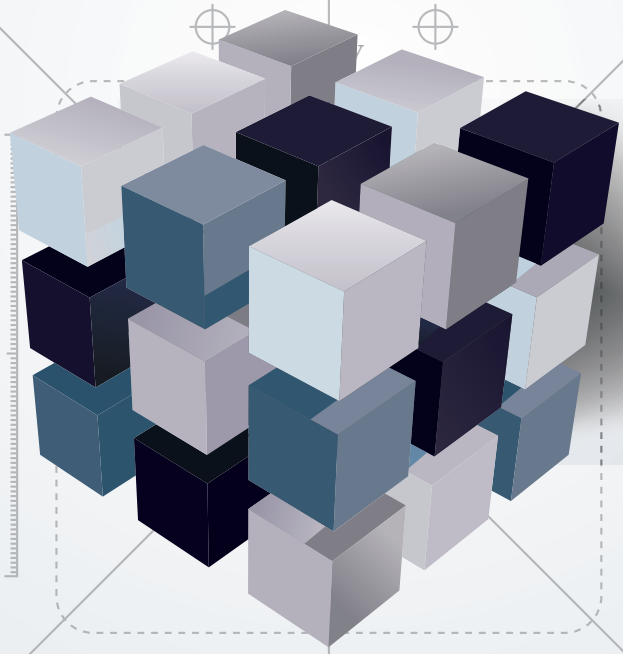
ALEX **PREUKSCHAT**
(COORDINADOR)

BLOCKCHAIN:
LA REVOLUCIÓN INDUSTRIAL DE INTERNET



Descubre la tecnología que transformará profundamente internet

Con la colaboración de los principales expertos españoles en Blockchain, entre ellos:
Carlos Kuchkovsky - BBVA
Gonzalo Gómez Lardies - IECISA
Daniel Díez García - everis
Íñigo Molero - OroyFinanzas.com

Alexander Preukschat (coordinador)
Carlos Kuchkovsky,
Gonzalo Gómez Lardies,
Daniel Díez García e Íñigo Molero

Blockchain: la revolución industrial de internet

Colaboradores:

José Luis Várez, Eusebio Felguera, Christoph Steck, Ignacio Madrid, Óscar Lage, Dioni Nespral, Roberto Díaz, Stefan Hamann, Covadonga Fernández, Roberto Fernández, Stefan Junestrand, Adolfo Contreras, Félix Moreno, Carlos Vivas, Javier Molina, Xavier Foz, Joaquim Matinero, José Ramón Morales, Cristina Carrascosa, Jaime Núñez, Víctor Escudero, Santiago Márquez, Luis Carlos García, Manuel Polo y Alex Puig

Gestión 2000

© Centro Libros PAPF, S.L.U., 2017
Gestión 2000 es un sello editorial de Centro Libros PAPF, S. L. U.
Grupo Planeta
Av. Diagonal, 662-664
08034 Barcelona

www.planetadelibros.com

ISBN: 978-84-9875-447-6
Depósito legal: B. 8.455-2017
Primera edición: mayo de 2017
Preimpresión: gama sl
Impreso por Black Print

Impreso en España - *Printed in Spain*

Sumario

Tercera parte. La tecnología blockchain

Capítulo 1
Los fundamentos de la tecnología blockchain

Álex Preukschat

Aunque generalmente hablamos de blockchain, lo cierto es que este concepto como tal no existe. O al menos no a secas, sino acompañado siempre de un adjetivo, de modo que podamos diferenciar entre «blockchains públicas», «blockchains privadas» o, incluso, «blockchains híbridas». No obstante, en general se puede hablar de una tecnología que ha llegado para quedarse y, más aún, para definir lo que será el mundo del futuro. Gracias a ella, el actual internet de la información alcanzará un nuevo paso evolutivo, que ya se ha dado en llamar internet del valor.

El consenso, la clave de la blockchain

Una blockchain no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. Expresado de forma más breve, es una base de datos descentralizada que no puede ser alterada. Otro elemento muy importante a tener en cuenta en ella es que, por definición, se trata de un sistema que permite que partes que no confían plenamente unas en otras puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos. El consenso es precisamente la clave de un sistema blockchain porque es el fundamento que permite que todos los participantes en el mismo puedan confiar en la información que se encuentra grabada en él. Se trata de un aspecto con un potencial increíble para transformar una infinidad de sectores clave de la industria y no menos de la sociedad en la

que vivimos, de tal modo que podría llegar a cambiar incluso nuestra forma de entender el mundo.

Desde un punto de vista técnico, ese sistema basado en la confianza y el consenso se construye a partir de una red global de ordenadores que gestionan una gigantesca base de datos. Ésta puede estar abierta a la participación de cualquiera que lo desee (hablamos entonces de una «blockchain pública») o bien limitada a sólo algunos participantes (caso de la «blockchain privada»), aunque siempre sin la necesidad de una entidad central que supervise o valide los procesos que se lleven a cabo.

La primera de todas las blockchains que han existido fue la blockchain pública de Bitcoin, lanzada en enero de 2009. En su funcionamiento juegan un papel importante términos como «minería», inspirado en la minería del oro y referido al proceso computacional necesario que opera para asegurar su red, la llamada «Prueba de Trabajo» (*Proof of Work*, en inglés, PoW). No obstante, para hacerse una idea del impacto que podría tener la blockchain en el mundo no es imprescindible entender desde un primer momento estos conceptos, en los que ya habrá ocasión de profundizar en los capítulos dedicados a criptografía, consenso y tecnología. En ellos podrás ver que no todas las blockchains se basan en la misma operativa y que incluso hay algunos proyectos que, a pesar de denominarse «blockchain», quizás no lo sean.

Los elementos básicos de la blockchain

Para entender el alcance de la tecnología blockchain hay que conocer los elementos básicos de que se compone. Son los siguientes:

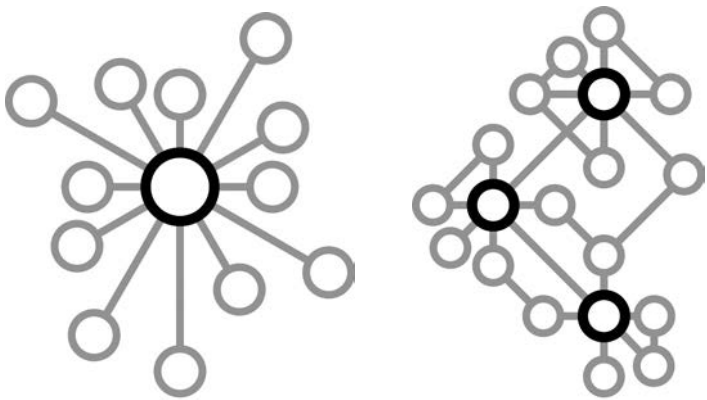
- **Un nodo:** puede ser un ordenador personal o, según la complejidad de la red, una megacomputadora. Con independencia de la capacidad de cómputo, todos los nodos han de poseer el mismo software/protocolo para comunicarse entre sí. De otro modo no podrán conectarse ni formar parte de la red de una blockchain, sea ésta pública, privada o híbrida. Si en una blockchain pública estos nodos no tienen por qué identificarse, en una blockchain

privada los nodos se conocen entre sí, pudiendo también ser iguales entre ellos.

- **Un protocolo estándar:** en forma de software informático para que una red de ordenadores (nodos) pueda comunicarse entre sí. Existen protocolos muy conocidos, como el TCP/IP para internet o el SMPT para el intercambio de correos electrónicos. El protocolo de una blockchain funciona de la misma forma: otorga un estándar común para definir la comunicación entre los ordenadores participantes en la red.
- **Una red entre pares o P2P (Peer-to-Peer, en inglés):** se trata de una red de nodos conectados directamente en una misma red. Un ejemplo muy conocido de red P2P es BitTorrent.
- **Un sistema descentralizado:** a diferencia de un sistema centralizado, donde toda la información está controlada por una única entidad, aquí son todos los ordenadores conectados los que controlan la red porque todos son iguales entre sí; es decir, no hay una jerarquía entre los nodos, al menos en una blockchain pública. En una privada sí puede haber jerarquía.

De lo dicho se desprende que una blockchain es un conjunto de ordenadores (o servidores) llamados «nodos» que, conectados en red,

Modelo de red centralizada y de red descentralizada.



utilizan un mismo sistema de comunicación (el protocolo) con el objetivo de validar y almacenar la misma información registrada en una red P2P. Podríamos decir que ésta sería la estructura «física», como lo es la carrocería en un coche... Pero ¿y el motor? El motor de la blockchain es la suma de todos esos elementos que logran que la información recogida no pueda modificarse porque complejos algoritmos criptográficos, sumados a la propia capacidad colectiva de la red, contribuyen a asegurar la irreversibilidad de la información.

Las claves de la tecnología blockchain

Una blockchain se compone de tres partes que, combinadas e integradas, cumplen un propósito determinado y fundamental. Son éstas:

- **La criptografía:** por tal entendemos un procedimiento que, utilizando un algoritmo con clave (clave de cifrado), transforma un mensaje sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo empleado. En la blockchain, la criptografía tiene la responsabilidad de proveer un mecanismo infalible para la codificación segura de las reglas del protocolo que rigen el sistema. Es también fundamental para evitar la manipulación, hurto o introducción errónea de información en la cadena de bloques, así como la responsable de generar firmas e identidades digitales encriptadas.
- **La cadena de bloques o blockchain:** es la base de datos diseñada para el almacenamiento de los registros realizados por los usuarios. Todas las blockchains han de actuar bajo las mismas reglas o protocolo para dar validez al bloque —y a la información recogida— e incorporarlo a la cadena de bloques. Una vez realizada esta tarea, la cadena continuará con la emisión del siguiente bloque, permaneciendo inalterable la información registrada a través de la criptografía. Esta forma de obrar elimina la necesidad de un tercer ente de confianza.

- **Un consenso:** se trata de una parte imprescindible entre los usuarios de la blockchain. Este consenso se sustenta en un protocolo común que verifica y confirma las transacciones realizadas, y asegura la irreversibilidad de las mismas. De igual modo, este consenso debe proporcionar a todos los usuarios una copia inalterable y actualizada de las operaciones realizadas en la blockchain.

Independientemente de si se opta por una cadena de bloques pública o privada, la combinación de estos tres elementos dentro del protocolo/software otorgan ese sello de calidad que certifica que es un motor blockchain.

Las blockchains públicas *versus* privadas

Como se ha dicho, la blockchain se puede dividir en dos grandes grupos: públicas y privadas. Siguiendo con nuestro ejemplo del coche, ambas poseen la misma carrocería y el mismo motor, sólo que ahora pueden optar por complementos diferentes, a gusto del consumidor. Las primeras blockchains fueron diseñadas para ser:

- **Públicas:** cualquier persona sin ser usuario puede acceder y consultar las transacciones realizadas.
- **Abiertas:** cualquier persona puede convertirse en usuario y participar del protocolo común si posee unos mínimos conocimientos técnicos.
- **Descentralizadas:** lo son en cuanto que no existe un usuario que tenga más poder que otro en la red y todos los nodos son iguales entre sí.
- **Pseudoanónimas:** los propietarios de transacciones no son identificables personalmente, pero sus direcciones sí son rastreables debido a su carácter público. Por eso, la mayoría de blockchains públicas no pueden ser anónimas, excepto aquellas expresamente diseñadas para ser anónimas.

Por definición, una blockchain pública es una red descentralizada de ordenadores que utilizan un protocolo común asumido por todos

los usuarios y que permite a éstos registrar transacciones en el libro mayor (*ledger*, en inglés) de la base de datos. Esas anotaciones son inalterables, si bien los participantes en una blockchain de estas características pueden verificar de forma independiente y por consenso los cambios que se realizan en los registros.

Las unidades de cuenta que se utilizan en las blockchains públicas muchas veces se denominan tokens.[2] Un token no es más que una serie de dígitos que representan un registro dentro de la cadena de bloques. Por ejemplo, una cadena alfanumérica como 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy es un token. Por tanto, un token en una blockchain pública puede ser cualquier cadena alfanumérica que represente un registro en la base de datos descentralizada y que sea aceptada, por consenso, dentro de esa misma blockchain.

Características de la blockchain privada

Ahora bien, la propia tecnología blockchain ofrece la posibilidad de establecer una cadena de bloques con otras características distintas. Así que, de la misma forma, también puede construirse una blockchain privada, cerrada y con participantes identificados. O una privada, abierta y anónima, o una híbrida por asumir características propias de las blockchains públicas y privadas...

Uno de los argumentos esgrimidos por el sector financiero y otros sectores regulados para el desarrollo de las blockchains privadas ha sido la imposibilidad de compartir, por razones regulatorias o de confidencialidad, sus bases de datos de forma abierta. Por tanto, estas blockchains privadas son:

- **Privadas:** porque no todos los datos inscritos en la blockchain tienen difusión pública y sólo los participantes o usuarios pueden acceder y consultar todas o algunas de las transacciones realizadas.
- **Cerradas:** sólo las personas o entidades invitadas a participar adquieren la condición de usuarios o registradores de las tran-

2. OroyFinanzas.com: Token Bitcoin: ¿Qué es un token en Bitcoin?, octubre de 2014.

sacciones. En este sentido, el protocolo predeterminado podrá incluir distintos niveles de acceso a los usuarios, de modo que unos puedan tener la capacidad de registrar información y otros tener vetada esta opción. El diseño va siempre en función de los fines perseguidos.

- **Distribuidas:** el número de nodos de los que se componga la blockchain privada puede estar limitado al número de participantes o a cierto número de ellos. En cualquier caso, todos los nodos se conocen. La fortaleza de una blockchain se basa en gran medida en la cantidad de los nodos que la protegen y en los incentivos que éstos puedan recibir por cumplir este papel. A mayor número de nodos operativos, menor es la posibilidad de sufrir ataques. Pero, a diferencia de las blockchains públicas, donde el mantenimiento de los nodos depende de la voluntad de los usuarios, en las privadas son los participantes quienes se comprometen a mantener la estabilidad del sistema. Esto significa que una blockchain privada no está sujeta, por así decirlo, a las veleidades que puede sufrir una cadena pública, en la cual es sumamente importante definir correctamente medidas que trabajen a favor de su propia protección.
- **Anónimas:** una blockchain privada puede establecer el nivel de anonimato que quiera para realizar o proteger transacciones. Los usuarios que registran anotaciones pueden estar o no perfectamente identificados.

Los participantes en una blockchain privada, es decir, aquellos que hayan obtenido la condición de usuarios, están sujetos a un protocolo predeterminado que los podrá capacitar, según se establezca, para participar en el registro de las anotaciones y/o verificar los cambios introducidos en la cadena. En este sentido, una blockchain privada podría estar más centralizada y el número de nodos que componen la red podría limitarse al número de usuarios necesarios establecido por los promotores. Hablaríamos entonces de una base de datos conjunta gestionada por ese grupo de usuarios, en la que —y de la misma forma que en una blockchain pública— las anotaciones realizadas serán inalterables.

En la tecnología blockchain privada también se habla muchas veces de libro mayor en referencia a un registro global de transacciones, tal y como se conoce en la contabilidad tradicional. Tanto es así que las iniciativas de blockchains privadas se denominan con frecuencia en inglés *Distributed Ledger Technology* (DLT), lo que en castellano equivale a decir Tecnología de Libro Mayor Distribuido. Por otro lado, la blockchain privada es distribuida, en el sentido de que es una base de datos repartida en varios nodos, mientras que la pública es descentralizada, porque en ella no se controla quién participa en la misma.

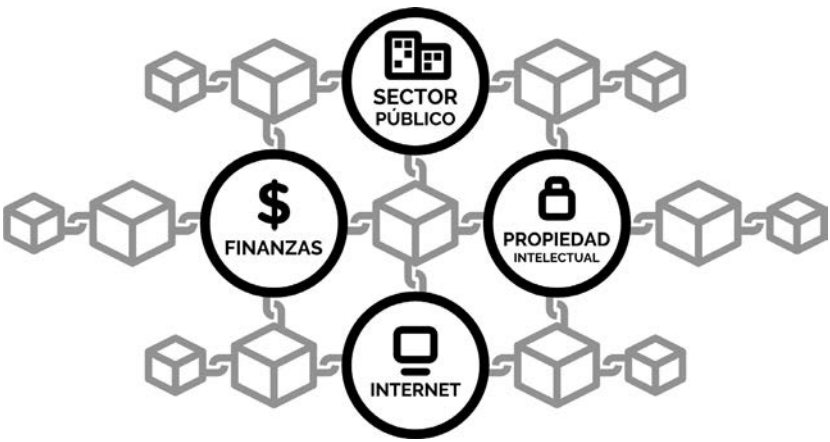
De forma coloquial se puede decir que una blockchain es pública si cualquier usuario puede participar en ella libremente, de ahí que se la llame también «blockchain sin permiso» (*permisionless*, en inglés). En cambio, en una privada la posibilidad de participar no está al alcance de todo el mundo, aunque el código utilizado sea público: la persona debe ser invitada a participar, razón por la cual en ocasiones se la denomina «blockchain con permiso» (*permissioned*, en inglés). Con el tiempo se consolidarán multitud de blockchains con características distintas para cumplir con diferentes fines. Unas serán públicas, otras privadas[3] y no faltarán tampoco las híbridas, dependiendo del modelo de uso para el que hayan sido concebidas.

3. OroyFinanzas.com: Diferencias entre las cadenas de bloques (blockchain) públicas y cadenas de bloques privadas, octubre de 2015.

Capítulo 2
El impacto de la blockchain en las diferentes industrias

El internet de la información empezó a tomar forma dentro de los sectores militar y académico, y desde ellos se expandió al resto de industrias. En el internet del valor ha sido el sector financiero el primero en tomar la iniciativa. Pero, como en el caso anterior, la aplicación de esta tecnología no será exclusiva de un único sector, pues cada vez son más las industrias que exploran todo su potencial. A lo largo de este capítulo presentaremos algunas de ellas.

Ejemplos de industrias dentro del internet del valor.



Banca y blockchain, ¿pioneros por necesidad?

Daniel Díez García y Gonzalo Gómez Lardies

Desde la crisis financiera de 2008, el sector bancario experimenta dificultades para mantener los niveles de rentabilidad anteriores a esa fecha. No es extraño así que busque revertir esta tendencia apostando por una fuerte inversión en la innovación representada por la tecnología blockchain. Los bancos e instituciones financieras apuestan, sobre todo, por las blockchains privadas para desarrollar modelos de uso. Frente a ellas, se sitúan las grandes empresas de capital riesgo de Silicon Valley y los gigantes de internet, que prefieren las blockchains públicas para introducirse en el mundo Fintech e Insurtech (empresas de tecnología centradas en la industria del seguro).

Bitcoin: el nacimiento de la banca descentralizada

En la década de los noventa, un grupo de personas conocidas como cypherpunks decidió aprovechar todo el potencial de la infraestructura de internet y crear un sistema financiero abierto, sin entes centrales, que garantizara el anonimato, el control de la oferta monetaria y, a la vez, fuera totalmente transparente. El resultado llegó en 2008 con la creación de una criptodivisa: bitcoin.[4] Con ella se inició una primera ola de descentralización en campos tan importantes como son los pagos, las transferencias internacionales y las remesas. Pero la importancia del bitcoin va más allá de todo esto: mostró que ya no era necesario contar con un banco o ningún tipo de tercero de confianza para llevar a cabo gran parte de las labores que tradicional-

4. ‹https://bitcoin.org/bitcoin.pdf›.

mente ha desempeñado la banca. Fue, por tanto, el primer caso de uso de la tecnología blockchain.

La blockchain permite simplificar, en gran medida, pagos internacionales al eliminar potencialmente la necesidad de cámaras de compensación y crear un nuevo estándar de interoperabilidad entre entidades financieras. Añadiendo sistemas desintermediados, transparentes y automatizados, desaparecen los riesgos operativos, ya que no hay posibilidad de incumplir las condiciones de los contratos digitales inteligentes que hayan firmado las diferentes partes involucradas. La consecuencia de todo esto es que se reduce considerablemente la necesidad de disponer de circulante o líneas de crédito, y se da pie a ofrecer márgenes mucho más ajustados en los servicios (por ejemplo, préstamos), eliminándose de paso la necesidad de confianza entre las diferentes partes.

Banca: ¿cuál podría ser su futuro?

Existen diversas razones por las cuales el sector bancario se encuentra en plena transformación. No se trata de un cambio exclusivamente tecnológico, sino también cultural y regulatorio, debido a nuevos hábitos de vida y consumo de servicios que afectan también a la relación entre empresa y cliente. Nos movemos en un paradigma en el que el objetivo ya no es vender servicios a los clientes como tal, sino acompañarlos a lo largo de sus vidas para satisfacer sus deseos y necesidades de la forma más líquida posible. Entre los motivos que han acelerado este cambio cultural y operativo destacan la rentabilidad de la banca, su regulación, los nuevos competidores que le han surgido y la distribución de capacidades y cambio de modelo comercial. A continuación explicamos cada uno de ellos en detalle.

La rentabilidad de la banca

Las principales líneas de negocio de la banca son el crédito, en primer lugar, y la venta de productos financieros, en segundo. En el primer caso, la banca había contado históricamente con un amplio margen entre los intereses que se pagaban a los depositantes y los que se cobraban a los solicitantes de préstamos. Asimismo, debido a la asime-

tría de información entre las instituciones financieras y los clientes, la opacidad y falta de información para estos últimos permitía que las primeras minusvalorasen riesgos en la venta de productos financieros de baja calidad, calificándolos, en ocasiones, como depósitos o productos de renta fija cuando en realidad eran de renta variable. Eso es lo que pasó en el conocido caso del fraude de las preferentes en España.

En los últimos años, las políticas monetarias expansivas y las bajadas de los tipos de interés han afectado negativamente a la rentabilidad bancaria. Debido al exceso de liquidez, los tipos de interés de los préstamos siguen cayendo, mientras que los de los depósitos a cuenta mantienen un suelo del 0 %. En esta situación el margen de intermediación con el que cuenta la banca se hace cada vez más estrecho, por lo que las entidades se ven obligadas a realizar el cobro de comisiones de forma más directa. Lo que los clientes pagaban antiguamente sin ser conscientes de ello (debido a ese mayor margen de intermediación), ahora deben pagarlo de forma explícita con comisiones por retirada de efectivo, transferencias o mantenimiento de cuenta, entre otros servicios complementarios. La consecuencia de esto no es otra que la pérdida de confianza por parte de los clientes y el empeoramiento de la experiencia como usuario.

Este estrecho margen de intermediación se ha traducido en dos estrategias comerciales para intentar mejorar la operativa: por un lado, la reducción de los gastos de explotación mediante recortes de plantilla, cierre de oficinas, fusiones e inversiones en tecnología; por otro, y muy especialmente, la reorientación del modelo de negocio a actividades que generen ingresos distintos al cobro de intereses y aporten nuevas capas de valor sobre la operativa existente.

Desde el prisma de la blockchain se puede optimizar en gran medida la operativa reduciendo notablemente los costes. Pero es en la segunda vía, en la de la reorientación, donde encontramos un valor diferencial para esta tecnología gracias a la generación de nuevas plataformas y modelos de negocio en los que la flexibilidad, la transparencia, la interoperabilidad, la automatización y las experiencias del usuario cobran un papel fundamental.

La regulación de la banca

Existen dos iniciativas legales llamadas a cambiar radicalmente el ecosistema de servicios bancarios y la relación entre entidad y cliente: la MiFID II (Markets in Financial Instruments Directive II) y la PSD2 (Directive on Payment Services 2).

La primera de ellas, la MiFID II, con entrada en vigor en enero del año 2018, tiene como objetivo transformar el modelo de asesoramiento y venta de productos financieros a clientes, aportando más transparencia a un mercado tradicionalmente opaco y evitando malas prácticas como la venta en masa de productos «genéricos» cuyos riesgos se acostumbraba a minusvalorar.

Con la MiFID II, los asesores financieros tienen opción de elegir entre declararse independientes (lo que les impide cobrar el porcentaje de los productos de las gestoras que venden) o dependientes, y vender entonces aquellos productos de mayor comisión. La MiFID II permite también que donde antes un inversor pensaba que el asesoramiento era gratuito, ahora identifique perfectamente toda la relación de costes. En definitiva, se pasa a un modelo en el que el objetivo del asesoramiento no consiste en cumplir con los objetivos del banco, sino con los del cliente.

En lo que respecta a la normativa PSD2, supone una revolución en la naturaleza del modelo de negocio de la banca aplicada al ámbito de los pagos, pues con ella se pasa de un modelo de negocio tradicional a otro con un carácter mucho más abierto, en el que la banca tiene que exponer sus «entrañas» a la comunidad abierta de desarrolladores y nuevas Fintechs mediante la implementación de interfaces de programación de aplicaciones (en inglés, Application Programming Interface, API). Estas API pueden dirigirse a dos tipos de proveedores: los que puedan iniciar pagos desde cualquier plataforma online, y aquellos otros que ya sean conocidos como agregadores de información financiera y permitan acceder a información del cliente y ofrecerle servicios de valor añadido.

Si la MiFID II tiene como objetivo velar por la protección al consumidor, la PSD2 persigue generar oferta para los consumidores y fomentar la competencia. Es alineándose con esta nueva normativa

como la blockchain puede ofrecer un valor diferencial a las empresas que les permita alcanzar nuevos estándares de transparencia y apertura de modelos de negocio. Por todo lo expuesto, podemos convenir que la regulación avanza en la línea de ser más una gran aliada que una barrera en lo que a la adopción de esta tecnología se refiere.

La blockchain posibilita la transición a un mundo transparente, abierto, seguro y altamente interconectado, en el cual los clientes tienen pleno control sobre su identidad digital y conocimiento de los activos y servicios que contratan. Aquellos agentes que consigan dar un mayor valor a sus productos serán quienes obtengan una principal ventaja competitiva y unos mayores rendimientos económicos.

Nuevos competidores de la banca

Tanto la regulación como las nuevas tecnologías han propiciado la aparición de nuevos competidores, capaces de desintermediar crédito, pagos y envíos de remesas entre otros mercados. Estos competidores tiempo atrás estaban caracterizados por la oferta de nuevas soluciones, que si bien proveían de un gran valor a los clientes con magníficas experiencias de usuario, no cumplían con la regulación pertinente.

Actualmente, y más allá de la incursión de gigantes tecnológicos como las GAFA (Google, Apple, Facebook y Amazon), contamos con un amplio espectro de empresas que, frente a la incapacidad de innovar de las grandes firmas (en el caso de la banca, en numerosos casos resulta más eficiente crear otro banco desde cero que innovar sobre el original), se muestran flexibles, ágiles y completamente volcadas sobre el cliente. Se trata de una clara propuesta de valor que llega a ofrecer incluso servicios bancarios a usuarios de países desbancarizados (recordemos que el 38 % de la población mundial carece de una cuenta bancaria). En una era digital en la que priman los servicios vivos y las expectativas líquidas, la propia experiencia del usuario será la principal ventaja competitiva que determinará el crecimiento y la supervivencia de las empresas, quedando la propia naturaleza de cada modelo de negocio relegada a un segundo plano.

Nos encontramos, pues, en una etapa en la que el foco de las empresas ha pasado del plano de la competición directa (aquellos que

venden el mismo producto) a situarse en el plano experiencial (aquellos competidores que ofrecen experiencias que sustituyen a las nuestras) para, finalmente, centrarse en el plano perceptual (competidores que pueden cambiar los hábitos de consumo y expectativas de nuestros clientes).

La conclusión es clara: necesitamos empresas que acompañen a sus clientes y los provean del máximo valor en tiempo real y en cualquier sitio, conociendo e incluso anticipándose a sus demandas, deseos y necesidades.

Por ello, el siguiente reto de la banca pasa por ofrecer experiencias de usuario excepcionales y obtener un rendimiento de la información que las entidades están ofreciendo a terceros, yendo más allá de una API limitada que cumpla con la regulación. En suma, se convertirá en un proveedor de información de cuentas abierto que trabaje con comunidades abiertas de desarrolladores y compita directamente con las GAFA y Fintechs.

Distribución de capacidades y cambio de modelo comercial (sucursal digital)

Tradicionalmente, el asesor comercial y el cliente concertaban una cita y se encontraban en persona, estableciéndose entre ellos una relación de larga duración basada en la confianza. El conocimiento del cliente posibilitaba unas soluciones personalizadas. Esto era un activo mucho más valioso que todos los registros que pudiera haber en la base de datos de la entidad.

En la actualidad, la crisis de reputación del sector y el auge de las nuevas tecnologías está propiciando que el cliente sustituya la figura del asesor comercial por diferentes proveedores de información y servicios que pasan a asumir ese rol. Debido al grado de disponibilidad de información sobre nuestros gustos, situación personal y preferencias, las oficinas de siempre no consiguen ya ofrecer una experiencia de usuario equivalente a la de otros competidores perceptuales. Dejan, por tanto, de ser rentables. Hay que redifinirlas, y lo mismo puede decirse de la propia figura del asesor comercial. Gracias a las nuevas herramientas tecnológicas disponibles, esta figura

en concreto podría incluso digitalizarse, transformarse en una inteligencia artificial.

Para llevar a cabo este cambio al modelo digital se precisa una visión más global, puesto que el análisis de capacidades que ha de llevar al cumplimiento de las necesidades, deseos y demandas de los clientes no debe recaer sobre el equipo comercial, sino sobre toda la organización en su conjunto. Esto significa que la labor comercial deberá ser el último eslabón de un conjunto de elementos que proporcionen al cliente el mejor servicio y experiencia de usuario posibles.

La blockchain: casos de uso en la banca

La blockchain nace para descentralizar la confianza que hemos depositado en las instituciones financieras. En la era digital es necesario que, dada la elevada interconectividad, competencia y automatización de procesos, las empresas tanto tradicionales como de nueva creación modifiquen sus mecanismos para innovar en base a estándares y modelos de negocio lo más abiertos posibles. Más allá de programar el dinero, la blockchain nos permite programar confianza, propiedad, identidad, activos y contratos, mediante pagos, transacciones, procesos, autentificación, reconciliación e información en tiempo real, y todo con plena transparencia y auditabilidad.

Existen cuatro principales aplicaciones de la blockchain para optimizar el entorno bancario, que más allá del ahorro y simplificación estructural y reducción de costes operativos, permiten la creación de nuevos servicios y modelos de negocio. Estas aplicaciones son: Pagos Globales, Trade Finance, Liquidación de Transacciones y Cumplimentación de la Regulación Automatizada.

Tradicionalmente, ha existido un problema de falta de interoperabilidad entre las diferentes entidades financieras, incluso entre aquellas que pertenecen al mismo grupo, debido a la diferente regulación que se aplica en cada país. En la actualidad existen numerosos proveedores de pagos, el más popular de los cuales es SWIFT, con más de diez mil sociedades financieras formando parte de la cooperativa. La función de SWIFT es la de establecer un estándar de mensajería entre bancos. Para entender en qué consiste, imaginemos que queremos

enviar 1.000 euros a un pariente que se encuentra en Estados Unidos: cuando iniciamos la transferencia, el banco emisor genera un mensaje que indica de qué forma vamos a hacer llegar los fondos a ese cliente (fecha, divisas, gastos, a través de qué intermediarios...). Ese mensaje es el SWIFT, la prueba de la realización irrevocable de una transferencia internacional, lo que proporciona una gran seguridad tanto al emisor como al receptor del pago.

La propia naturaleza de SWIFT y la necesidad de un posterior proceso de liquidación entre entidades hace que este tipo de transferencias se lleguen a demorar entre dos y cuatro días, lo que abre la necesidad de establecer líneas de crédito para aquellas empresas que tengan operaciones globales. Si estos pagos fueran instantáneos, desaparecería la necesidad de este tipo de operaciones, reduciéndose en gran medida también el volumen del circulante. Afortunadamente, todo eso ha cambiado hoy gracias a las blockchains, tanto a las públicas como a las privadas. Ambas son ya las dos principales vías para llevar a cabo pagos internacionales.

Las blockchains públicas y su uso en la banca

Las blockchains públicas más populares son Bitcoin y Ethereum. Gracias a ellas, cualquier persona o empresa puede convertirse tanto en usuario como en validador de la red y formar parte como un nodo de la misma. En este tipo de redes, en las que no es necesario ningún tipo de confianza entre las diferentes partes para llegar al consenso sobre el estado y evolución de una serie de factores compartidos (función de una blockchain), cualquier usuario puede enviar dinero sin que importen las fronteras territoriales y, en función de la plataforma y nivel de seguridad elegidos, en un lapso que oscila entre los 15 segundos y los 60 minutos, y con un coste reducido. La principal limitación de estas plataformas es la necesidad de emplear criptomonedas o tokens para transmitir el valor, aspecto este que se explica con más detalle en el apartado de inversión de este libro.

Frente a plataformas consolidadas en un modelo tradicional, como Western Union o Moneygram, las nuevas propuestas aportan un especial valor en países donde no existe una infraestructura fi-

nanciera sólida y puede que haya fuertes controles de capital e inflación (caso de Venezuela, Argentina, Zimbabue o China), se da un elevado número de población desbancarizada (México) o esa población ha perdido la confianza en su propio sistema financiero (Chipre). Es en estos casos donde las criptomonedas aportan un plus en seguridad a los usuarios en términos de facilidad de uso, imposibilidad de confiscación o control y reserva de valor. En este ámbito existen tres ejemplos de referencia:

- **Abra** (goabra.com): es un servicio de remesas persona a persona. En el caso de que el destinatario no tenga una cuenta de banco (no bancarizada), Abra gestiona una red de personas físicas en muchos países, llamadas *Tellers*, que hacen la función de cajero automático y entregan el dinero al destinatario.
- **BitPesa** (bitpesa.com): se ha especializado en envíos de dinero a y desde África, especialmente en países como Kenia, Nigeria, Tanzania y Uganda. De este modo, un pequeño comerciante puede desarrollar su negocio de importación y/o exportación gracias a una mayor agilidad y un menor coste en el envío de dinero.
- **Circle** (circle.com): es una startup que permite realizar envíos de dinero sin comisiones. Para aquellos envíos que tengan como destino países desbancarizados o con controles de divisas, recurre a criptomonedas.

Las blockchains privadas y su uso en la banca

Una de las plataformas más prometedoras en el ámbito de las blockchains privadas es Ripple (ripple.com). Su especialidad son los pagos internacionales interbancarios, así como el proceso de conversión de divisas. En sí, Ripple es un sistema abierto (cualquiera puede usar Ripple, al igual que Bitcoin o Ethereum), si bien aquellas partes que quieran participar como proveedoras de liquidez para las conversiones de divisas deben estar previamente autorizadas por Ripple. Es, por tanto, un sistema más privado y con un ámbito de confianza más reducido que los públicos descritos anteriormente.

Las transacciones internacionales se completan en tan solo 5 o 10 segundos, y en ellas se hace uso de un proceso de subasta a la baja en el que los diferentes proveedores de liquidez compiten para procesar los pagos. Una vez se produce el *match*, Ripple se encarga del proceso de liquidación entre las dos partes, tarea ejecutada en tiempo real.

Otras soluciones son las que ofrecen R3 (con su producto Corda) o Hyperledger, perteneciente a la Fundación Linux. Ambas trabajan en soluciones para la banca y apuestan por un registro distribuido entre las diferentes entidades del consorcio, lo que les confiere la posibilidad de transferir en tiempo real dinero y otros activos digitales mediante tokens.

Trade Finance en la blockchain

El elevado nivel de burocracia y de procesos manuales de las transacciones tradicionales suman tiempos muertos en los diferentes procesos. Además, siempre queda el miedo de que una de las partes no cumpla con los tiempos de envío y pago, o con las condiciones de calidad. Por suerte, en la actualidad existe una gran oportunidad para digitalizar la comunicación y automatizar procesos en la cadena de suministro.

Más allá de la notable reducción del circulante que aportan los pagos en tiempo real, los contratos inteligentes y el internet de las cosas e identidad digital podrían permitir automatizar la compraventa de mercancía de forma segura, incluyendo todas y cada una de las etapas involucradas en el proceso. Asimismo, gracias a la transparencia, inmutabilidad y trazabilidad características de la blockchain, podríamos conocer y certificar el origen de la mercancía, sin posibilidad de falsificación alguna de la información relativa a la misma. El objetivo es la digitalización de la *Bill of Lading* («conocimiento del embarque»), es decir, el conocimiento que establece la relación contractual entre el cargador, consignatario de la carga y el transportista. Entre las startups que están trabajando en esa línea destacan Fluent, Provenance, Skuchain y Wave.

Cumplimentación de la regulación automatizada

Gracias a la tokenización de identidades y consorcios de identidades digitales será posible que un usuario que se ha dado de alta en una entidad no tenga que aportar de nuevo toda su información personal en el momento de darse de alta en otra de las entidades que pertenezcan a dicho consorcio. Esa cuenta podría crearse con tan sólo una foto de su rostro, limitándose así la cantidad de información cedida y el riesgo de robo y suplantación de identidad.

Este conocimiento de la identidad, sumado a una completa trazabilidad de las operaciones de inicio a fin, permite la monitorización y detección de actividad sospechosa, y propicia también una fácil incorporación de organismos que puedan auditar la información en tiempo real y de ese modo imposibilitar el fraude.

Préstamos en la blockchain

La causa principal por la que individuos y empresas recurren al crédito suministrado por grandes entidades financieras no es otra que la confianza. Ésta, sin embargo, puede convertirse en algo prescindible si se elimina la figura de los intermediarios que arbitran entre ahorradores y solicitantes de crédito. Para ello bastaría con aplicar un software autónomo y los Smart Contracts que garanticen que ambas partes cumplen con sus obligaciones contractuales.

Más allá de la transparencia y de los nuevos modelos de *scoring* (ese sistema automático que, partiendo de una información dada, recomienda la aprobación o no de una operación de financiación), esta desintermediación haría posible que se desarrollen plataformas que permitan un acuerdo entre las diferentes partes, sin ofrecer ellas mismas el préstamo en sí ni retener en ningún momento los fondos, ni siquiera la identidad de los usuarios, pues son ellos mismos quienes la proporcionan para ejecutar acciones mediante su token de identidad. Una de las principales aplicaciones sería el crédito al consumo, donde diferentes individuos o empresas podrían competir mediante subastas a la baja en proporcionar estos fondos, a cambio de unas condiciones transparentes y previamente pactadas.