

4 Tecnología de cadena de bloques (*blockchain*)

La última disrupción en el sistema financiero

Los libros contables de cadena de bloques (*blockchain*) eluden la infraestructura financiera centralizada. Esto lleva al desarrollo de nuevos negocios y a la revisión de los existentes. Para el sector financiero podría implicar la mayor disrupción que ha habido hasta la fecha.

¿Qué es la cadena de bloques (*blockchain*)?

Blockchain es una contabilidad pública entre pares que se mantiene mediante una red distribuida de ordenadores y que no requiere ninguna autoridad central ni terceras partes que actúen como intermediarios. Consta de tres componentes fundamentales: una transacción, un registro de transacciones y un sistema que verifica y almacena la transacción. Los bloques se generan a través de software de código abierto y registran la información sobre cuándo y en qué secuencia ha tenido lugar la transacción. Este "bloque" almacena cronológicamente información de todas las transacciones que tienen lugar en la cadena, de ahí el nombre de cadena de bloques o *blockchain*. Dicho de otro modo, una *blockchain* es una base de datos con información horaria estampada e inmutable de cada transacción que se replica en servidores de todo el mundo. Esta tecnología es la base de bitcoin, una moneda criptográfica³.

En las transacciones tradicionales, como las transferencias de dinero o de divisas, normalmente hay un intermediario o una entidad centralizada que registra la transmisión de dinero o de divisas y que existe de forma independiente. En *blockchain*, el propio *token* o moneda digital es lo que tiene valor, que viene determinado por el mercado. Esto es lo que hace que el sistema sea un intercambio verdaderamente descentralizado. Cuando las personas compran o venden bitcoins, se envía una clave secreta o *token* al sistema. Los "mineros" utilizan nodos, ordenadores o dispositivos conectados a una red para identificar y validar la transacción, utilizando copias de todo o alguna información de *blockchain*. Antes de que la red acepte la transacción, los mineros tienen que mostrar una "prueba de trabajo" utilizando una función de almohadilla criptográfica: un algoritmo especial que tiene por objeto proporcionar altos niveles de protección. Los mineros reciben algún tipo de remuneración por su contribución a la potencia informática, evitando así la necesidad de un sistema centralizado. Los nuevos protocolos como *Ripple* se basan en un proceso de consenso que no necesita mineros ni prueba de trabajo y que puede aceptar los cambios de *blockchain* en segundos.

En cualquier caso, *blockchain* ofrece un nivel inherente de confianza para el usuario, con lo cual se elimina la necesidad del intermediario y se reduce el riesgo de error humano. En esta contabilidad pública, los datos están protegidos contra la manipulación y la revisión, y los individuos no pueden sustituir partes de la *blockchain*, pues el costo de hacerlo es importante: hipotéticamente habría que controlar más de la mitad de los "nodos" para alterar clandestinamente la *blockchain*. De este modo se garantiza que no se duplica el gasto. Sin embargo, algunos estudios muestran que defraudar al sistema creando transacciones falsas sería posible dependiendo de la potencia informática, la posición del atacante y el momento del ataque.

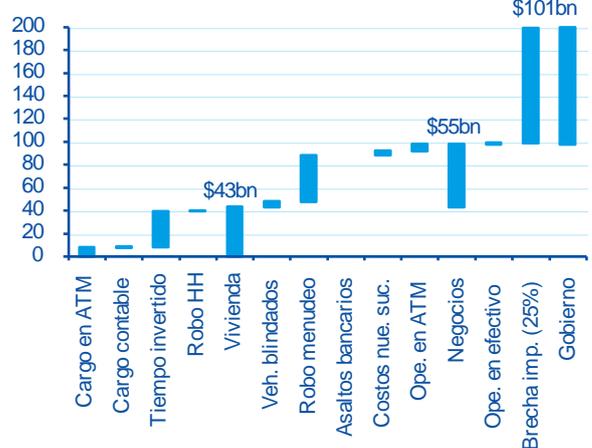
3: Para más información sobre Bitcoin, véase el Observatorio Económico Global *Bitcoin: un capítulo en la adopción de la moneda digital*, disponible en: https://www.bbva.com/wp-content/uploads/migrados/130731_ObservatorioEconomicoEEUU_Bitcoin_tcm346-398292.pdf

Figura 4.1
Bitcoin: transacciones por día y tasa de hash (TH/s)



Fuente: blockchain.info

Figura 4.2
Coste del dinero en efectivo en EEUU (mmd, anual)



Fuente: BBVA Research e Instituto Fletcher

La disrupción

Aunque el propio Bitcoin ha recibido muchas críticas, se considera que la tecnología de *blockchain* ofrece un gran potencial, por lo que atrae la atención de gobiernos, empresas y capital de riesgo a un ritmo rápido. Entre las ideas que se han desarrollado en los últimos años se incluye el sistema de pago por servicio, que permite a los usuarios transmitir video; una estructura que permite compartir espacio-información del programa o formas de registrar información empresarial como las auditorías. En la mayoría de los casos, se cree que estas opciones ofrecen mayor seguridad, rapidez y fiabilidad a una fracción del costo de las infraestructuras más tradicionales.

Otras ideas son por ejemplo la posibilidad de alquilar el exceso de capacidad de almacenamiento, la creación de identidades digitales que podrían sustituir a docenas de nombres de usuario y contraseñas y ofrecer al mismo tiempo mejores características de seguridad, y "contratos inteligentes" con propiedades de aplicación automática que convertirían el contrato en "indisoluble". Además, ha habido importantes avances en la creación de un sistema de votación digital muy seguro. Los votantes se inscriben en línea y reciben un voto electrónico o una voto-moneda exclusivos. Los votos electrónicos se registran en la *blockchain*, reduciendo así la posibilidad de fraude y permitiendo a la vez que la red haga una verificación rápida y confiable. Esto podría resultar atractivo si tenemos en cuenta que se han producido importantes anomalías incluso en democracias bien establecidas (por ejemplo, en las elecciones presidenciales del año 2000 en EE.UU.), pues cada votante podría verificar su decisión. Con ello se podría aumentar la participación y reducir los costos.

En el sector financiero, las instituciones han sido lentas en reconocer el potencial de la tecnología de *blockchain*; sin embargo, muchos grandes bancos han invertido considerables sumas de dinero en esta tecnología. Esta atención probablemente es el resultado de lo disruptiva que es dicha tecnología para el sector financiero, especialmente si permite la simplificación masiva de los procesos bancarios y reduce notablemente los costos.

Los primeros niveles de disrupción parecen más probables en el espacio de los pagos, donde transacciones tradicionales como las transferencias de dinero, los pagos con tarjetas de crédito y de débito, las remesas, los pagos de divisas y en línea requieren un intermediario, como una cámara de compensación bancaria o

una entidad financiera. En estos casos, la transacción ocurriría directamente entre el comprador y el vendedor sin ningún intermediario y la validación de la transacción se produciría de forma descentralizada o en una "contabilidad distribuida". El resultado sería un importante ahorro en infraestructura para los bancos, lo que les permitiría evitar las redes de pago, que a menudo son lentas, incómodas y caras.

Sin embargo, el mayor impacto potencial de una contabilidad pública podría ir más allá del sistema de pagos. Dado que la mayoría de los activos financieros, como bonos, valores, derivados y préstamos ya son electrónicos, sería posible que algún día todo el sistema se reemplazara por una estructura descentralizada. De hecho, las últimas innovaciones utilizan *tokens* para almacenar y comercializar activos como valores, bonos, automóviles, casas y productos básicos. Las llamadas "monedas de colores" llevan información adicional sobre el activo, lo que genera una "propiedad inteligente" o la capacidad de registrar y hacer transacciones con estos activos utilizando "contratos inteligentes", que se imponen por medio de algoritmos complejos a través de plataformas distribuidas sin un registro centralizado, aumentando así su eficiencia. En este entorno, el sistema actual en que las entidades financieras registran las cuentas de los individuos de forma centralizada y las reservas de los bancos se almacenan en el banco central (por ejemplo la Reserva Federal) se sustituiría por el "Internet del dinero" o el "Internet de las finanzas", un sistema financiero completamente descentralizado.

Riesgos y desafíos

La probabilidad de que un sistema descentralizado se convierta en algo común no está clara, ya que tendría que ofrecer el mismo o un mayor nivel de confianza y protección que el sistema actual. Para que esto ocurra, el sistema debe disponer de una gran cantidad de potencia informática y afrontar de forma eficiente el enorme consumo energético que se requiere. Además, no está claro cómo este sistema podría lidiar con las cuestiones legales y regulatorias, así como con asuntos de seguridad nacional, como el lavado de dinero, el fraude, la evasión fiscal o el terrorismo. Además, las monedas digitales no estarían a salvo de accidentes potenciales; al igual que el sistema actual, si su uso alcanza niveles sustanciales, estos choques podrían generar riesgos sistémicos y graves crisis económicas. En este escenario, la política monetaria no podría responder de forma eficaz si no puede impulsar la demanda entre una gran proporción de agentes económicos que utilizan monedas digitales.

No obstante, las mejoras y modificaciones de la tecnología *blockchain* podrían superar algunos de estos obstáculos y dar lugar a una aceptación más generalizada. Por tanto, ahora la pregunta clave no es cómo sino cuándo la disrupción será de amplio alcance. Como ha sucedido en otros sectores que se han transformado por las nuevas tecnologías y la digitalización, la tecnología *blockchain* podría reestructurar el sector financiero mucho más allá del sistema de pagos.

AVISO LEGAL

El presente documento, elaborado por el Departamento de BBVA Research, tiene carácter divulgativo y contiene datos, opiniones o estimaciones referidas a la fecha del mismo, de elaboración propia o procedentes o basadas en fuentes que consideramos fiables, sin que hayan sido objeto de verificación independiente por BBVA. BBVA, por tanto, no ofrece garantía, expresa o implícita, en cuanto a su precisión, integridad o corrección.

Las estimaciones que este documento puede contener han sido realizadas conforme a metodologías generalmente aceptadas y deben tomarse como tales, es decir, como previsiones o proyecciones. La evolución histórica de las variables económicas (positiva o negativa) no garantiza una evolución equivalente en el futuro.

El contenido de este documento está sujeto a cambios sin previo aviso en función, por ejemplo, del contexto económico o las fluctuaciones del mercado. BBVA no asume compromiso alguno de actualizar dicho contenido o comunicar esos cambios.

BBVA no asume responsabilidad alguna por cualquier pérdida, directa o indirecta, que pudiera resultar del uso de este documento o de su contenido.

Ni el presente documento, ni su contenido, constituyen una oferta, invitación o solicitud para adquirir, desinvertir u obtener interés alguno en activos o instrumentos financieros, ni pueden servir de base para ningún contrato, compromiso o decisión de ningún tipo.

Especialmente en lo que se refiere a la inversión en activos financieros que pudieran estar relacionados con las variables económicas que este documento puede desarrollar, los lectores deben ser conscientes de que en ningún caso deben tomar este documento como base para tomar sus decisiones de inversión y que las personas o entidades que potencialmente les puedan ofrecer productos de inversión serán las obligadas legalmente a proporcionarles toda la información que necesiten para esta toma de decisión.

El contenido del presente documento está protegido por la legislación de propiedad intelectual. Queda expresamente prohibida su reproducción, transformación, distribución, comunicación pública, puesta a disposición, extracción, reutilización, reenvío o la utilización de cualquier naturaleza, por cualquier medio o procedimiento, salvo en los casos en que esté legalmente permitido o sea autorizado expresamente por BBVA.

Este informe ha sido elaborado por la Unidad de Inclusión Financiera:

Economista Jefe

David Tuesta
david.tuesta@bbva.com

Javier Alonso
javier.alonso.meseguer@bbva.com

Noelia Cámara
noelia.camara@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

Isabel Vegas
isabel.vegas@bbva.com

Con la colaboración de:

Alfonso Arellano Espinar
alfonso.arellano.espinar.contractor@bbva.com

Sistemas financieros
Olga Cerqueira
olga.gouveia@bbva.com

España
Juan Ramón García
juanramon.gl@bbva.com

EEUU
Nathaniel Karp
Nathaniel.Karp@bbva.com

BBVA Research

Economista Jefe Grupo BBVA

Jorge Sicilia Serrano

Área de Economías Desarrolladas
Rafael Doménech
r.domenech@bbva.com

Área de Economías Emergentes
Alicia García-Herrero
alicia.garcia-herrero@bbva.com

Área de Sistemas Financieros y Regulación
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Áreas Globales

España
Miguel Cardoso
miguel.cardoso@bbva.com

Análisis Transversal de Economías Emergentes
Alvaro Ortiz
alvaro.ortiz@bbva.com

Sistemas Financieros
Ana Rubio arubiog@bbva.com

Escenarios Económicos
Julián Cubero
juan.cubero@bbva.com

Europa
Miguel Jiménez
mjimenezg@bbva.com

Asia
Le Xia
le.xia@bbva.com

Inclusión Financiera
David Tuesta
david.tuesta@bbva.com

Escenarios Financieros
Sonsoles Castillo
s.castillo@bbva.com

Estados Unidos
Nathaniel Karp
Nathaniel.Karp@bbva.com

México
Carlos Serrano
carlos.serranoh@bbva.com

Regulación y Políticas Públicas
María Abascal
maria.abascal@bbva.com

Innovación y Procesos
Oscar de las Peñas
oscar.delaspenas@bbva.com

Coordinación LATAM
Juan Manuel Ruiz
juan.ruiz@bbva.com

Política de Recuperación y Resolución
José Carlos Pardo
josecarlos.pardo@bbva.com

Coordinación Regulatoria Global
Matías Viola
matias.viola@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Perú
Hugo Perea
hperea@bbva.com

Venezuela
Oswaldo López
oswaldo.lopez@bbva.com

Interesados dirigirse a:

BBVA Research
Calle Azul, 4
Edificio de la Vela - 4ª y 5ª plantas
28050 Madrid (España)
Tel.: +34 91 374 60 00 y +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com