del protocolo Bitcoin, desarrollado en 2008 por Satoshi Nakamoto (pseudónimo), los pagos entre pares (P2P) basados en una red des-

BANCA Y *BLOCKCHAIN*



Fuente: *Reuters*.



Fuente: *Afi*.

centralizada no se habían podido desarrollar porque existía un problema de confianza que daba lugar al conocido «problema del doble gasto».

El problema del doble gasto consiste en que dado que un fichero digital se puede reproducir infinitamente, tradicionalmente había necesario que un intermediario (sistema centralizado) verificase el origen y destino de las transacciones. Sin embargo, el protocolo Bitcoin resuelve este problema ya que todos los movimientos quedan identificados por medio de su *hash*, que no se puede alterar sin la confirmación por parte de todas las copias, y registrados de manera ordenada en el libro de contabilidad distribuido. Así mismo, si una transacción se alterara (pirateara) todos los bloques posteriores quedarían modificados (cambiaria el *hash*) y tendrían que ser también alterados.

Gracias a este sistema de verificación, autoridades financieras y agentes privados a nivel global están explorando las posibilidades de la tecnología *blockchain* para sus funciones de compensación y liquidación multilateral de pagos y de valores.

Y es que *blockchain* tiene un enorme potencial para mejorar la eficiencia, autenticidad y registro de cualquier proceso que requiera «dar fe» de su realización efectiva y correcta: contratos, registros de propiedad (inmobiliaria, intelectual, etc.), contraprestaciones, etc. en la medida en que permite «obviar» la necesidad de una autoridad central que certifique las transacciones ya que estas permanecen registradas e inalterables en un libro de contabilidad permanente y validado de forma distribuida (por consenso de los participantes).

Además del registro de transacciones financieras, los atributos de esta tecnología permitirán su utilización para la transacción de cualquier activo que tenga valor, ya sea tangible (un edificio, una obra de arte) o intangible (horas de trabajo, títulos académicos) mediante su tokenización, esto es, mediante la emisión de derechos sobre un activo e que habilitarán la transimisión libre y segura de la propiedad en *blockchain*, abriendo infinitas posibilidades a nuevas formas de comercio (comercio 4.0). A ello se unen nuevas modalidades de contratación (contratos inteligentes o *Smart contracts*) y la creación de nuevas figuras organizativas como las organizaciones autónomas descentralizadas (DAO, por sus siglas en inglés) sobre las que trataremos en un próximo artículo en esta sección de Empresa Global.

Retos

Los principales retos a los que los diversos desarrollos de la tecnología *blockchain* se enfrentan a mediados del 2017 son fundamentalmente de tres tipos: tecnológicos, políticos y legales.

Entre los retos relacionados con la tecnología destacan (i) la latencia (tiempo de procesamiento / validación de transacciones), reto que enfrenta bitcoin con mayor urgencia dado que la cola de cadenas de bloques en espera de confirmación no hace más que crecer; (ii) la escalabilidad –la aspiración de alcanzar escala global, y (ii) el elevado consumo energético fruto del proceso de minado– proceso del que la Red Lyra, por ejemplo, se ha independizado al decidir contar con tokens que representan euros. Otros de carácter técnico (escalabilidad, capacidad de la red, amenaza del *hackeo* por consenso del 51%, etc.) y el coste de sustitución de la infraestructura *legacy*, especialmente en el sector financiero, forman parte de esta categoría de retos.

Entre los retos políticos se encuentra la dificultad de alcanzar reglas de consenso robustas entre la comunidad participante de la correspondiente red

blockchain, tanto en la fase de diseño de red como en el momento en que sea necesario modificar las reglas por motivos técnicos, como actualmente está sucediendo con la comunidad Bitcoin.

Entre los retos legales, en general, las autoridades consideran que es aún pronto para poder elaborar una opinión definitiva sobre esta tecnología y sus aplicaciones, con especial incidencia en algunas jurisdicciones. Por señalar aquellos retos más relevantes, destacamos: (i) la falta de un marco jurídico que reconozca al *blockchain* como fuente de veracidad inmutable y a prueba de manipulación para su uso como prueba de existencia o propiedad de la información incorporada en la plataforma (identidad digital); (ii) la multiplicidad de jurisdicciones territoriales potencialmente afectas en los SC; (iii) la dotación de identidad digital a los objetos para la aplicación de *blockchain* a la Internet de las cosas; (iv) la tokenización de activos reales, dado que implica su desmaterialización, y (iv) el derecho al olvido.

Sobre este último, señalar que la inmutabilidad de los datos podría entrar en conflicto directo con este derecho recogido en el artículo 17 del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, de obligado cumplimiento en mayo de 2018. Algunos expertos indican que este reto podría resolverse sustituyendo el derecho a la «eliminación» de información de carácter personal por el de «imposibilidad de uso» por parte de terceros.

La realidad es que, una vez identificados los retos, solo es cuestión de tiempo y trabajo resolverlos, y son muchos los agentes dedicados a encontrar soluciones factibles, de forma colaborativa.

Desde Afi consideramos que es muy difícil apostar por un escenario realista en el que en 10 años no estemos conectados de una forma u otra a *blockchain*, como hoy lo estamos a Internet, y que contemos con una identidad digital en *blockchain* a la que asociemos nuestros activos tangibles e intangibles (reputación) ::

Lecturas recomendadas

1. ESMA, 2016 Discussion Paper The Distributed Ledger Technology Applied to Securities Markets
2. WEF, 2016: The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services
3. Preukschat, A. (Coordinador), 2017 Blockchain: La revolución industrial de internet

[1] 2013 WhitePaper, 30-07-2015 software y 1er bloque.