UNIVERSIDAD D SEVILLA

MÁSTER UNIVERSITARIO EN ESTUDIOS AVANZADOS
EN DIRECCIÓN DE EMPRESAS

TECNOLOGÍA BLOCKCHAIN COMO PALANCA DE CAMBIO EN EL SECTOR FINANCIERO Y BANCARIO

TRABAJO FIN DE MÁSTER

ANASTASIIA ZEMLIANSKAIA, JUNIO 2017

Departamento de Economía Financiera y Dirección de Operaciones

LA TECNOLOGÍA BLOCKCHAIN COMO PALANCA DE CAMBIO DEL SECTOR FINANCIERO Y BANCARIO

Trabajo Fin de Máster presentado para optar al Título de Máster Universitario de Estudios Avanzados en Dirección de Empresas por Anastasiia Zemlianskaia, siendo el tutor del mismo el Doctor Filippo Di Pietro.

Vº. Bº. del Tutor/a: Alumno/a:

D. Filippo Di Pietro Dª. Anastasiia Zemlianskaia

Sevilla, 5 de junio de 2017

MÁSTER UNIVERSITARIO DE ESTUDIOS AVANZADOS EN DIRECCIÓN DE EMPRESAS

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

TRABAJO FIN DE MÁSTER

CURSO ACADÉMICO [2016-2017]

TÍTULO:

LA TECNOLOGÍA BLOCKCHAIN COMO PALANCA DE CAMBIO DEL SECTOR FINANCIERO Y BANCARIO

AUTOR/A:

ANASTASIIA ZEMLIANSKAIA

TUTOR:

DR. D. FILIPPO DI PIETRO

LÍNEA DE TRABAJO:

FINANZAS

RESUMEN:

El trabajo se centra en la tecnología de cadena de bloques (la blockchain) y analiza en detalle todos los elementos clave de su ecosistema, desde las distintas criptomonedas, los usos futuros y presentes de esta tecnología en diferentes sectores, hasta los casos de implementación real, así como los beneficios que supone. En particular, se estudia la importancia de dicha innovación para el sector de las finanzas y la banca. Por otro lado, se describe la experiencia de la banca y las empresas nacionales e internacionales en este campo. Para concluir, se analizan las limitaciones y los retos que todavía debe afrontar y superar la tecnología blockchain para revolucionar la economía mundial.

PALABRAS CLAVE:

Blockchain, Bitcoin, Ethereum, Ripple, cadena de bloques, criptomonedas, tecnología en finanzas.

ÍNDICE

Relación de Figuras

Relación de Tablas

CAPÍTULO 1. INTRODUCCIÓN

1.1. JUSTIFICACIÓN DEL TEMA ELEGIDO

Desde el origen de la humanidad, el dinero siempre ha evolucionado con la sociedad y ha seguido sus avances. Sin embargo, su principal función siempre ha sido la misma: la de ser un medio de intercambio, un depósito de valor, una unidad de cuenta y de pagos diferidos (Mankiw, 2006). Analizando la historia del dinero podemos ver que desde sus inicios el valor de la moneda ha tenido relación con el peso del metal que lo ha respaldado, generalmente el oro o la plata. No obstante, con el tiempo su valor comenzó a estar ligado con los bancos privados y en concreto con la cantidad de metales nobles depositada en ellos.

El "patrón de oro", término introducido por David Hume en 1752, fue un periodo que marcó la historia económica: el dueño tenía garantías en papel de que la entidad emisora podría reintegrarle una cantidad de oro equivalente a la descrita y esto se convirtió en una forma de respaldar su valor. Este sistema imperaba prácticamente durante todo el siglo XIX hasta la Primera Guerra Mundial, cuando la emisión de dinero creció debido a los gastos bélicos y los gobiernos imprimían más dinero del que podían respaldar. En el año 1944 se firman los acuerdos de Bretton Woods, y el patrón-oro se sustituye por patrón-dólar vinculado al oro. Según estos acuerdos, el dólar podía ser canjeado por oro, lo que proporcionaba a los Estados Unidos una ventaja con respecto a otros países al poder pagar sus deudas imprimiendo dinero. A pesar de ello, después de la Segunda Guerra Mundial había varios países que, debido a los problemas económicos surgidos a causa de la guerra, exigían canjear los dólares por oro, lo que en aquel momento era totalmente insostenible. Entre otras razones, esto llevó a que las existencias de oro no fueran suficientes para satisfacer las necesidades y cubrir la deuda, lo que propició que en 1971 Richard Nixon rompiera el acuerdo de Bretton Woods, momento a partir del cual el dólar fue declarado inconvertible en oro. En otras palabras, a partir de este momento la confianza de los poseedores se convirtió en el único respaldo del dólar. En la actualidad, el valor de las divisas se acuerda en el mercado internacional de divisas FOREX, aunque el dólar sigue dominando las operaciones.

La última crisis económico-financiera ha socavado la confianza en las principales divisas mundiales, como el dólar americano o el euro. Fue entonces cuando aparece la primera moneda criptográfica descentralizada – el Bitcoin. Hasta el día de hoy esta criptodivisa no ha podido convertirse en una competencia real del dinero fiduciario, sin embargo, la tecnología en la que se basa, llamada blockchain o cadena de bloques, está llamando la atención de los expertos del sector bancario y financiero cada vez más, ya que permite ahorrar significativamente los costes y ofrecer un servicio mucho más rápido y eficaz a sus clientes. Además, es capaz de resolver varios problemas del sistema económico-financiero, como la prevención de fraude o la inserción financiera, que son comunes en el mundo cada vez más globalizado y transparente.

1.2. OBJETIVOS

Los objetivos previos de este trabajo son los siguientes:

- Conocer en detalle el ecosistema de la tecnología de cadena de bloques (blockchain) y las nuevas oportunidades que ofrece al sector bancario y financiero.
- Explicar cuáles son las diferencias de las criptomonedas con las divisas fiduciarias y describir las criptomonedas de mayor capitalización de mercado.
- Definir la tecnología blockchain, sus principales características, ventajas y limitaciones.

- Descubrir las innovaciones y nuevas tendencias que brinda la tecnología blockchain.
- Analizar las principales aportaciones a día de hoy de esta tecnología y los experimentos que han sido llevados a cabo por instituciones financieras en todo el mundo.
- Describir la situación en diferentes países y en España en particular con la regulación de esta tecnología.

El objetivo principal que persigue este trabajo es:

- Llegar a conclusiones acerca de si es posible la implementación masiva de la blockchain y si podría llevar a beneficios tanto a las instituciones, así como a los clientes finales, o si sus ventajas están exageradas y no puede ofrecer soluciones reales.

1.3. ESTRUCTURA DEL TRABAJO

El trabajo está estructurado en cinco capítulos:

El capítulo 1 se explica el contexto en el que apareció la primera criptodivisa Bitcoin y la tecnología en la que se basa – la blockchain. Por otra parte, se describen los objetivos perseguidos por este trabajo y su estructuración por capítulos. Además, se habla sobre la metodología elegida para la realización de este trabajo.

En el capítulo 2, se describen los factores determinantes para la aparición de la primera moneda criptográfica y los investigaciones y pruebas en esta área que han sido realizadas anteriormente. Luego, se definen las principales características que tienen las criptodivisas en general y el Bitcoin en partícular, además de los problemas que resuelve, las ventajas e inconvenientes que tiene y la situación actual de su utilización e implementación. Se analizan también otras criptomonedas con la mayor capitalización del mercado, como Litecoin, Ripple, Ethereum, y las monedas anónimas, como Monero, Dash y Zcash, sus diferencias y similitudes, ya que juntos forman parte de un gran ecosistema monetaria basada en la tecnología de cadena de bloques.

El capítulo 3 se adentra en el mundo de la Blockchain. Se analizan los escenarios en los que se están haciendo pruebas con esta tecnología actualmente y se definen los principales ámbitos de su implementación y se comparan diferentes tipos de las cadenas de bloques. También se describen las primeras propuestas para el sector bancario y financiero y se definen los servicios financieros en los que esta tecnología tendría el mayor impacto. En esta parte se observan las propuestas para las transferencias internacionales (caso Ripple) y las posibilidades de los contratos inteligentes para la banca. Por último, se analizan las oportunidades que ofrece la blockchain para el sector de finanzas corporativas, desde la contabilidad de partida triple y la dirección descentralizada de empresas (DAO) hasta la nueva forma de financiación ICO, que se compara con la inversión de capital de riesgo tradicional.

El capítulo 4 ofrece ejemplos y casos reales de la implementación y uso de la tecnología blockchain. Se investigan las formas que utilizan las instituciones y empresas para estudiar esta tecnología de forma individual o formando grandes asociaciones y consorcios. Se analizan las similitudes y diferencias entre los principales consorcios, y también se describen las propuestas realizadas por bancos y organizaciones. Además, se centra en la situación global y se dan ejemplos de la implementación de la blockchain en distintos países, sus aportaciones en el sector gubernamental y servicios públicos. Por otra parte, se observan las limitaciones y regulaciones legales del uso de las criptodivisas y la tecnología blockchain, se definen los obstáculos que existen actualmente para su amplia adopción y se describe la situación en España.

Finalmente, en el capítulo 5 se presentan las principales conclusiones a las que se han llegado tras el estudio realizado en los capítulos anteriores.

1.4. METODOLOGÍA

El proceso de realización de este trabajo de investigación incluye las siguientes etapas:

I. Se han recopilado noticias de los periódicos más influyentes internacionalmente en las que se detallan el potencial que ofrece la tecnología Blockchain así como las principales tendencias del sector.
II. Se han consultado los libros más recientes que estudian esta tecnología y su posible influencia en la sociedad y la economía, como “La revolución Blockchain” de Don y Alex Tapscott (2017) o “The Business Blockchain” de Willian Mougayar (2017), entre otros.
III. Se ha interpretado la información estadística y los gráficos de capitalización de mercado, cotizaciones y volatilidad de las monedas criptográficas analizadas.
IV. Se han analizado los informes de las instituciones financieras, bancos y consultoras con la descripción de experimentos puestos en práctica.
V. Se ha estudiado el contenido de distintas páginas web con opiniones de expertos e inversores, así como entrevistas con ingenieros y criptógrafos acerca de las perspectivas de la blockchain.
VI. Se han tomado como referencia numerosos Trabajos Fin de Máster de diferentes Universidades del mundo y artículos en revistas científicas internacionales dedicados a finanzas, economía digital e innovación en sector bancario y financiero.

A pesar de que existen diversos trabajos dedicados al estudio de Bitcoin como tal, hay muy pocos estudios en los que Bitcoin se analice únicamente como una parte del ecosistema Blockchain. Por esta razón, en este trabajo se analiza el ecosistema blockchain en su totalidad. Este ecosistema está formado por múltiples criptodivisas con diferentes ventajas e inconvenientes, pero que entendidas dentro de su contexto de aplicación pueden suponer un cambio tecnológico trascendental para gobiernos, bancos y corporaciones en general.

CAPÍTULO 2. ESTUDIO DEL ESTADO DEL ARTE DE LAS CADENAS DE BLOQUES CON MAYOR CAPITALIZACIÓN DE MERCADO

2.1. LOS PRECURSORES DE BITCOIN: ECASH, B-MONEY Y BIT GOLD

Antes de la aparición de Bitcoin ya existían numerosas investigaciones en el campo de las transacciones económicas cifradas, así como algunos prototipos iniciales de criptodivisas.

En el año 1983 David Chaum, un investigador de la facultad de ciencias computacionales de la Universidad de California empezó a estudiar cómo combinar la transparencia con el anonimato en las transacciones de todos los miembros de un mercado. El científico propuso utilizar la "fórmula cegadora" o "blinding formula" (Chaum, 1983) que está basada en una extensión del algoritmo criptográfico RSA (algoritmo que se utiliza también a día de hoy en la encriptación de páginas web) para permitir a un usuario enviar dinero a otro sin dejar constancia del emisor. Además, Chaum desarrolló protocolos de "efectivo virtual", y en el año 1990 creó su propia empresa bajo el nombre de DigiCash. A diferencia de las criptodivisas desarrolladas después, la emisión y la liquidación de su moneda – ecash – eran centralizadas. Además de una elevada repercusión mediática, recibió una propuesta por parte de Microsoft para implementar su tecnología en todos los ordenadores de la empresa por valor de 180 millones de dólares, oferta que rechazó. Numerosos bancos también estaban interesados en la tecnología de DigiCash, sin embargo, en el año 1998 la empresa acabó en bancarrota después de romper su acuerdo con el Banco Central de Holanda. No obstante, DigiCash no era la única tecnología desarrollada en este campo.

El concepto de "criptodivisa" como lo conocemos hoy en día fue propuesto por un ingeniero informático, Wei Dai, que en 1998 publicó un trabajo con el nombre de "B-money, an anonymous, distributed electronic cash system" (Dai, 1998). Su teoría se basaba en que el dinero se podía generar mediante la resolución de problemas computacionales. Además, Wei Dai menciona en su artículo fundamentos que luego jugarán un papel fundamental en las criptodivisas creadas posteriormente, incluida el Bitcoin. En particular, en este artículo destaca el término de "prueba de trabajo" (proof-of-work) – como la posibilidad de, por un lado, determinar cuánta potencia computacional es necesaria para resolver un determinado problema, y por otro lado, de inducir que si se conoce la solución a dicho problema es porque se ha realizado previamente el trabajo computacional determinado. Por primera vez este concepto fue propuesto por Adam Back en el protocolo Hashcash – un sistema de limitación de correos electrónicos que requería realizar un trabajo computacional para enviar un email, mecanismo que encarecía el envío masivo de correo basura. Por otro lado, cuando una transacción B-money es realizada se transmite públicamente al resto de participantes que tienen acceso tanto a la información de esta red como al contenido de las cuentas del resto de participantes. Por último, B-money establece una figura de "guardián" – un conjunto de participantes a cargo de la conservación y publicación del registro de transacciones.

En este mismo año (1998) fue creado otro precursor de Bitcoin – "Bit Gold" por Nick Szabo. Aunque este sistema nunca fue implementado en la práctica, los conceptos sentados por "Bit Gold" (por ejemplo, la descentralización o los micropagos digitales) fueron muy importantes para la aparición de Bitcoin tal y como lo conocemos hoy en día.

2.2. BITCOIN (BTC)

Como hemos visto hasta ahora, las ideas y teorías sobre una "moneda criptográfica virtual" ya existían desde los años ochenta, pero la primera implementación de estas investigaciones en realidad surgió a finales del año 2008, cuando salió a la luz un artículo bajo el título "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008), que incluía la descripción teórica y la primera versión del código. Hasta el día de hoy no está claro quién ha sido el autor de este trabajo, si bajo este seudónimo se esconde una persona en concreto o incluso un grupo de personas, ya que Satoshi Nakamoto prefiere mantener su anonimato, y además dejó de colaborar con otros programadores y abandonó el proyecto a mediados de 2010.

En su página oficial (www.bitcoin.org), el Bitcoin se define como *"una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital".* Básicamente, cuando hablamos de Bitcoin nos podemos referir por un lado a la criptodivisa (con su abreviatura de unidad – BTC), pero por otro lado también al protocolo de código abierto y a la red P2P en la que se basa la tecnología. En los informes oficiales del Banco Mundial y Banco Central Europeo el BTC se denomina "moneda virtual". Hablaremos más en detalle de la situación legal de Bitcoin en particular y criptodivisas en general en el capítulo 4.

2.2.1. Propuesta de Satoshi

La nueva tecnología tomó como fundamento al sistema "Blockchain" o cadena de bloques, parcialmente basada en las investigaciones de Chaum y Back.

Vamos a analizar algunos conceptos principales para entender el significado de Bitcoin y las criptodivisas.

1) **La tecnología P2P** (peer-to-peer) sirve para intercambiar distintos archivos entre los ordenadores que actúan como cliente y servidor al mismo tiempo, permitiendo de este modo un intercambio directo de información o datos sin necesidad de un intermediario. La misma tecnología P2P es utilizada en BitTorrent – un protocolo para intercambio de archivos o ficheros grandes en internet. La gran ventaja de P2P que utiliza Bitcoin es la descentralización, ya que se pueden crear grandes bases de datos de los que todos los ordenadores implementados pueden descargar la información distribuida. Esta base de datos con todas las operaciones registradas se denomina Cadena de bloques (Blockchain), y la detallaremos más adelante. Esa descentralización que se logra a través de la tecnología P2P permite eliminar por completo la figura de "administrador" o cualquier análogo, lo cual es la principal diferencia de los sistemas monetarios tradicionales.
2) **La seguridad y la imposibilidad del doble gasto y duplicidad de las monedas** – también gracias a la base de datos financiera distribuida en cadenas de bloques (Blockchain). De esta manera, la falsificación se vuelve prácticamente imposible, ya que todas las transacciones se guardan en un bloque y para cambiar los detalles de una transacción sería imprescindible cambiar toda la cadena desde el principio en todos los ordenadores pertenecientes a la red, cosa que en la práctica sería imposible por diversas razones tanto técnicas como de teoría de juegos. Esta característica también hace que las operaciones sean irreversibles. Cuando un usuario envía una cantidad de dinero a otro, se crea una nueva transacción la que contiene el hash (un resumen) de la transacción firmada con la clave privada del emisor. Esta información se envía a la red distribuida. Otros nodos de la cadena revisan las firmas antes de confirmar la transacción. Si el usuario intentara volver a enviar los BTC que ya han sido enviados anteriormente, la red no aceptaría esta transacción como válida pues el usuario ya no poseería dicha cantidad.
3) **La privacidad.** Todas las transacciones son de acceso abierto, aunque sin desvelar la información privada de la persona que las ha llevado a cabo. Cada

usuario puede crear un número infinito de direcciones para mandar o recibir dinero. El nombre de la cuenta (o cartera) de Bitcoin no lleva ningún dato relacionado son su dueño, es solo una secuencia de números y letras totalmente aleatoria. Por ello, la facilidad con la que se crean y se operan las cuentas, las direcciones y las carteras de Bitcoin hacen que en principio pudiera ser relativamente complicado reconocer a qué persona física van asociadas estas carteras. Sin embargo, Bitcoin que en principio se proclamó "criptomoneda anónima", a día de hoy prácticamente ha perdido esta función, dado que es muy difícil no dejar ningún rastro, y además ya existen servicios que permiten investigar y encontrar la identidad del dueño de la cartera Bitcoin (por ejemplo, lo ofrece una startup danesa con nombre "Chainalysis", que opera contra el blanqueo de capitales a través de la red Bitcoin).

4) **La emisión descentralizada.** La emisión de nuevas monedas de Bitcoin no depende de la decisión de alguna entidad monetaria ni tampoco puede ser controlada por ningún órgano específico – está determinada por una rutina computacional preestablecida. La emisión de Bitcoins tiene una previsión concreta y no es infinita, el número de monedas nunca superará los 21 millones de unidades, lo que está preestablecido por el protocolo desde su creación.
5) **Los mineros.** La emisión de nuevas monedas de Bitcoin depende única y exclusivamente de los mineros. Estos mineros son los encargados de mantener la red segura realizando una prueba de trabajo (en inglés "proof-of-work") que permite mantener la red completamente segura frente a ataques de denegación de servicio, entre otros. La suma de la potencia computacional de todos los mineros de Bitcoin es tan grande a día de hoy que sería completamente inviable realizar un ataque a la red, llegando a ser imposible incluso para los gobiernos o instituciones censurar o atacar la red Bitcoin. Como recompensa por mantener la red segura, el primer minero que estuviera realizando la prueba de trabajo y encuentre la solución al problema matemático lo difunde al resto de nodos de la red, y los nodos le premian con la recompensa por dicha solución. La dificultad del problema matemático que se resuelve depende del número de bloques de la cadena de Bitcoin, siendo la recompensa mayor cuanto menor es el número de bloque, es decir, cuando la red es más joven y la emisión total es menor, y siendo la recompensa menor cuanto mayor es el bloque y más madura (y segura) es la red. El reajuste de esta recompensa se realiza cada cierto número de bloques resueltos, ajuste denominado "Halvening" que reduce la recompensa otorgada a la mitad a partir de este momento. Actualmente, la recompensa es de 12,5 BTC por bloque, es decir, unos 15 mil dólares al precio actual.
6) **La divisibilidad** es uno de los conceptos fundamentales en macroeconomía cuando hablamos del dinero. En caso de Bitcoin, este puede ser dividido hasta 8 decimales. Asimismo, 0,00000001 BTC es la cantidad más pequeña que puede ser enviada en una transacción y tiene la denominación "Satoshi". Si fuera necesario, el protocolo y el software podría ser modificados para manejar cantidades incluso más pequeñas. Claramente, la elevada divisibilidad es una ventaja de BTC frente las monedas tradicionales con las que estamos acostumbrados a tratar.
7) **La fungibilidad** es una de las características con las que cuenta Bitcoin y se refiere a que cualquier unidad de dinero es indistinguible de otra, es decir, cualquier moneda tiene el mismo valor y las mismas características que otra. En este caso es parecido a las monedas tradicionales, como el dólar, y el concepto del dinero en general. La fungibilidad del dinero tiene consecuencias no solo en el ámbito financiero, sino también en el ámbito jurídico. Aun así, no todas las criptomonedas son verdaderamente fungibles. Por ejemplo, en el caso de Bitcoin, se puede saber cada transacción que está detrás de esta misma moneda, y si ha sido utilizado para pagar actividades ilícitas puede perjudicar a su dueño actual, por lo cual no es exactamente lo mismo que si fuera uno sin

este historial. Pero este problema se soluciona con el uso de criptodivisas anónimas o confidenciales, como Monero o Zcash, que no desvelan las transacciones ni los dueños anteriores ni presentes de una moneda.

8) **La transferibilidad** de criptodivisas es mucho mayor que en el caso de las divisas fiduciarias, ya que son totalmente digitales y las transacciones tardan minutos en vez de días como podría tardar una transacción bancaria común.

En resumen, la descentralización y la distribución, la ausencia de intermediarios, las transacciones irreversibles, el gran potencial de divisibilidad, la fungibilidad y la transferibilidad, entre otras razones nombradas anteriormente, son los pilares en los que está basada la tecnología Bitcoin tal y como fue conocida en el año 2009, y posteriormente muchas otras criptodivisas que la tomaron como referencia.

2.2.2. Problemas que resuelve, y cómo los resuelve

¿Por qué es tan importante la aparición de Bitcoin?

En primer lugar, fundamentalmente es un gran avance en el campo computacional, que está basado en más de 20 años de estudios teóricos de monedas criptográficas y más de 40 años de investigaciones en el campo de criptografía de miles de científicos por de todo el mundo. Muchos lo ven, además, como un paso hacia el cambio del paradigma económico.

En segundo lugar, Bitcoin es la primera solución práctica de un experimento mental llamado “Problema de los generales bizantinos” (Pérez-Soì & Herrera-Joancomartí, 2014). Se trata del dilema de lograr un consenso entre un conjunto de entidades con un objetivo común donde todos persiguen el mismo objetivo a la vez que carecen de confianza entre sí. El problema original es el siguiente:

“*Existe un grupo de generales del ejército de Bizantina que ha acampado alrededor de una ciudad del enemigo. Pudiendo comunicarse solamente a través de un mensajero, los generales deben coordinar su plan de batalla. Sin embargo, algunos de los generales pueden ser traidores que van a intentar confundir a los demás. La cuestión es encontrar un algoritmo con la ayuda del cual los generales pueden llegar a un acuerdo”.*

En otras palabras, el dilema plantea la cuestión de cómo es posible la confianza entre dos partes que están conectadas solamente a través de la red internet a la que no se puede confiar. La solución práctica de este experimento mental es que Bitcoin por primera vez permite a un usuario de internet transferir su propiedad digital única a otro usuario del internet, mientras que la seguridad y la protección de la transferencia están garantizadas, todos saben que ha sucedido y nadie puede desafiar su legitimidad. Con “propiedad digital única” podemos entender no sólo el dinero virtual, sino también por ejemplo contratos digitales, derechos de la propiedad, firmas electrónicas, acciones o activos digitales etc. Todo eso puede ser intercambiado a través de una red distribuida que no necesita ningún intermediario centralizado, como un banco o un bróker. Solo el dueño del activo digital tiene derecho de enviarlo al receptor, y solo el receptor puede recibirlo, mientras el activo sólo puede existir en un lugar en el momento preciso, pero cualquiera puede ver la transacción en cualquier momento.

2.2.3. La situación actual

A día 11 de abril del 2017, existen más de 700 criptomonedas con una capitalización de mercado total de $27.920.316.272, y un volumen en 24 horas de casi 500 mil millones de dólares. Sin embargo, el Bitcoin [Figura 1] domina casi el 70% del mercado, siendo la criptomoneda con mayor capitalización - $19.367.803.766 en USD (16.268.400 BTC). Según Bloomberg, en el año 2016 Bitcoin ha sido el activo más rentable para la inversión, con un crecimiento del 125%. El 9 de abril del 2017 el precio del BTC con respecto al USD ha superado el límite psicológico de 1220 USD por 1 BTC.

Figura 1.Gráfico de precio y capitalización histórica de Bitcoin en USD

Fuente: CryptoCurrency Market Capitalizacion, https://coinmarketcap.com/currencies/bitcoin/

2.2.4. Los inconvenientes detectados

Al margen de los evidentes beneficios que ofrece Bitcoin al usuario final, su utilización puede llegar a provocar ciertas amenazas para las instituciones tradicionales.

En la nota informativa sobre divisas o monedas virtuales emitida por el Departamento de Sistemas de Pago del Banco de España (Gorjón, 2014) en la que se han analizado las ventajas e inconvenientes de Bitcoin, se encontraron también varios riesgos relacionados con esta divisa para el sector bancario y financiero global. Vamos a nombrar algunos de los focos de preocupación que indica Gorjón, y analizar cómo han actuado en realidad a lo largo de los tres años desde el momento de la publicación de la nota. Las amenazas que puede provocar Bitcoin respecto a la banca tradicional son las siguientes:

1) Posibilidad del blanqueo de capitales y financiación de actividades ilícitas

El anonimato, la exclusión del intermediario que pueda detectar comportamientos sospechosos y la descentralización del sistema hacen muy difícil la prevención de actividades ilícitas a través del uso de las monedas digitales. El diseño de la tecnología supone que la responsabilidad completa de sus transacciones caiga a los usuarios, y para los órganos administrativos y regulatorios es una cuestión que puede causar preocupación.

2) Efectos negativos sobre la reputación de pasarelas de pago digitales

Según afirma Gorjón, la reputación negativa y la relación de las monedas digitales con actividades ilícitas pueden provocar la falta de confianza del consumidor a la hora de utilizar las pasarelas de pago online convencionales, que son cada vez más importantes teniendo en cuenta el rápido desarrollo del sector del comercio electrónico en nuestro país y en Europa en general.

3) Tendencias oligopólicas en la creación de la moneda virtual

Debido al diseño del sistema, para conseguir nuevos Bitcoins hace falta implicar cierto poder computacional en verificación de operaciones trascurridas anteriormente y su almacenaje en la cadena de bloques, lo que favorece mayormente a los usuarios que disponen de recursos necesarios, y a su vez hace el “minado” casi inaccesible para los usuarios comunes. No obstante, el autor del informe no ha tenido en cuenta que existe también otra forma de conseguir Bitcoin: además de minar invirtiendo en recursos informáticos y teniendo conocimientos técnicos avanzados, se pueden simplemente comprar criptodivisas al precio actual de mercado en una de las muchas plataformas online, que funcionan como casas de cambio (similar a una casa de cambio de divisa

extranjera convencional), por lo que es totalmente accesible para cualquiera que disponga de conexión a internet. A pesar de ello, se conoce que a día de hoy casi el 80% de toda la potencia de minería está concentrada en China, el país responsable de la mayor parte del volumen de comercio de BTC.

4) Posibilidad de realizar acciones fraudulentas

El protocolo en el que se basa Bitcoin por sí mismo no puede fallar ni ser interrumpido por un tercero. Sin embargo, existen varias "casas de cambio" a través de las cuales se pueden comprar o intercambiar criptodivisas que pueden presentar fallos técnicos a los usuarios a la hora de comprar/intercambiar dinero online. Este tipo de fallos sería completamente centralizado y responsabilidad de la sociedad propietaria de la casa de cambio, que tiene el deber de mantener sus propios servidores protegidos y seguros.

5) Impacto sobre la estabilidad de los precios y estabilidad financiera

Teniendo en cuenta la volatilidad que demuestra Bitcoin en su tasa de cambio respecto a otras divisas o metales preciosos a día de hoy, es posible predecir el efecto que puede tener en la economía general, lo que abre muchas posibilidades para la especulación, por ejemplo. El hecho de que sea tan volátil a la hora de cambiarlo por monedas de curso legal perjudica su función como posible unidad de cuenta para transacciones comerciales. Todo esto sugiere ciertos riesgos operacionales y financieros.

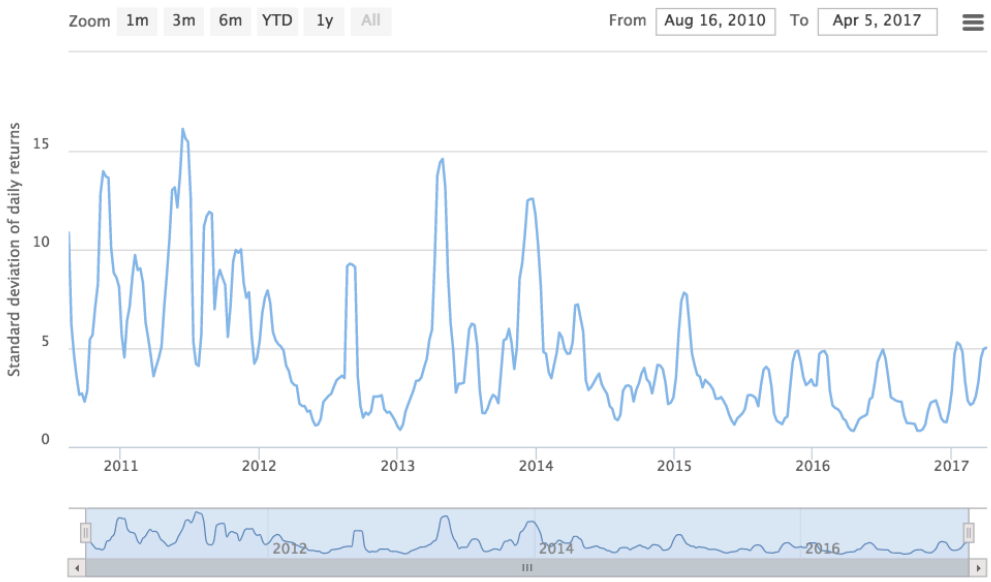

Figura 2. El gráfico histórico de la volatilidad BTC/USD (30 días)

Fuente: The Bitcoin Volatility Index, https://btcvol.info/

En la Figura 2 podemos observar los cambios históricos de la volatilidad de BTC frente al USD. El cálculo del índice está basado en la desviación estándar de las ganancias diarias en los últimos 30 días, son las medidas de la volatilidad histórica de los precios de BTC anteriores. En comparación con monedas fiduciarias, las fluctuaciones de criptodivisa son superiores. Por ejemplo, la volatilidad promedio del oro respecto al USD se calcula alrededor del 1,2%, y en divisas más maduras el promedio es entre un 0,5% y un 0,1%, mientras que la volatilidad de BTC estimada para los próximos 30 días en el momento de nuestro análisis es del 5%. Para que el precio de BTC se estabilice, haría falta una economía de escala que incluyera más usuarios y negocios involucrados en ella. De momento, para evitar la repercusión de la volatilidad y cambios de precios de BTC como el medio de pago es posible (y, de hecho, recomendable) transferir los ingresos de forma instantánea a una moneda más estable, en el caso de un comercio que recibe pagos en BTC y teme perder en la fluctuación de su valor.

Entre otros inconvenientes, Gorjón nombra, por ejemplo, la imposibilidad de realizar el reembolso en caso de fraude, como el que se puede hacer cuando la transacción se realiza mediante un pago con tarjeta bancaria, dado que las transacciones en Bitcoin son irreversibles gracias a la estructura de este medio de pago.

No obstante, existen otras amenazas y problemas fundamentales alrededor de Bitcoin. Vamos a nombrar algunos de ellos.

1) Escalabilidad

Es uno de los temas más polémicos cuando hablamos del futuro y posibilidades de esta criptomoneda. Por un lado, nos referimos a la imagen del Bitcoin: la mayoría de las personas no comprenden su funcionamiento y no confían en él, por lo que está claro que en el corto-medio plazo el crecimiento del uso de BTC está limitado a su adopción. Por otro lado, existen limitaciones técnicas, en concreto, del tamaño de un bloque donde se almacenan las transacciones en la blockchain (o cadena de bloques), que ralentiza la confirmación de transacciones y aumenta el esfuerzo tanto computacional como energético necesario para su ejecución. Como consecuencia, se prevé que para el año 2020 Bitcoin consuma más energía que un país completo como Dinamarca y que producir un solo Bitcoin podría generar más de 4000 kilos de carbono directo a la atmósfera.

Además, los pagos no son instantáneos y requieren confirmación, las comisiones son bastante elevadas y existe un riesgo constante de centralización de la minería. No debemos olvidar que, a pesar de todas las pretensiones de ser un sistema global que revolucionará el sector financiero, Bitcoin sigue siendo un experimento y tiene mucho que desarrollar y mejorar.

2) Comunidad

Siendo un protocolo de código abierto, hay muchas discusiones y debates públicos entre los usuarios y los desarrolladores del Bitcoin acerca de su futuro y la forma de superar las amenazas. La toma de decisiones “colaborativa” respaldada por la comunidad puede ser uno de los puntos fuertes del sistema, pero a su vez la falta de jerarquía en este modelo puede provocar conflictos e incluso caos. La imposibilidad de llegar a un acuerdo acerca del futuro de la criptomoneda puede perjudicar su estabilidad. Por ejemplo, existen 3 principales visiones respecto a la solución del problema de escalabilidad, que representan las propuestas de “Bitcoin unlimited”, “Bitcoin core” y “Bitcoin classic”. La implementación de cualquiera de estas propuestas supondría grandes actualizaciones del software, técnicamente conocidas como “hard fork” (bifurcación – actualización del código o introducción de ciertos cambios en él). Sin entrar en las diferencias técnicas de cada una de las propuestas, podemos decir que el “hard fork” en este caso podría llevar a los usuarios no-expertos en la tecnología a confusión debido a la aparición de diversas opciones bajo el mismo nombre, lo que mermaría la confianza afectando a su cotización y a su valor. Además, la descentralización y la falta de un regulador central podrían tener consecuencias negativas a la hora de resolver problemas técnicos y crisis internas.

3) El rechazo del ETF

El 11 de marzo del 2017 la Comisión de Bolsa y Valores de Estados Unidos (SEC por sus siglas en inglés) ha rechazado el primer fondo de inversión cotizado en bolsa de valores (ETF) basado en Bitcoin - Winklevoss Bitcoin Trust. Entre las razones por las que no ha sido aprobado, la SEC menciona la falta de regulación y control sobre el mercado, altas posibilidades de fraude y la inmadurez general del mercado de Bitcoin. Esto muestra una vez más a Bitcoin como a una divisa a la cual todavía le falta madurar y solucionar muchas cuestiones técnicas y monetarias para poder alcanzar el nivel requerido por la Comisión de Bolsa y Valores.

A día de hoy existen varias investigaciones tanto en el ámbito académico como científico que ponen el foco en el funcionamiento de Bitcoin. Sin embargo, en este

trabajo nos gustaría analizar más en detalle, por un lado, otros sistemas de criptodividas parecidos a Bitcoin o basados en él, y por otro, fundamentalmente, la tecnología de cadenas de bloque, tecnología que muchos llaman la más disruptiva desde la creación de internet, y que tiene todos los requisitos para ser una base de la transformación digital en el sistema financiero y bancario por su capacidad de registrar transacciones sin necesidad de intermediarios, de forma rápida, distribuida y mucho más segura.

2.3. LITECOIN

El hecho de que a día de hoy Bitcoin siga siendo la moneda digital más conocida y popular no impide la existencia de otras criptodivisas (llamadas también "monedas alternativas" al BTC – altcoins) que funcionan principalmente mediante la tecnología de cadena de bloques y los fundamentos del protocolo de Bitcoin, mejorado o modificado de alguna forma.

Litecoin (LTC) es una moneda criptográfica creada en el año 2011 como un "fork" de Bitcoin, es decir, desarrollada de forma independiente a partir de la base del software del Bitcoin. Litecoin ha sido el segundo proyecto "alternativo" de criptodivisa basado en la blockchain después de Namecoin que fue creada en 2010 con pocas diferencias significativas con respecto a Bitcoin. A su vez, Litecoin apareció como una mejora de Bitcoin: su principal objetivo era hacer que las transacciones se ejecutaran más rápido y el proceso de minado fuera más eficiente en costes en recursos invertidos (Haferkorn & Quintana Diaz, 2015).

Actualmente, a 11 de abril del 2017, Litecoin es la cuarta moneda criptográfica con mayor capitalización del mercado (en concreto, $454.042.076). El precio a día de hoy de 1 LTC es 8,98 USD. Actualmente, de los 84 millones de monedas emitidas, 50,5 millones están en circulación [Figura 3].

Figura 3. El gráfico histórico de la evolución del precio LTC/USD y LTC/BTC y la capitalización de mercado (abril 2013-abril 2017)

Fuente: CryptoCurrency Market Capitalizacion, https://coinmarketcap.com/currencies/litecoin/

2.3.1. Propuesta y diferencias con BTC

Litecoin ha "heredado" de Bitcoin sus principales ventajas: la descentralización del sistema, el protocolo criptográfico de código abierto y el funcionamiento por red P2P. No existe ningún órgano que pueda controlar las transacciones entre los usuarios ni influir en ellos de ninguna forma. Por otro lado, se implementa al igual que en Bitcoin el

concepto de anonimato – no es posible saber con certeza la identidad de los actores de la transacción. Además, la emisión de nuevas criptomonedas se produce continuamente a través del proceso del minado y se requiere una elevada potencia computacional. Por último, tanto en Litecoin como en Bitcoin la emisión de monedas no es infinita y está limitada a un número concreto de unidades monetarias.

A pesar de las evidentes coincidencias que podemos observar entre LTC y BTC, existen algunas diferencias.

1) Transacciones más rápidas

En el Litecoin, el nuevo bloque se procesa y se adjunta a la cadena 4 veces más rápido que en BTC (2,5 minutos frente a 10 minutos). Esto permite hacer la confirmación de transacciones con mayor rapidez. Como consecuencia de este incremento de velocidad, también existe un mayor (aunque igualmente mínimo) riesgo de ataque al sistema que en el caso del BTC.

2) Límite de emisión mayor

La emisión de las monedas LTC está limitada a 84 millones de unidades, mientras que en el caso de Bitcoin la emisión está limitada a 21 millones BTC.

3) Barreras de entrada menos rígidas

Litecoin utiliza un algoritmo criptográfico Scrypt, distinto al usado por Bitcoin, SHA256, lo que, por un lado, aumenta la velocidad del proceso de minado, y por otro lado en muchos casos elimina la necesidad de sistemas complejos, haciendo el proceso de minado más accesible y menos costoso para los usuarios y nuevos "mineros".

En resumen, podemos decir que Litecoin es más "ligero" que Bitcoin en todos los sentidos: más veloz para su utilización y minado, y más accesible a cualquier usuario, propuestas que fueron el propósito de su creación.

2.4. RIPPLE

Después de analizar la primera criptomoneda exitosa Bitcoin y su versión mejorada – Litecoin, vamos a hablar de Ripple, una propuesta muy diferente de las anteriores. Existen dudas acerca de que si es correcto llamar Ripple (XRP) criptodivisa debido a numerosas diferencias. Es cierto que su principal función no es esta, pero podríamos decir que sí es una criptomoneda, aunque no es "altcoin", y su solución no está basada en el protocolo del Bitcoin (es decir, no es un fork) ni en la tecnología blockchain por completo. A pesar de esto, a día de hoy la capitalización de Ripple es la tercera mayor del mercado de criptodivisas después de Bitcoin y Ethereum, el cual analizaremos en el apartado 2.5.

El desarrollo de Ripple fue iniciado en el año 2004 por un informático canadiense, Ryan Fugger, y la primera versión RipplePay.com salió a la luz en 2005, unos años antes de la aparición de Bitcoin. En principio Ripple no fue creado como una criptodivisa, sino como un sistema distribuido de pagos internacionales (tanto para monedas digitales como para fiduciarias). De hecho, es un protocolo de código abierto para las transacciones e intercambios financieros. Podemos encontrar muchas similitudes con Bitcoin a la hora de basarse en una base de datos pública distribuida abierta que contiene registro de todas las cuentas y cantidades de monedas en ellas. Sin embargo, entre BTC y la moneda de Ripple XRP existe multitud de diferencias.

Actualmente, Ripple es la tercera criptomoneda con mayor capitalización del mercado, que a 11 de abril de 2017 es de $1.292.619.762 [Figura 4]. Debido a que no estaba pensada como moneda, sino para verificar las transacciones, existe una elevada emisión y el precio de 1 token de XRP es de $0,034455.

Figura 4. El gráfico histórico de la evolución del precio XRP/USD y XRP/BTC y la capitalización de mercado (abril 2013-abril 2017)

Fuente: CryptoCurrency Market Capitalizacion, https://coinmarketcap.com/currencies/ripple/

2.4.1. Propuestas y diferencias con BTC

Para empezar, los usuarios no están obligados a guardar los ahorros en XRP. Ripple tiene tan solo dos objetivos principales – es necesario para el intercambio de divisas y para la protección contra ataques fraudulentos a la red. Cada transacción en la red requiere una comisión mínima de $0,0001, pero a diferencia de BTC esa comisión no se reparte entre la comunidad de mineros, sino que se autodestruye. De esta forma, cada transacción disminuye el número total de monedas de XRP disponibles. Asimismo, si alguien con intenciones de cometer un fraude intenta hacer un ataque en la red mandando miles o millones de transacciones de pequeño volumen con la idea de ralentizar el sistema sobrecargando la red, tendría que pagar un elevado coste.

Una de las características principales de XRP es el gran número de tokens (monedas) emitidos – 100 mil millones. Al mismo tiempo, en Ripple no existe un proceso de emisión de nuevas monedas a través de minado, como en el caso de BTC o LTC, ya que todas han sido emitidas por Ripple Labs (los creadores y desarrolladores del sistema). A día de hoy, se puede comprar XRP en casi cualquier casa de cambio. Cabe destacar que los propios creadores de Ripple definen XRP en la página oficial del proyecto como una “moneda puente” para el intercambio de divisas fiduciarios que como un valor por sí mismo.

Muchos investigadores en el campo de las criptodivisas critican a Ripple por la falta de descentralización real en comparación con BTC. En el caso de Ripple, como hemos mencionado antes, todas las monedas han sido minados por Ripple Labs, por lo que podemos suponer que esa misma organización no solo posee una gran parte de los tokens, sino también controla la seguridad de todas las transacciones dentro del sistema y por tanto la economía de Ripple en general (Armknecht, Karame, Mandal, Youssef, & Zenner, n.d.). Además, si en la comunidad de Bitcoin todos los cambios o implementaciones de mejora se discuten públicamente entre los desarrolladores de diferentes niveles, en Ripple no podemos ver este nivel de transparencia.

Así pues, el proyecto Ripple no es una criptodivisa 100% tal y como la entendemos (poca descentralización, ausencia de proceso de emisión por minado). Sin embargo, no hay que infravalorar su potencial para el sector bancario y las transferencias internacionales. Los casos de implementación del sistema Ripple los analizaremos en el apartado 3.1.

2.5. ETHEREUM

Ethereum es una plataforma para la creación de aplicaciones descentralizadas basadas en la blockchain (cadena de bloques) y acuerdos denominados contratos inteligentes. Además, incluye un lenguaje de programación, un protocolo y una criptodivisa de segunda generación (Ether o ETH). Ha sido propuesta por el creador de la revista Bitcoin Magazine Vitalik Buterin a finales del año 2013, fue desarrollada por él junto a los cofundadores Gavin Woods y Jeffery Wilcke, mientras que la red en versión beta empezó a funcionar en 2015. Ethereum no es una fork de Bitcoin, su protocolo no se basa en él y fue creado de forma independiente, por lo que no es una "altcoin" en el sentido completo. No obstante, les une el concepto de cadena de bloques (en el que Bitcoin fue pionero), la red P2P, la descentralización y la imposibilidad de ser manipuladas, la existencia de una fuerte comunidad de desarrolladores y la emisión de nuevas unidades mediante un proceso de minado.

La "moneda virtual" que se utiliza en el sistema Ethereum – el Ether (ETH) – no fue creada con el objetivo de hacer competencia a BTC en la función monetaria, sino de facilitar las transacciones en la red Ethereum, siendo como "gasolina" para las operaciones. Asimismo, las principales funciones de los Ether son:

1) Prevenir el uso malicioso de la red y la pérdida de control de ella (por ejemplo, ataque de denegación de servicio DDoS), ya que las aplicaciones tienen que pagar Ethers por cada operación ejecutada.
2) Recompensar el esfuerzo de los mineros que contribuyen con la potencia computacional al funcionamiento adecuado de la red descentralizada (algo parecido al concepto de minería en Bitcoin).

Los Ethers son necesarios tanto para los desarrolladores que quieren crear sus aplicaciones en la cadena de bloques Ethereum como para los usuarios que quieren acceder a los contratos inteligentes en Ethereum e interactuar con ellos (Buterin, 2014). En este momento Ethereum es la segunda moneda con mayor capitalización de mercado después de Bitcoin, alcanza un valor de $3.978.823.529, y su evolución está representada en la Figura 5.

Figura 5. El gráfico histórico de la evolución del precio ETH/USD y ETH/BTC y la capitalización de mercado (abril 2013-abril 2017)

Fuente: CryptoCurrency Market Capitalizacion, https://coinmarketcap.com/currencies/ethereum/

2.5.1. Propuesta y diferencias con BTC

Básicamente, Ethereum como sistema es una blockchain programable. En comparación con Bitcoin, que permite a los usuarios realizar ciertas operaciones programadas previamente (como las transacciones), Ethereum hace posible a los

usuarios crear sus propias aplicaciones descentralizadas en la blockchain: no sólo se limita a ser una criptomoneda, sino que les ofrece un uso mucho más amplio. Todo eso gracias a la implementación de la Máquina Virtual de Ethereum (Ethereum Virtual Machine o EVM), que permite desarrollar aplicaciones utilizando lenguajes de programación sencillos basadas en los existentes, como JavaScript o Python. Mientras que Bitcoin permite a los particulares intercambiar efectivo sin la presencia de un intermediario como las instituciones financieras, bancos o gobiernos, el impacto de Ethereum es mucho más amplio. Teóricamente, las interacciones o intercambios financieros de cualquier complejidad pueden ser llevados a cabo automáticamente a través del código escrito en Ethereum. Aparte del uso financiero, puede servir para entornos donde la seguridad y la confianza son esenciales, por ejemplo, en el proceso de elecciones del gobierno, plataformas de crowdfunding o propiedad intelectual, o para asegurar el funcionamiento de IoT (Internet of things o Internet de las cosas).

Siendo una plataforma de código abierto, Ethereum facilita significativamente la implementación de la tecnología blockchain, lo que explica el interés hacia ella no solo por parte de desarrolladores y startups dedicadas a fintech, sino también por parte de las grandes corporaciones tecnológicas, como IBM, Microsoft y Acronis o bancos y entidades financieras como JP Morgan Chase.

2.5.2. Smart Contracts

El funcionamiento del Ethereum se hace posible debido a los contratos inteligentes (Smart contracts). Han sido descritos por primera vez en el 1997 por el criptógrafo y jurista Nick Szabo, aunque el concepto no se ha podido realizar en práctica por falta de la infraestructura necesaria: transacciones programables y un sistema financiero que las reconozca (Szabo, 1997). Gracias a Bitcoin y concretamente su tecnología, la cadena de bloques, esta tecnología ha sido puesta en práctica y empieza a jugar un papel cada vez más importante en el sector financiero, entre otros.

2.5.3. ¿Qué son los Smart Contracts y cómo funcionan?

Esencialmente, con “contrato inteligente” entendemos un algoritmo electrónico (o programa informático) que se ejecuta de forma autónoma y automática para hacer efectivos los términos de un contrato cuando se cumplen las condiciones estipuladas previamente por las partes implicadas en el contrato en el momento de su firma. Tanto personas como máquinas pueden actuar como partes de un contrato inteligente, lo que abre una puerta al funcionamiento del Internet de las cosas, sin necesitar ninguna intervención humana en el proceso. A diferencia de un documento legal tradicional, el contrato inteligente no necesita confianza, ya que todo está automatizado y la posibilidad de engaño es nula, y además no requiere de un tercero (como un notario, un abogado o un banco). A causa de esta ausencia de intermediarios, los gastos de operación bajan significativamente, aumentando a la vez la velocidad del procedimiento. Los usos que se podrían dar a los contratos inteligentes son muy variados. Por ejemplo, control de gastos, desde los límites de reintegro diarios hasta la concesión o la recisión del acceso a entidades específicas. Igualmente, podrían ser base para los préstamos, depósito de garantía o regular el procesamiento de herencias y donaciones.

2.5.4. Ventajas e inconvenientes de los Smart Contracts

Aparte de eliminar la necesidad de confianza en terceros y de intermediarios, reducir el tiempo de ejecución y disminuir las comisiones, existen también otras ventajas propias de los Smart contracts. El hecho de estar registrado y almacenado en la cadena de bloques distribuida aporta al contrato inteligente una gran seguridad: no puede ser destruido por fuerza física o robado. Por otro lado, su amplio uso y bajo coste son otras ventajas que lo hacen tan atractivo para los usuarios. No obstante, como cualquier tecnología que está en fase de implementación y desarrollo, tiene sus imperfecciones y una serie de inconvenientes.

1) **La imposibilidad de modificar directamente la información dentro de un contrato una vez suscrito.**

La imposibilidad de realizar un cambio en la cadena de bloques que por un lado puede ser una ventaja fundamental, pero también puede resultar un problema a la hora de firmar un contrato a largo plazo: si la legislación o las condiciones cambian, e incluso las dos partes que firmaron el contrato estén de acuerdo en la alteración de obligaciones o requisitos, no existe forma de cancelarlo o modificar, el programa va a ejecutarlo igualmente.

2) **La necesidad de altos conocimientos técnicos para la creación de un contrato inteligente.**

Si un individuo quiere crear un contrato programándolo, le harán faltan, por un lado, altos conocimientos de programación, del protocolo de la blockchain y de la criptodivisa para realizarlo con éxito. Por otro lado, le sería imprescindible tener una fuerte base de conocimientos legales, porque al final se trata de un contrato con fuerza jurídica. Por lo tanto, es muy probable que en un futuro la profesión del abogado no desaparezca, sino que su labor se transforme a la programación de contratos inteligentes individualmente. Aun así, por ahora la figura de este notario digital va a seguir existiendo, hasta que aparezcan plataformas que permitan crear este tipo de contratos a base de una plantilla (como analogía con la creación de las páginas web: en principio se necesitaban conocimientos para programar una, pero a día de hoy casi cualquiera puede crear su página web sin necesidad de conocimientos informáticos). Tampoco podemos olvidar de que en el caso de contrato inteligente un error en su programación puede costar muy caro a los que lo firman, ya que, como hemos explicado en el punto anterior, es irreversible.

3) **Falta de legislación en los diferentes países**

Aunque creemos que es una cuestión del tiempo, por ahora existe un vacío legal con respecto al uso de contrates inteligentes. Esa falta de precedentes jurídicos genera desconfianza por parte del usuario que no tiene conocimientos técnicos ni entiende cómo funciona. No obstante, la realidad es que muchas entidades financieras, como BBVA o Banco Santander, están desarrollando contratos en este campo y empiezan a implementar esta tecnología, lo que podría dar pie a que en un futuro la legislación considere la validez de este tipo de contratos.

2.6. CRIPTODIVISAS ANÓNIMAS (DASH, XMR, ZEC)

Actualmente existen también criptodivisas basadas en la blockchain cuyo valor principal es la privacidad y el anonimato, ya que, como sabemos, en el sistema de Bitcoin las transacciones de una cartera a otra están abiertas y es fácil de seguir el rastro y descubrir de dónde viene ese dinero o a quien pertenecía antes a través de los registros en la Blockchain. Aunque no sabemos con seguridad a quien pertenece la cartera virtual, se puede detectar patrones en el comportamiento y analizarlo, o, en caso de las autoridades, se puede encontrar esa información a través de las casas de cambio, donde el primer comprador sí ha abierto sus datos personales. Pues en este apartado vamos a ver en términos generales las tres criptodivisas que pretenden ofrecer confidencialidad completa a sus dueños – DASH, Monero (XMR) y Zcash (ZEC).

2.6.1. Propuesta y diferencias con BTC

1) **Dash**

Dash (previamente Darkcoin y XCoin) es un sistema de pago descentralizado que utiliza la tecnología “Darksend” para anonimizar las transacciones. Fue creado en 2014 como un fork de Bitcoin, y a día de hoy su criptodivisa DASH tiene una de las mayores capitalizaciones de mercado (por encima de 450 millones de dólares en abril del 2017). La cantidad de monedas emitidas es igual que en Bitcoin y se limita a 21

millón de unidades monetarias. En la actualidad, DASH es la cuarta criptomoneda con mayor capitalización de mercado y su valor a 11 de abril de 2017 es de $62,32 [Figura 6].

Figura 6. El gráfico histórico de la evolución del precio DASH/USD y DASH/BTC y la capitalización de mercado (abril 2013-abril 2017)

Fuente: CryptoCurrency Market Capitalizacion, https://coinmarketcap.com/currencies/dash/

Las principales diferencias con Bitcoin son los siguientes:

- El anonimato completo de las transacciones.
- En vez de usar un solo algoritmo criptográfico, Dash utiliza una combinación de varios a la vez.
- El minado de DASH requiere menos recursos energéticos que el de Bitcoin.
- Todas las decisiones acerca de crecimiento y desarrollo del sistema las toman todos los usuarios del sistema, y no programadores particulares, mediante la "Gobernanza descentralizada" (Descentralized Governance). Cualquier usuario puede ofrecer una mejora o un cambio en el sistema DASH, y el resto vota a favor o en contra de la propuesta.

2) Monero

Monero o XMR es una criptodivisa con código abierto para las transacciones monetarias anónimas. Antes de la aparición de Zcash, la cual analizaremos más adelante, Monero se consideraba como la moneda más privada y segura de todas. Apareció en abril del 2014 como otro fork de Bytecoin, que fue la primera en usar un protocolo criptográfico distinto al de Bitcoin – CryptoNote, el que permite no desvelar el emisor ni receptor ni tampoco la cantidad de la transacción, aunque también se registran en la Blockchain.

Otra novedad implementada por Monero es la tecnología "ring signatures" (o firmas de anillo) – es un grupo de firmas criptográficas en la que solo una de las que aparecen es real, pero no hay forma de saber de dónde provienen, por lo que de esa manera se mantiene el anonimato excepto para las partes involucradas. Aun así, existen expertos que advierten que el anonimato de Monero no es absoluto y en ciertas circunstancias existe la posibilidad de desanonimizar una parte de transacciones.

Monero es la sexta moneda digital con mayor capitalización del mercado. A día de hoy circulan más de 14 millones de unidades monetarias XMR, y el precio actual de 1 XMR es de $21,47.

Figura 7. El gráfico histórico de la evolución del precio XMR/USD y XMR/BTC y la capitalización de mercado (abril 2013-abril 2017)

Fuente: CryptoCurrency Market Capitalizacion, https://coinmarketcap.com/currencies/monero/

A diferencia con muchas otras criptomonedas, la cantidad de emisión de XMR es ilimitada, es decir, virtualmente infinita. En el aspecto legal, el anonimato les preocupa a las autoridades, y existen países donde se está intentando prohibir el uso de monedas digitales completamente anónimas (por ejemplo, Italia). Y esas preocupaciones tienen su base: se conoce que Monero se utiliza activamente por los usuarios de la "Dark web" (o el internet oscuro, que básicamente es el "mercado negro" online donde se puede comprar todo tipo de objetos o actividades ilegales, como drogas y armas) que lo utilizan como medio de pago frecuente por el anonimato que les permite tener.

3) Zcash

Esta criptomoneda descentralizada de código abierto hace énfasis en la privacidad de las transacciones, y aunque la blockchain en la que se publican es pública, no desvela al receptor y ni el emisor, ni la cantidad enviada. Mientras que la infraestructura de Zcash no pretende ser muy innovadora, la innovación está en el algoritmo "zero-knowledge proofs" (prueba de conocimiento cero), que permite al creador de la transacción incluir en ella una prueba de validez (que en la cuenta existe cantidad de monedas necesaria para la transacción) sin necesidad de trasmitir ninguna información aparte del hecho de que la transacción es cierta (Ben-Sasson et al., 2014). De este modo, no es posible que un tercero lea la información privada, a menos que las partes que participaron en la transacción deseen desvelar su información.

La criptomoneda Zcash se sitúa actualmente en el puesto número 11 en la lista de las divisas criptográficas con la mayor capitalización del mercado con un valor de $67.495.717 [Figura 8], y su precio de momento está a $63,59, mientras que en libre circulación existen poco más de un millón de unidades monetarias ZEC.

Figura 8. El gráfico histórico de la evolución del precio ZEC/USD y ZEC/BTC y la capitalización de mercado (abril 2013-abril 2017)

Fuente: CryptoCurrency Market Capitalizacion, https://coinmarketcap.com/currencies/zcash/

Salida a la luz a finales del 2016, la criptomoneda Zcash reúne en sí los nuevos avances de la criptografía y la experiencia del funcionamiento de las criptodivisas desde su creación. Además, esta divisa tiene una diferencia con respecto a Bitcoin y muchas otras monedas – Zcash es también una empresa, lo que hace su producto más atractivo para los inversores. La limitación de la emisión de unidades monetarias es la misma que en Bitcoin, 21 millones de las unidades monetarias, pero el 10% de ellas se repartirán entre los fundadores, inversores y empleados.

CAPÍTULO 3. LA TECNOLOGÍA DE CADENA DE BLOQUES EN EL SECTOR FINANCIERO Y BANCARIO

Después de analizar las criptomonedas con mayor capitalización de mercado, nos vamos a centrar en la tecnología que hace que todas ellas sean posibles – la cadena de bloques o Blockchain, ya que su uso no está limitado sólo a la creación de divisas alternativas, sino que abre muchas oportunidades para diferentes sectores, sobre todo el bancario y el financiero.

Según el informe "Blurred lines: Cómo Fintech está redefiniendo el sector financiero" elaborado por la consultora PwC en 2016, el 56% de los profesionales de la banca reconocen su importancia, ya con este protocolo podría cambiar radicalmente el sector, mientras que un 57% aseguran que no saben cómo responder a los desafíos que plantea, y tan solo un 15% de los directivos encuestados han afirmado estar familiarizados con la tecnología Blockchain (Kashyap, Garfinkel, & Shipman, 2016).

Pero, ¿qué es exactamente la Blockchain? Básicamente, es un registro distribuido entre muchas partes diferentes y protegido criptográficamente. Esta base de datos distribuida registra bloques de información y los entrelaza para facilitar la recuperación de la información y verificación de que esta no ha sido cambiada, por lo que nunca puede ser borrada y contiene todas las transacciones que se han hecho en su historia. Es decir, una red distribuida, resistente a la manipulación de datos y en la que queda totalmente identificada la autoría de la transacción. Es global, perpetua, inmutable y automática. Además, es un algoritmo matemático y criptográfico de elevada dificultad, lo que garantiza la máxima eficacia y eficiencia de esta tecnología.

Los escenarios en los que se está haciendo pruebas son bastante amplios, aunque se podrían destacar los siguientes usos:

- **Comprobar la titularidad y propiedad**

Implementar la tecnología Blockchain imposibilita la manipulación o eliminación de datos ya introducidos en un bloque de la cadena, lo que permite registrar las operaciones de manera segura y permanente.

- **Demostrar la autenticidad**

Registrar en la Blockchain datos de la fuente de donde fue obtenida una propiedad y una prueba de su autenticidad evita casos de falsificación de productos.

- **Gestionar la información descentralizada**

Es posible almacenar la información sensible de forma distribuida y, de esa manera, protegerla más que si fuera guardada en un servidor, ya que los servidores centralizados son mucho más vulnerables a los ataques y los datos pueden ser robados y/o borrados con relativa facilidad.

- **Transferir activos tanto digitales como reales**

Utilizar contratos inteligentes (Smart contracts) permite realizar transferencias de activos de forma transparente, prácticamente instantánea, automatizada y a coste menor que si se hiciese de forma tradicional.

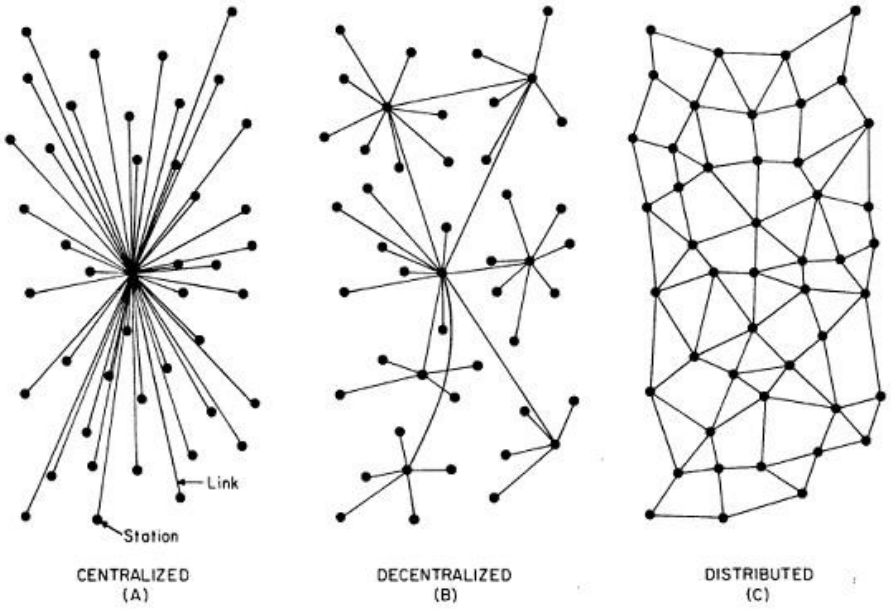

Figura 9. Ilustración de los conceptos: centralizado, descentralizado y distribuido

Fuente: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Los principales ámbitos en los que se podría aplicar son los siguientes:

- Gestión de bienes digitales, certificación de propiedad intelectual o industrial de cualquier tipo de creación (desde la propiedad intelectual de artistas o músicos particulares hasta propiedad de terrenos e inmobiliario).
- La sanidad – la información que gestiona el sistema sanitario puede estar almacenada de forma ágil y privada (encriptada) de tal forma que solo el paciente mismo decide quién puede ver su expediente médico.
- El internet de las cosas (IoT por sus siglas en inglés "Internet of Things") – en el futuro próximo nos espera la aparición de miles de millones de dispositivos conectados a internet (desde los frigoríficos y lavadoras inteligentes hasta coches autónomos), y el modelo centralizado no va a tener suficiente capacidad para almacenar toda la información que producen y comparten. Además, la Blockchain es la mejor solución para los pagos M2M (machine to machine, máquina a máquina) utilizados ampliamente en IoT.
- La Identidad Digital – por un lado, permite al usuario compartir los datos personales solo con las entidades necesarias y en la cantidad necesaria, y por otro lado soluciona el problema de algunas regiones del mundo (por ejemplo, África Subsahariana) donde un gran porcentaje de la población no tiene ningún tipo de documentación personal. La identidad digital sería totalmente transparente para su dueño, a la vez se protegerían sus derechos de privacidad. El certificado de nacimiento, certificados de matrimonio, cuentas bancarias, títulos universitarios o diplomas de educación, básicamente cualquier tipo de documento personal puede ser almacenado en tiempo real en la cadena de bloques y pertenecer solo al poseedor del mismo y no a terceros.
- Seguridad alimenticia (posibilidad de rastrear todo el camino de un alimento desde el primer eslabón de la cadena de suministro hasta la mesa del consumidor) o seguridad farmacéutica, ya que para esta industria supone pérdidas millonarias la falsificación de medicamentos. A día de hoy ya existe una startup con nombre bext360 que está implementando un sistema para los pagos justos e instantáneos a los proveedores del café (el segundo bien más comprado después del petróleo), para almacenar en la cadena de bloques toda la información sobre el origen de donde provienen los granos y quién ha pagado por ellos, haciendo que el comercio sea más justo para los pequeños productores del café en los países subdesarrollados.

- El sector gubernamental – la blockchain permite almacenar la información de forma distribuida y disminuir la burocracia. Además, daría lugar a nuevas formas de votación popular en elecciones de diferentes niveles, garantizando la transparencia total de este procedimiento democrático líquido.
- Control y gestión de la cadena de suministro – monitorizar las transacciones y hacerlas más transparentes podría hacer a la cadena de suministro más eficiente, reduciendo el tiempo, costes adicionales y la posibilidad del fallo humano.
- La economía compartida – la solución que ofrece la Blockchain permite realizar pagos P2P en los servicios tipo Blablacar, Uber o Airbnb, que los haría verdaderamente transparentes y reduciría significativamente los costes, ya que eliminaría la parte de intermediación que ofrecen estas empresas. Así, para compartir un viaje con otra persona el conductor podría recibir pagos directos, pero a la vez estar convencido de que no se trata de un fraude, porque el viaje estaría registrado en el sistema distribuido.

Como vemos, las aplicaciones que puede tener la Blockchain van mucho más allá de Bitcoin o las criptodivisas, se siguen desarrollando y se están estudiando las nuevas formas de beneficiar a la sociedad. La funcionalidad de la tecnología Blockchain, que muchos de los investigadores comparan con internet por el gran impacto que puede causar, es capaz de eliminar la figura de un intermediario – una empresa o corporación que se encarga de guardar los datos o información sobre los derechos del usuario. Pero para eliminar las instituciones intermediarias hace falta crear todo un nuevo paradigma de conocimiento y confianza hacia la tecnología que lo permite. Por lo tanto, en caso de los bancos y entidades financieras la única forma de no quedarse atrás es implementando esta tecnología verdaderamente disruptiva para mejorar la calidad y la viabilidad de sus servicios, ya que la Blockchain se lo permite.

En el informe “Top 10 Strategic Technology Trends for 2017” la consultora de investigación de las tecnologías informáticas Gartner ha posicionado la tecnología Blockchain y los registros distribuidos en el sexto lugar de las más disruptivas y prometedoras. Según Gartner, la mayoría de las iniciativas de registros distribuidos están en la fase temprana de desarrollo. Los múltiples casos de utilización en los negocios también están en el proceso de pruebas, sin embargo, el 52% de los encuestados por la consultora creen que la tecnología blockchain afectará a su negocio (Cearley, Walker, & Burke, 2016), lo que hace esta tendencia difícil de ignorar.

En un mundo en el que se realizan transacciones las veinticuatro horas del día en cualquier sector empresarial y a través de varios canales, la verdadera aportación de la tecnología blockchain sería permitir que las transacciones ocurran cada vez más rápido, fácil y con menores costes. Está claro que la implementación de la tecnología de cadenas de bloques será un desafío. Aprovechar esta tendencia requiere una supervisión estrecha, definiciones claras y el conocimiento de las limitaciones, pero su adopción con éxito, sin duda, va a revolucionar los modelos operativos para todas las industrias en los próximos años.

Otra de las características que hay que destacar cuando hablamos de esta tecnología, es que la Blockchain no es única. Debemos diferenciar entre la tecnología Blockchain pública y la tecnología Blockchain privada. Aunque los principios en los que se basan son, básicamente, iguales, cada una tiene objetivos, modelos de financiación y de inversión completamente diferentes.

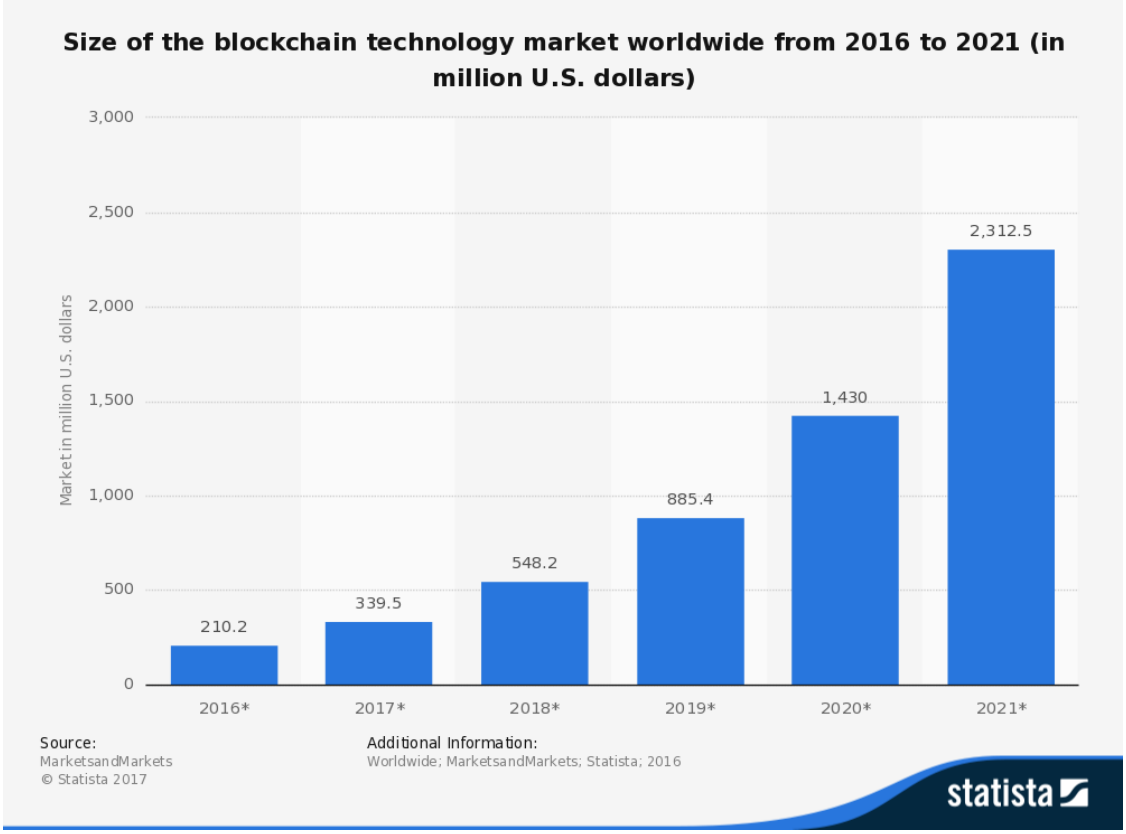

Figura 10. El volumen del mercado global de la tecnología Blockchain entre los años 2016 y 2021 (millones de dólares)

Fuente: MarketansMarkets, Statista, 2017

1) **Blockchain públicas**, también llamadas cadenas de bloques sin permiso (en inglés "permissionless"). Puede ser consultadas en cualquier momento por cualquiera, y todos pueden enviar transacciones que se guardarán en los bloques de la cadena una vez dispongan de recursos necesarios en su cartera digital. Es la más conocida, ya que las criptodivisas como Bitcoin, Ethereum o Zcash han sido emitidas en ella, y esa ha sido la forma para financiarla, aunque ya sabemos que las cotizaciones son muy inestables y suponen un riesgo elevado para los inversores. Otra diferencia es que dentro de la Blockchain pública el proceso de consenso (cuáles son los bloques que serán agregados a la cadena) es abierto. Además, pretende ser "totalmente descentralizada". La seguridad se la cadena pública está en los mecanismos criptográficos (por ejemplo, la prueba de trabajo o proof-of-work). Los usuarios tienen que disponer de una firma digital para realizar las transferencias bajo pseudo-anonimato, lo que supone que el usuario, por un lado, puede crear un número ilimitado de carteras, pero, por otro lado, el acceso a todas las transacciones es público y existe la posibilidad de encontrar patrones y formas de conocer el usuario final.
2) **Blockchain consorciada,** o híbrida. Se financian principalmente por consorcios de empresas y por capital de riesgo. Los consorcios suelen ser formados por las empresas líderes en el sector financiero y bancario, donde todas están conectadas a la cadena de bloques y algunas tienen que verificar cada bloque para confirmar su validez. En este caso, el consenso es necesario, aunque las normas pueden modificarse por un acuerdo con las instituciones que forman el consorcio. También se puede exigir el cumplimiento de ciertas normativas, por ejemplo, la de identificación del usuario – KYC (Know Your Customer). Siendo las propias partes del consorcio los que verifican las transacciones, no es necesario tener una criptomoneda como incentivo. Obviamente, en el caso de la Blockchain consorciada la descentralización

global no es posible de conseguir, pero sí puede estar distribuida entre las entidades preseleccionadas.

3) **Blockchain privadas**, llamadas también con permiso (en inglés "permissioned"). Consiste en construir una Blockchain dentro de la empresa o un organismo particular, y con permiso de escritura solo dentro de la organización, mientras que los permisos de lectura pueden ser totalmente privados o de alguna forma restringidos. Lo más parecido a la blockchain privada es una base de datos encriptada.

	BLOCKCHAIN PUBLICA	BLOCKCHAIN PRIVADA
ACCESO	Lectura y escritura abiertas	Lectura y/o escritura bajo permiso
VELOCIDAD	Más lenta	Más rápida
SEGURIDAD	Red abierta	Participantes aprobados
IDENTIFICACIÓN	Anónimas o pseudo-anónimas	Las identidades se conocen
ACTIVOS	Nativos	Cualquier activo

Tabla 1. Cadenas de bloques privadas y públicas

Fuente: Elaboración propia, datos: http://www.coindesk.com/research/state-of-blockchain-q4-2016/

Mientras que las cadenas de bloques públicas (como la de Bitcoin) suponen un cambio de paradigma y un paso hacia la economía global digital, las privadas pueden formar parte de las estructuras existentes.

Está claro que la Blockchain no es la respuesta a todo, sin embargo, existen varios ámbitos en los cuales su implementación puede llevar a mejoras significativas tanto para los clientes particulares como para los principales protagonistas del sector, y entre ellos destaca el sector bancario y financiero.

3.1. PRIMERAS PROPUESTAS PARA BANCA

Los bancos tradicionales disponen de las siguientes características:

1) Son altamente centralizados y teóricamente pueden sufrir un ataque a los servidores donde se almacena la información de sus clientes.
2) Excluyen una gran parte de la población. Según el informe del Banco Mundial, el 74% de la población del mundo no tiene acceso a los servicios financieros básicos (Demirgüç-Kunt, Klapper, Singer, & Van Oudheusden, 2015). La tecnología Blockchain permitiría incluir esa población en la economía global.
3) Ralentizan los procesos – las transacciones incluso dentro de la misma ciudad pueden tardar días o semanas en ser operadas.
4) Altas comisiones (10 o 20% solo por el hecho de enviar dinero a otro país).
5) No aseguran la privacidad de los usuarios al cien por cien.

La blockchain a menudo se compara con Internet, pero mientras internet es la red que permite trasladar la información, blockchain es la red que permite hacerlo con el valor. Aunque la innovación ha revolucionado todos los ámbitos de la sociedad y del mundo global, los bancos todavía utilizan tecnologías e infraestructuras que han sido creadas hace muchos años y deben renovar algo que es totalmente ineficiente en esta época, cuando el comercio electrónico internacional está en auge y la globalización permite a la gente vivir y trabajar en diferentes países con diferentes divisas.

Según los datos de Aite Group, las instituciones financieras solo en el año 2015 han invertido 75 millones de dólares en la tecnología blockchain (Petrasic & Bornfreund, 2016). Es casi doble de lo invertido en el 2014, y Aite estima que las inversiones van a seguir aumentando anualmente.

Los servicios financieros en los que la tecnología blockchain puede tener el mayor impacto son los siguientes:

1) **Seguridad y autenticación**: la tecnología de cadena de bloques permite verificar la identidad de forma segura en el proceso de transacción sin necesidad de intermediarios – algo que hoy en día hacen las instituciones supervisoras y los bancos.
2) **Ahorros**: también gestionados por bancos de inversión y los brokers, los bonos, las acciones y las letras del Tesoro podrían ser gestionados a través de la blockchain y en concreto gracias a la utilización de la red P2P.
3) **Inversión y capital de riesgo**: este tipo de inversiones son muy frecuentes en el mundo del emprendimiento, aunque el proceso es bastante complejo ya que la inversión puede provenir de diferentes actores. El uso de la tecnología y la red P2P en este caso podría hacer este proceso más seguro y transparente.
4) **Innovación en contabilidad**: el registro financiero puede llevarse a cabo de una forma más fiable y sistemática. Eso ayudaría a las auditorías a ser más transparentes, ya que la contabilidad es una de las áreas de los negocios que menos ha abrazado la transformación digital. Además, las auditorías tendrían acceso fácil y rápido a los movimientos y datos de distintas empresas.
5) **Contratos inteligentes:** la implementación de contratos informatizados y automatizados podrían acelerar procesos que hasta el día de hoy han sido lentos y costosos, y muchas veces necesitan participación de intermediarios. Vamos a analizar este tipo de contratos y su utilidad para el sector bancario y financiero en los apartados 3.2 y 3.3 del presente capítulo.
6) **Las operaciones bursátiles**: reduciendo los tiempos de liquidación, la tecnología blockchain podría generar oportunidades más grandes para el acceso a servicios financieros, sobre todo en las operaciones bursátiles que consisten en el intercambio de diferentes instrumentos para la inversión o especulación. Dentro de este ámbito, la tecnología permitirá cambios principalmente en los servicios de compensación y liquidación de valores.
7) **La seguridad de los préstamos:** utilizando un nuevo tipo de derivados que se basan en la reputación, definidas por el capital económico y social y por el comportamiento digital de particulares y empresas, la blockchain permite reducir el "riesgo de contraparte", que es el riesgo de que la otra parte con la que se negocia se pueda declarar insolvente antes de la finalización del acuerdo. Es decir, se podría garantizar la solvencia de los sujetos financieros.
8) **Servicios y sistemas de pago:** la blockchain, gracias a sus algoritmos criptográficos, es capaz de solucionar el "problema de doble gasto", es decir, que el dinero que se está transfiriendo no se puede duplicar y ser gastado más veces de lo debido. Pero además la tecnología ayudaría a la democratización del crecimiento económico, pudiendo transferir no solo el dinero a través de las redes de pago, sino también cualquier bien financiero, como los bonos, por ejemplo.

Además, gracias a la tecnología Blockchain se podría reducir e incluso eliminar varias formas de riesgo financiero. Aparte del riesgo de contraparte, que hemos mencionado anteriormente, se reduciría el riesgo de liquidación (que por algún fallo técnico la transacción sea devuelta al remitente) y el riesgo del agente. Aunque lo más importante sería reducir de esta manera el riesgo sistemático, disminuyendo las interdependencias de las entidades financieras. La gestión de riesgos en los mercados financieros ha causado la aparición de distintos productos derivados y otras herramientas financieras. Según las últimas estimaciones, el valor de todos los

derivados extrabursátiles puede llegar a 600 mil millones de dólares (Tapscott, Salmerón Arjona, & Tapscott, 2017). Pero el uso de este tipo de derivados para gestión de riesgo podría ser mucho más transparente si se utilizasen los modelos de seguros descentralizados que la blockchain hace posibles, por ejemplo, basados en la reputación o el capital socioeconómico. En el año 2015 los profesionales de Wall Street ya tenían una opinión altamente positiva sobre la tecnología blockchain y su impacto en el sector: según la encuesta, el 94% de los entrevistados están convencidos de que el sistema de cadena de bloques tiene todos los requisitos para desempeñar un papel importante en las finanzas (Leising, 2015), sobre todo por la capacidad de reducir el riego sistemático.

3.1.1. El caso de Ripple

En el apartado 2.4 hemos analizado la criptodivisa XRP y la hemos comparado con BTC, pues ahora veremos cómo funciona la tecnología Ripple y qué ventajas puede ofrecer a los bancos.

Ripple se pone como objetivo renovar y reinventar la infraestructura de los pagos, especialmente a nivel internacional, los que más tardan y más comisiones llevan en el sistema actual. Ellos proponen utilizar generalmente las monedas fiat, y es un mercado bastante estable que tiene barreras de entrada muy rígidas y líderes como Western Union, mientras que la tecnología Ripple podría poner en peligro su funcionalidad e incluso existencia. Aun así, el creador de Ripple y CEO de Ripple Labs Chris Larsen admite que pueden ofrecer más transparencia, mejores costes y mayor rapidez, lo que puede ser fundamental para las empresas y los particulares.

Las cadenas de bloques privadas, como la que tiene Ripple, se diseñan con el objetivo de ser más eficientes y escalables para manejar el volumen de transacciones muy alto. La blockchain de Ripple es capaz de verificar las transacciones mucho más rápido que la blockchain de Bitcoin. Sin embargo, los validadores de transacciones en el caso de Ripple son empresas privadas, tienen sistemas informáticos reguladores con varias limitaciones. Una solución interesante a esta limitación ha sido el desarrollo del protocolo intermediador - “the InterLedger Protocol” (ILP). ILP por sí no es un “libro mayor”, ya que no busca el consenso hacia ningún estado, sino que provee un sistema criptográfico de garantías de capa superior que permite el movimiento de fondos entre los registros distribuidos (por ejemplo, como las bases de datos tradicionales) con la ayuda de intermediarios llamados “conectores” (Bheemaiah, 2017). Como resultado, las barreras de entrada son bajas, y los bancos pueden conectar sus sistemas centrales a la red de Ripple de la misma manera que se conectan con la red SWIFT.

En el proceso de una transacción internacional, Ripple Connect coordina el intercambio de información directamente entre el banco remitente y el receptor, sin tener que utilizar el intermediario. Además, ILP Ledger utiliza el Protocolo Interledger (protocolo de código abierto creado por los ingenieros de Ripple para interconectar los bancos con la Blockchain) para coordinar el movimiento de fondos entre las instituciones involucradas en la transacción.

El proceso de pago a través de Ripple es el siguiente. Primero, la capa de traducción analiza el mensaje y recoge la información necesaria para comenzar el proceso de pago. Ripple Connect se comunica con el banco correspondiente y el beneficiario para obtener sus tasas de procesamiento de pagos y el coste total al cliente. Después se produce la validación anterior a la transacción (pre-transaction validation) que incluye la verificación de las cuentas. Cuando los dos bancos tienen todos los datos necesarios, pueden pre-validar el pago incluso antes de que se produzca el movimiento de fondos. Luego se coordina el flujo de fondos a través de ILP Ledgers privadas de las tres instituciones distintas (banco de origen, banco correspondiente y banco beneficiario). Ripple coordina el proceso de retención de fondos en esos tres niveles. ILP Ledger genera firmas criptográficas para verificar que los fondos están comprometidos con la transacción. Después, los fondos son liberados

simultáneamente en los tres registros. Este proceso garantiza que no haya ningún riesgo de liquidación, los pagos pueden ser ejecutados o fallados. Al finalizar, Ripple envía mensaje de confirmación a todas las contrapartes. Todo el proceso entre múltiples bancos tarda segundos y proporciona visibilidad y transparencia de la transacción de extremo a extremo, aumentando las tasas de procesamiento y bajando costes operacionales de transacción. Asimismo, el tiempo y el coste son las dos principales ventajas que ofrece Ripple a sus clientes. En el caso de las empresas con las que trabaja, otra de las ventajas es la eliminación del riesgo de liquidación. Además, Ripple utiliza mensajería estándar del sector – ISO y MT – y por eso no hay pérdida de datos corporativos en los mensajes de pago, dado que los participantes están multilateralmente conectados.

Las etapas son las siguientes:

1) **Obtener cotización**[1].

El banco de origen envía una solicitud de cotización a través de la red Ripple para el pago en cuestión. Las cotizaciones recibidas en respuesta incluyen también tarifas y requisitos de cumplimiento.

2) **Aceptar cotización.**

El banco de origen acepta la mejor cotización para que puedan cumplir con los requisitos. El banco beneficiario puede bloquear la cotización. En este punto, Ripple bloquea los fondos en los "ledgers" o libros mayores de los dos bancos, algo así como un segundo acuerdo de depósito de garantía (sin transferencia de título todavía).

3) **Enviar el pago.**

El banco de origen transfiere los fondos de la cuenta del abonador y de ILP al banco beneficiario.

4) **Afirmar el recibo del pago.**

El banco beneficiario confirma que los fondos han sido acreditados a la cuenta del beneficiario. Todo el proceso tarda entre 1 y 2 segundos.

A contrario de otras startups del sector fintech, Ripple se centra en los bancos, y son ellos y no los clientes finales los que se tienen que conectar a la red Ripple. Esto tiene dos principales ventajas. Por un lado, los consumidores están acostumbrados a confiar en los bancos y es mucho más probable que para las operaciones financieras elijan un banco de confianza que una startup nueva. Por otro lado, en cuanto a la comunicación con las entidades reguladoras, también resulta menos complicado teniendo como socios a los bancos tradicionales (Blair, 2016).

Los creadores de Ripple admiten, que su proyecto en alguna forma es contradictorio a lo que era la idea de Satoshi y lo que ha llamado la atención de tanta gente de la comunidad Bitcoin en su momento, que era destruir todo el sistema financiero centralizado actual. No obstante, ellos creen que los bancos tienen potencial para la innovación y deben ser el corazón de la nueva realidad financiera, y por eso quieren proveer la tecnología que puede ayudarles a conseguir este objetivo.

[1] Con la cotización en este contexto entendemos el valor alcanzado por una divisa, el precio al que se puede efectuar su compra o venta (Montes de Oca, 2017)

Figura 11. El funcionamiento de la criptomoneda XRP dentro de Ripple

Fuente: http://www.ripple.com

3.1.2. Ripple y GPII: la comparación

En respuesta al desafío de Ripple, SWIFT (por sus siglas en inglés: Society for Worldwide Interbank Financial Telecommunication o Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales) en enero del 2017 ha lanzado GPII (Global Payments Initiative o Iniciativa de pagos globales). No obstante, este sistema tiene varios inconvenientes frente a Ripple. Vamos a nombrar algunos de ellos:

- La velocidad de pagos

Si en Ripple un pago se tarda entre 1 y 2 segundos en procesar, GPII puede tardar horas e incluso días.

- La tasa de cambio

En el caso de Ripple, el sistema automáticamente elige la menor tasa de cambio posible, mientras que en GPII la tasa se determina por el mismo banco.

- La información de seguimiento

El rastreo es totalmente innecesario en Ripple, por lo cual no existe. Sin embargo, en GPII sí se puede obtener esa información.

Por consiguiente, aunque GPII claramente aporta algunas mejoras significativas en el sector de transacciones bancarias internacionales, el impacto de esta tecnología es menor en comparación con Ripple, ya que no cambia tan radicalmente los pagos transfronterizos. Ripple propone pagos casi instantáneos, lo que reduce considerablemente los riesgos de liquidez y de crédito, por lo cual tiene mucho más potencial. Por otra parte, GPII puede parecerles a los bancos y las instituciones más segura, siendo un proyecto de SWIFT y basado en los acuerdos existentes entre los bancos correspondientes.

3.2. EVOLUCIÓN: HACIA EL USO DE SMART CONTRACTS

El potencial de los contratos inteligentes o smart contracts, los que se ejecutan automáticamente solo cuando las condiciones predefinidas se cumplen, ha sido objeto de mucho debate e interés en el sector de servicios financieros. Estos contratos inteligentes, cuyo funcionamiento está basado en la tecnología blockchain o registros distribuidos, se han pensado como una resolución para muchos de los problemas asociados con los contratos financieros tradicionales, que simplemente no están adaptados para la era digital. La dependencia de documentos físicos lleva a demoras, ineficiencias e incrementa la posibilidad de errores y fraude. Los intermediarios

financieros, a la vez que proporcionan interoperabilidad al sistema financiero y reducen el riesgo, crean costes adicionales y aumentan los requisitos de cumplimiento.

Existen beneficios inherentes para las entidades financieras y sus clientes en el uso de los contratos inteligentes, sobre todo para la banca de inversión, la banca minorista y el sector de los seguros.

1) **Banca de inversión:** En *trading* y liquidación de préstamos sindicados, los clientes corporativos podrían beneficiarse de ciclos de liquidación más cortos. En lugar de los actuales 20 días o más, los contratos inteligentes podrían llevar esto en el periodo entre 6 y 10 días, lo que podría llevar a un crecimiento adicional de entre el 5% y el 6% (con el crecimiento en la demanda en el futuro), lo que llevaría a ingresos adicionales de entre 2 mil millones y 7 mil millones de dólares anuales. Los bancos de inversión en Estados Unidos y Europa también tendrían menores costos operativos.
2) **Banca minorista:** Gracias al uso de contratos inteligentes, en operaciones como, por ejemplo, la solicitud de una hipoteca, se eliminarían los procesos tradicionales de tasación y documentación, lo que llevaría a la reducción de tiempo invertido en contactar con las entidades para verificar la situación del solicitante y los datos del inmueble. Todo eso supone una reducción significativa de costes de la operación.
3) **Seguros**: Tan solo en el segmento automovilístico, el potencial de ahorro para las aseguradoras es aproximadamente de 21 mil millones de dólares anuales, debido a la reducción de costes de tramitación. Además, la implantación de Smart contracts significaría una mayor agilidad administrativa y la reducción de contactos entre reclamantes y aseguradoras.

Hemos conceptualizado los Smart Contracts, su funcionamiento y sus ventajas e inconvenientes en el apartado 2.5.2, y en este punto vamos a centrarnos en el uso que podrían ofrecer al sector bancario y financiero.

3.3. USO DE SMART CONTRACTS EN EL SECTOR BANCARIO

Según la consultora Capgemini que, en su informe "Smart Contracts in Financial Services: Getting from Hype to Reality" (Cant et al., 2016), el consumidor medio podría ahorrarse aproximadamente entre 500 y 1000 dólares al año en concepto de comisiones bancarias gracias a los contratos inteligentes basados en las cadenas de bloques del blockchain. Desde el punto de vista del sector de banca minorista, el ahorro de costes para las entidades podría oscilar entre los 3000 y los 11000 millones al año.

Una de las características de los contratos inteligentes es que pueden reflejar cualquier tipo de lógica empresarial basada en los datos, desde la posibilidad de votar por una publicación en un foro hasta acciones más complejas como garantías de préstamos y contratos de futuros, e incluso los que suponen un nivel de complejidad más elevado aun, como la fijación de prioridades de pago en una nota estructurada (Fernández Espinosa, 2016).

A día de hoy, existen varias instituciones que están desarrollando plataformas que permitirán la implementación de la tecnología de registros distribuidos y contratos inteligentes, entre ellos la plataforma para crear aplicaciones en la blockchain y Smart contracts de Ethereum, o consorcios como Hyperledger, Corda o R3, de los cuales hablaremos en el capítulo 4.

3.3.1. Análisis de aportación a este sector

Vamos a nombrar algunos de los usos que se están en desarrollo y se pueden implementar en el sector de servicios financieros en el futuro próximo:

- **Información de los préstamos**

Tanto la información de las garantías de propiedad como los detalles de préstamos pueden ser almacenados en forma de un contrato inteligente en el registro distribuido de la cadena de bloques. De esa forma, en el caso de que el deudor no efectúe el pago acordado, el Smart contract tendría la posibilidad de revocar las claves digitales que permiten acceder a las garantías de forma automática.

- **Gestión de herencias**

Una de las características de un contrato inteligente es que puede consultar eventos que condicionan su ejecución, es decir, captar la información necesaria y después de su procesamiento adoptar una medida establecida. En el caso de herencias, la asignación de activos podría preestablecerse y ejecutarse en el caso de fallecimiento.

- **Configuración de depósitos en garantía**

Otra singularidad de los Smart contracts es que es posible su configuración como cuentas de depósito en garantía que permiten seguir el proceso de intercambio entre dos partes. Como ya hemos mencionado anteriormente, el contrato es capaz de adaptar las acciones en acuerdo con las condiciones preestablecidas, en este caso pues sería supervisar los servicios externos (a través de la localización del GPS, por ejemplo) y en el momento de que la propiedad se transfiriera del comerciante al cliente se liberarían los fondos a favor del primero.

- **Controles de carteras en criptodivisas**

Gracias a los contratos inteligentes sería posible incluir diferentes tipos de controles de los monederos electrónicos, por ejemplo, control de límites de reintegro diario o incluso tan complejos como permitir o restringir acceso a algunas entidades concretas. De esta forma, podrían convertirse en una especie de dinero programable, cuyo poseedor podría definir previamente mediante la programación prácticamente todo acerca del gasto: desde el tipo de activo que se quiere gastar, hasta la zona geográfica donde el gasto podría proceder o las fechas concretas.

- **Gestión de mercados de capitales**

Otra cosa que se podría escribir como un contrato inteligente serían los valores basados en pagos y derechos que se ejecutan de acuerdo con las reglas predefinidas. Ya en el año 2015 habían empezado pruebas y experimentos para emitir “bonos inteligentes” y gestionar mercados de valores privados. La función de los contratos es supervisar el rendimiento de activos tanto digitales como no digitales. Además, pueden ser utilizados como opciones, swaps, futuros o forwards.

No debemos olvidar que tanto la tecnología Blockchain, como los contratos inteligentes son tecnologías que todavía están en la fase de desarrollo. Aunque su potencial es enorme, todavía hace falta más tiempo y precedentes del uso para que obtengan la validez jurídica y la estandarización necesaria.

No obstante, están apareciendo cada vez más proyectos que intentan poner en práctica las ventajas que aporta la blockchain para mejorar el sector bancario y hacerlo más disponible para el cliente. Vamos a describir dos proyectos interesantes en esta dirección: Token Browser y TokenCard.

Token Browser es una aplicación privada y segura de mensajería instantánea que incluye una cartera Ethereum controlada únicamente por el usuario y el navegador. Hoy en día el mercado de micropagos digitales a través del smartphone está en auge, sobre todo en los mercados emergentes (por ejemplo, aplicaciones como WeChat en China, PayTM en India o MPESA en Kenia), ya que permite al usuario tener acceso a servicios financieros. El objetivo de Token es proporcionar este tipo de servicios, aunque el usuario no tenga una cuenta en un banco, y además hacer que las criptodivisas sean accesibles para cualquiera. Por otro lado, pretende que la moneda digital sea un instrumento de pago para bienes y servicios en vez de ser simplemente una inversión especulativa, como sucede a menudo a día de hoy. Es una aplicación de

código abierto y ahora está disponible su primera versión en tiendas de aplicaciones móviles App Store (iOS) y Google Play (Android).

TokenCard, aunque tiene un nombre similar al anterior, desarrolla un proyecto diferente. Es una plataforma de pagos con tarjeta de débito respaldada por un depósito de tokens de Ethereum. Cuando un usuario realiza una extracción de moneda fiduciaria o un pago en una tienda convencional, el sistema envía a un Smart contract la petición de pago, transacción que es aprobada y respaldada por Visa. El Smart contract automáticamente lanza una orden de venta a mercado de los tokens de la tarjeta para cubrir la liquidez de esta transacción, convirtiendo así los tokens en la divisa adecuada y siendo completamente transparente tanto para el cliente como para el establecimiento. Tiene tres elementos fundamentales: la cartera Token Contract, que protege los activos de los usuarios y hace cumplir los parámetros de seguridad y el gasto determinados por el usuario, la tarjeta física TokenCard, que conecta la cartera virtual con la red de Visa, permitiendo pagos en línea, transacciones o retiros en cajeros automáticos, y la aplicación Token App para móviles, que unifica todo el proceso, ofreciendo a los clientes tanto la experiencia de usuario más intuitiva, como el poder de no depender de los bancos dondequiera que estén. La posibilidad de unificar, por un lado, los contratos inteligentes de Ethereum y por otro los pagos Visa, en una tarjeta física y digital – es lo que hace TokenCard una propuesta realmente especial para la banca distribuida.

3.4. USO DE BLOCKCHAIN EN EL SECTOR DE LAS FINANZAS CORPORATIVAS

Los bancos y las instituciones han empezado a invertir masivamente en la tecnología Blockchain, aunque todavía muchas veces en forma de prueba para conocer el grado de integración de la nueva tecnología con la infraestructura existente desde los casos particulares del uso hasta su utilización a gran escala, en el caso empresarial. Los líderes del campo ahora tendrán que trabajar en el establecimiento de procedimientos necesarios que conecten los abundantes datos de la cadena de bloques con la empresa, permitiendo analizar la información de forma rápida y eficaz para poder tomar decisiones de manera informada y argumentada sobre las operaciones o las estrategias de la empresa.

No puede haber duda de que el proceso de adaptación e integración masiva es un largo camino que supone diversos desafíos, ya que desde el principio el sistema blockchain no estaba diseñado para el uso corporativo (sino para el usuario de la moneda virtual Bitcoin) y no estaba considerando todas las complejidades del sector empresarial. Para tener éxito en este campo y ser un instrumento de finanzas corporativas ampliamente usado por las entidades, debe haber un hincapié en la arquitectura y la integración de información, así como la seguridad y las políticas regulatorias.

Los departamentos financieros de las empresas deben plantear nuevas formas de su actividad profesional. Después de cientos de años sin cambios en procesos empresariales fundamentales, como contabilidad y auditoría, la implementación del sistema de registros distribuidos sería un cambio transcendental. El concepto de doble reserva, y luego la reconciliación y la auditoría se podrían convertir en contabilidad por partida triple, ya que la blockchain activa la tercera entrada (Hetherington & Schiebs, 2016). Aparte de su efecto en la contabilidad, la tecnología blockchain podría también cambiar la forma de la toma de decisiones dentro de la empresa y su dirección, e incluso en la forma de financiación.

3.4.1. Smart contracts: análisis de aportación a este sector

Los contratos inteligentes abren muchas posibilidades no solo para el sector jurídico, sino también para la gestión y control de las finanzas de la empresa. Vamos a analizar

las dos principales propuestas para esa innovación: la contabilidad de partida triple y la organización autónoma descentralizada.

1) Contabilidad de partida triple

En contabilidad la blockchain tiene gran potencial para mejorar la calidad de la información que reciben los inversores en dos formas: por un lado, haciéndola más confiable y, por otro lado, más oportuna. En cuanto a confianza, si las empresas pudieran almacenar sus registros financieros en la cadena de bloques, las oportunidades de hacer los trucos contables disminuirían drásticamente. Las transacciones entre empresas también serían mucho más transparentes. En cuando a tiempo, la contabilidad basada en la tecnología blockchain haría todas las transacciones de la empresa disponibles instantáneamente, sería posible actualizar la información en tiempo real (Byström, 2016). Finalmente, la aplicación de esta tecnología podría suponer la agilización de auditorías de registros, la optimización de relaciones entre la empresa y sus clientes, y aumentar de manera significativa la seguridad de los sistemas gracias al uso de la criptografía.

Otra de las ventajas que aporta la tecnología Blockchain a la contabilidad es el sistema distribuida de triple entrada (o de partida triple). La contabilidad de dobre entrada (o de partida doble) utilizada hoy en día se registra un asiento de deuda y uno de crédito a cada lado de la hoja de balance, mientras que en la de triple entrada aparte de esos dos asientos se registra un tercer asiento adicional en una cadena de bloques. Al registrarse en la blockchain se vuelve totalmente inmutable y transparente, lo que permite a los auditores u otras partes interesadas observar el estado de la empresa de forma mucho más fiable. Por ejemplo, un contrato inteligente para sistemas contables de triple entrada se está desarrollando por varias startups en el sector fintech, entre ellos Balanc3 (afiliados del estudio de producción ConsenSys), que utilizan el protocolo Ethereum.

2) DAO

Una DAO (por sus siglas en inglés “Descentralized Autonomus Organization”, organización autónoma descentralizada) es un tipo de organización que es posible gracias a la tecnología blockchain en general y los Smart contracts en concreto. Su diferencia de las empresas convencionales está en que una DAO tiene las reglas de gobierno automatizadas, formalizadas y que se hacen cumplir a través de un algoritmo informático. Básicamente, es un sofrware que permite que los poderes de decisión de la empresa tengan no solo los directores, sino toda la comunidad que posee tokens (una especie de acciones). La posesión de tokens permite participar en la votación o incluso introducir una propuesta para que el resto la vote. De esta forma, todas las decisiones que se toman están asegurados por la participación comunitaria en la votación.

A día de hoy existen dos conceptos de las organizaciones descentralizadas, aunque la idea fundamental es la misma: crear una organización automatizada para gestionar recursos sin el control human. La primera visión y la más extendida es la de Ethereum, y se trata del cumplimiento automático o semiautomático de contratos inteligentes. La segunda y menos conocida está realizada en Bitshare y supone delegación de función de organización al círculo limitado. Los accionistas de la empresa delegan su derecho a voto a los participantes más competentes, enviando los tokens a su favor.

El formato DAO es válido para gestión de activos de cualquier empresa o comunidad, sobre todo si se trata de los intangibles, por ejemplo, la venta de contenido digital. La gran ventaja que ofrece DAO es la eliminación del factor humano y la necesidad de confiar. En el paradigma existente de relaciones contractuales no existe una garantía o forma segura de prevenir errores por culpa del descuido o incluso por mala fe del registrador. Pues todo eso se podría solucionar implementando la forma descentralizada de gestión y dirección de la empresa o institución.

Esencialmente, una DAO es una asociación de inversores que votan las decisiones de inversión, cuyos estatutos están incorporados y cuyas funciones administrativas están garantizadas por to contratos inteligentes. Además, sus relaciones con las inversiones (las propuestas) también están incorporados en los contratos inteligentes. En teoría, los socios de la DAO podrían votar para invertir en un proyecto a cambio de una rentabilidad fija (como una inversión de capital de riesgo), o para financiar un proyecto que luego se convierte en parte de la propia organización DAO (como una división de un conglomerado), o para pagar en efectivo por servicios externos (como contratar a un programador para escribir contratos inteligentes), o simplemente donar dinero a un proyecto benéfico o hacer cualquier otra cosa que puede estar codificado en un contrato inteligente. Al igual que una sociedad colectiva puede hacer una inversión, iniciar un negocio, pagar por los servicios o donar caridad (Levine, 2016).

Sin embargo, esta forma de organización no se utiliza ni se encuentra a menudo, por dos principales razones. En primer lugar, para que el sistema funcione, el código fuente debe estar escrito de manera impecable, y por desgracia muchas veces no es así. Y los errores pueden llevar a graves consecuencias – como al que pasó con "The DAO Project", un fondo de capital de riesgo abierto, el primer proyecto de organización descentralizada realizado con tecnología de contratos inteligentes y Ethereum, cuando un hacker logró robar 3.6 millones de Ethers (valorados en 50 millones de dólares en el momento del ataque) de un total de 11.5 millones de Ethers recaudados por inversores en todo el mundo. En segundo lugar, aunque la tecnología y la idea de DAO se encuentran muy avanzadas, a día de hoy el sistema legislativo está obsoleto y mientras no sea adaptado a esta nueva realidad continuará impidiendo la validez legal de cualquier DAO, aunque no su ejecución.

A pesar de todo, siguen apareciendo nuevas formas de aplicar la idea de DAO en el mundo empresarial. Una de estas propuestas la está llevando a cabo una fintech startup española con nombre Aragon. El proyecto de Aragon se define como "plataforma de dirección descentralizada" para las empresas, es decir, pretende cubrir todas las necesidades en la administración de empresa, como contabilidad, estatutos, la cap table (tabla de capitalización), gobernanza, recaudación de fondos y las nóminas de sueldos mediante una interfaz unificada. Las organizaciones de la red de Aragon van a ser construidas utilizando una DAO y aplicaciones descentralizadas basadas en la web (dApp). Todo esto les va a permitir responder a la demanda de cambio de los mecanismos establecidos de dirección de empresas, ya que con la aparición de internet en general y programación en la nube en particular en muchos casos la forma de administrar y gestionar empresas también requiere un cambio. Una de las innovaciones propuestas por Aragon es la de las votaciones líquidas – los poseedores de token de pueden pasar su derecho de voto a través de contratos inteligentes a otros, lo que haría el proceso de votación mucho más flexible, transparente y rápido. Las empresas que podrían ser adaptadores tempranos de la tecnología que ofrece Aragon son proyectos tecnológicos distribuidos de código abierto. Ahora mismo el proyecto está en etapa de pre-lanzamiento, y a partir de mayo empieza su ICO.

3) ICO: nueva forma de financiación

Otro ámbito empresarial que está transformándose gracias a la tecnología blockchain es el de la financiación de empresas. ICO (por sus siglas en inglés Initial Coin Offering) u Oferta inicial de moneda es una nueva forma para recaudar fondos y financiar el desarrollo de nuevos protocolos. En vez de intercambiar dólares por acciones de la empresa, como en una IPO (Oferta Pública Inicial), el ICO se trata del intercambio de dinero fíat o criptomonedas existentes como Bitcoin o Ether por la nueva moneda digital ofrecida por la startup, cuya funcionalidad está entre participación en la empresa y moneda como tal. Para los usuarios es una forma de comprar criptomoneda del nuevo proyecto a precio de mercado antes de que entren en circulación y posiblemente crezcan, mientras que para una startup es una manera de obtener un respaldo monetario que les da mayor incentivo y responsabilidad de seguir llevando a

cabo su propuesta tecnológica. Por otro lado, la forma de financiación ICO cada vez toma mayor importancia dentro del ecosistema, dado que sirve como medidor de confianza y las expectativas de los usuarios sobre el proyecto.

Además, este instrumento aporta valor a los inversores de riesgo, cuyo trabajo depende de tomar grandes riesgos en fase inicial a cambio de recompensas cuando una empresa se hace pública. En cuanto al dinero acumulado, los últimos ICO no están muy lejos de las inversiones medias de la ronda de financiación B, recaudando entre 5 y 15 millones de dólares, según el informe de Smith + Crown.

Figura 12. Los ICO más recientes, según los datos de Smith + Crown

Fuente: https://www.bloomberg.com/gadfly/articles/2017-04-18/beating-vc-funds-is-as-easy-as-flipping-a-bitcoin

Las ICO también las comparan con las campañas de crowdfunding (financiación colectiva), pero la gran diferencia está en que en el caso de ICO, los inversores buscan retorno a sus inversiones, mientras que crowdfunding es una forma de micro mecenazgo y las aportaciones que se hacen se parecen más a donaciones. Por otro lado, en el caso de ICO existen grandes posibilidades de especulación, por ejemplo, el fenómeno de mercados financieros conocido como “Pump and Dump” (“inflar y tirar”): la demanda de usuarios se acumula, lo que hace que el precio tiende a subir con rapidez e infla el valor de la criptomoneda, pero a la hora de lanzarla al mercado el precio puede decaer de forma radical, por la venta rápida de grandes cantidades monetarias. Para evitar que se produzca este tipo de especulación, los expertos recomiendan estudiar la base tecnológica de la startup en el que se planea invertir y el equipo que lo forma, como si se tratase de una inversión tradicional de capital de riesgo.

Entre las ICO más conocidas, podríamos destacar la de Ethereum y la de TheDAO. Ethereum fue el primer proyecto que tuvo un gran éxito en este campo en el verano de 2014. Han podido recaudar 31,5 mil Bitcoin, que en aquel momento equivalían a 15 millones de dólares (con el precio de 40 céntimos de dólar por un Ether). Ahora Ethereum es la segunda criptodivisa con la mayor capitalización del mercado, y el valor de 1 moneda Ether ronda unos 50 dólares. La revalorización del Ether sólo en los primeros seis meses del 2016 ha sido del 2000%, ya la tendencia sigue siendo alcista (Preukschat, 2017).

La campaña de TheDAO, que es un proyecto basado en Ethereum, ha podido recaudar más de 150 millones de dólares en verano de 2016, sin embargo, no ha tenido éxito por el ataque de un hacker que ha podido bloquear una parte de fondos recaudados. Aunque el problema fue un error humano y ha sido resuelto en semanas, la confianza ha sido socavada. No obstante, este error ha ayudado a aprender de los fallos cometidos mejorando enormemente la seguridad, así como a instaurar

protocolos de actuación en caso de error o ataque (como, por ejemplo, un sistema de emergencia que bloquee los fondos y los transfiera en caso de ataque).

A pesar de la posible especulación, la forma de financiación de un proyecto a través de la emisión de su propia moneda virtual dentro del ecosistema Blockchain es un paso interesante en el proceso de transformación digital de la economía global. En su libro "Business Blockchain" el inversor de riesgo Willian Mougayar propone un análisis comparativo de las similitudes y diferencias entre la inversión con enfoque tradicional y con enfoque descentralizado – ICO (Mougayar, 2016b).

		Capital de riesgo tradicional	Inversión a través de criptodivisas
1	**La duración de la inversión**	7-10 años	1-5 años
2	**Forma de posesión**	Acciones preferentes	Acciones, criptotoken y/o cripromoneda
3	**Fase de entrada**	Ronda de capital de riesgo (Business angels), capital semilla, ronda de inversión temprana o avanzada	Pre-mine (antes del comienzo del proceso de minado), Genesis (lanzamiento de la blockchain), ICO, compra de tokens en el mercado o de los fundadores
4	**Forma de salida**	IPO, M&A (Mergers and Acquisitions, fusions y acquisitions)	IPO, M&A y salida a la bolsa de criptodivisas
5	**Modelo de negocio**	Venta de servicios o de productos	Construcción de una economía cerrada asociada a los criptotokens del proyecto
6	**Forma jurídica**	Sociedad anónima en la jurisdicción seleccionada	Organización autónoma descentralizada, en general no registrada y sin ánimo de lucro, y sociedad anónima que vende servicios y productos relacionados con la blockchain
7	**Fuente de los fondos**	Inversores privados, fondos institucionales o familiares, organizaciones financieras	Crowdfunding (financiación colaborativa), fondos de inversión e inversores privados, futuros usuarios y clientes
8	**Divisa de la inversión**	Fiat (dólar, euro, yuan etc.)	Fiat y criptodivisas. Por lo general, para el importe total de la ronda se suele utilizar BTC.
9	**Criterios de la selección del mercado**	Modelos de negocio nuevos o tradicionales comprobados	Creación de nuevos modelos de negocio

Tabla 2. Comparación de características de la inversión de riesgo tradicional y las ICO

Fuente: Elaboración propia, datos de William Mougayar

Como podemos observar, las diferencias son significativas, pero el principal problema está el carácter especulativo de las inversiones. Sin embargo, en el primer trimestre del 2017 el panorama de la financiación ICO ha comenzado a cambiar. Por ejemplo, el fondo estadounidense de capital de riesgo “Blockchain Capital” anunció su intención de recaudar 10 millones de dólares para su nuevo fondo. Ha sido el primer ejemplo de IPO que no ha sido lanzado por una nueva startup, sino por un negocio existente, exitoso, rentable y con auditorias transparentes de anteriores resultados financieros. Como resultado, ha logrado recaudar los 10 millones necesarios en tan solo 6 horas, que es un tiempo récord (Kastelein, 2017).

Al final, el objetivo de ICO es la democratización del mercado del capital público, que, por un lado, se vuelve disponible a todos los negocios y, por otro lado, permite a los inversores obtener los token de la empresa directamente, sin necesidad de intermediarios como brokers, fondos o bolsas. Es muy probable que el volumen de inversiones en las ICO siga subiendo en un futuro, pero probablemente su calidad también se eleve. Muchos de los inversores están esperando la venta de tokens de proyectos de calidad, con modelos de negocio innovadoras, así como la aparición de instrumentos para la evaluación de riesgos de inversión.

CAPÍTULO 4. CASOS DE USO, REGULACIÓN Y LIMITACIONES

En el año 2016, aunque la incertidumbre en los mercados financieros crecía por razones políticas y económicas globales, las inversiones en el sector fintech no han parado de subir. Según el informe "The pulse of fintech Q4 2016" preparado por la consultora KPMG, la inversión de capital de riesgo en el sector creció un 7 por ciento, por un total de 13,6 millones de dólares, mientras que la inversión total en fintech alcanzó 24,7 mil millones, gracias a la tecnología y el éxito de las empresas centradas en proporcionar una experiencia excepcional al usuario (Fortnum, Mead, Pollari, Hughes, & Speier, 2017). Las predicciones para el año 2017 son aún más impresionantes, aunque esta vez la atención se centra en la cooperación. Los bancos tradicionales, instituciones financieras y las aseguradoras reconocen la importancia de ser más eficientes y enfocados en el cliente. Muchos de ellos también admiten la necesidad de colaborar con las startups tecnológicas para aumentar su capacidad.

En cuanto a la inversión en la tecnología Blockchain, después del fuerte interés durante todo el año 2016 por parte de los inversores, ha habido un cambio de enfoque, sobre todo por parte de los inversores corporativos. En concreto, el cambio de la inversión directa en los proveedores de la blockchain a la inversión en proyectos basados en esa solución. Ahora muchas miradas y muchas expectativas están puestas en esta tecnología, y los inversores necesitan ver que la blockchain es capaz de evolucionar desde los escenarios de prueba a soluciones reales que puedan ser comercializadas, escaladas y rentabilizadas.

El impacto que puede tener la tecnología blockchain en el sector bancario es realmente importante. Por ejemplo, el Banco Santander ha calculado que la utilización de esta tecnología disruptiva podría suponer para el año 2020 un ahorro de 20 mil millones de dólares para el sector bancario. Al mismo tiempo, el banco francés BNP Paribas incluso ha comparado el invento de esta tecnología con la aparición de la máquina de vapor o el motor de combustión por el impacto a la sociedad y economía que podría suponer (Fernández, 2016).

Se espera que en el año 2017 las inversiones en la tecnología blockchain sigan, aunque potencialmente con el "burn rate" (flujo de caja negativo) menor que anteriormente, ya que se espera que la blockchain logre entregar el valor percibido. También es posible que las inversiones impulsen avances en ámbitos de desarrollo de estándares consistentes para que sea utilizado en el manejo de esta tecnología a través de organizaciones y jurisdicciones.

A día de hoy en el mundo empresarial existen tres tipos de enfoques aprovechar el potencial de la tecnología blockchain. En primer lugar, la colaboración con las startups que ya investigan en este sector. En segundo lugar, la creación de un equipo propio de desarrolladores dentro de la organización. Y la tercera opción sería unirse a uno de los consorcios existentes.

En este capítulo analizaremos algunos casos de implementaciones de esta tecnología en instituciones financieras reales alrededor del mundo, las limitaciones de la tecnología blockchain y la situación de su regulación en diferentes países.

4.1. ASOCIACIONES Y CONSORCIOS

Las empresas e instituciones que quieren investigar la tecnología Blockchain optan cada vez más por hacerlo de forma conjunta a través de un consorcio. De esa manera, las startups disruptivas tienen una posibilidad de poner a prueba sus plataformas en el escenario real con corporaciones y empresas a gran escala, como grupos bancarios u otras empresas del sector financiero.

En su informe anual, una de las mayores compañías de servicios profesionales y consultoría Deloitte afirma la necesidad de crear consorcios entre bancos y otras instituciones financieras con el fin de favorecer la implementación y la comercialización de la tecnología blockchain. Su directivo Eric Piscini ha declarado en una entrevista que los consorcios y asociaciones del sector pueden ser un elemento fundamental para descubrir el valor de la tecnología blockchain a gran escala para que siga siendo relevante en los próximos años (Meijer, 2017).

A día de hoy existen más de 100 consorcios y colaboraciones en el sector blockchain (de los que al menos 25 son a nivel internacional), y el número sigue creciendo no solo a escala global, sino también en algunas regiones particulares. Han aparecido consocios en Canadá (Proyecto Jasper), Rusia (Consorcio Bancario Ruso de la Blockchain, julio del 2016), China (China Ledger Aliance, abril del 2016 y Consorcio de Blockchain financiero Chenzen, mayo 2016) y Japón (Consorcio Bancario Japonés Ripple, agosto 2016). También surgen colaboraciones basados en la investigación de la blockchain en otros sectores, como seguros o atención médica. Sin embargo, la mayoría de consorcios se encuentra en la industria financiera. Los más conocidos son R3CEV, the Hyperledger Project, Entreprise Ethereum Aliance y the Post Trade Distributed Ledger Group (PTDL).

En definitiva, la blockchain ya no es percibida por los bancos como una amenaza, sino como una herramienta de mejora, modernización y digitalización.

4.1.1. R3

R3 (o R3CEV LLC) es una empresa que desarrolla la tecnología de registro distribuido. Esta organización domina el consorcio en el que entran más de 70 de las instituciones financieras más grandes del mundo, con el fin de investigar y desarrollar formas de utilización del registro distribuido blockchain en el sistema financiero. Lo que más les interesa a los bancos es la optimización de los procesos a través de la utilización de las blockchain privadas, sistemas restringidos en los que solo pueden participar los que forman parte del consorcio.

El consorcio fue fundado en 2015 por nueve grandes organizaciones financieras: Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland y UBS. Desde su creación hasta 2017, el consorcio ha invertido unos 59 millones de dólares solamente en investigaciones en el campo de registros distribuidos. Sin embargo, en enero del 2017 R3CEV ha anunciado que está esperando otra inversión de 150 millones de dólares.

Entre los proyectos llamativos que ha realizado el consorcio destacan, por ejemplo, los experimentos para confirmar la hipótesis que la tecnología blockchain podría hacer las transacciones bancarias más rápidas y seguras. Las pruebas fueron llevadas a cabo en 2016 gracias al registro descentralizado P2P, creado a base de la plataforma Ethereum y disponible en la nube Microsoft Azure que ofrece soluciones BaaS (por sus siglas en inglés “Blockchain as a Service” o blockchain como servicio). Las operaciones financieras han sido realizadas entre los bancos participantes simultáneamente dentro de la blockchain privada. El intercambio de datos era directo en unidades del registro (tokens), sin necesidad de un intermediario centralizado. En este experimento participaron 11 de los 42 miembros del consorcio en aquel momento, entre ellos Barclays, Credit Suisse, HSBC y Wells Fargo (McDonald, 2016).

Otro ejemplo de la actividad del consorcio es la creación de la plataforma de registro distribuido para los bancos con nombre Corda. Esta plataforma de código abierto ha surgido como una forma de crear estándares del sector para la nueva tecnología y está pensada para el manejo de datos de transacciones e incluso complejos contratos inteligentes. Siendo desarrollada principalmente para el sector financiero y diseñada para los bancos, la plataforma permite procesar los pagos o de valores y derivados.

Algunas de las principales características de la plataforma Corda son los siguientes:

- El acceso a los datos de la operación solo estará disponible a las partes con necesidades legitimas de tener el acceso a ellos, es decir, que la difusión global de datos solo se realiza hasta el punto necesario para su procesamiento.
- La plataforma está basada en herramientas estándar de la industria, y es compatible con varios mecanismos de consenso.
- Es descentralizada y coordina el flujo de trabajo entre las empresas sin la necesidad de un intermediario o controlador central.
- El consenso que se logra es entre empresas y a nivel de acuerdos individuales, no a nivel del sistema.
- Las funciones de supervisión y regulación son cumplidas por los nodos directamente gracias al diseño de la plataforma.
- No posee una criptomoneda propia, ya que en el contexto para el que está pensada no existe esa necesidad.
- Es capaz de registrar la relación explícita entre los documentos jurídicos en el formato al que estamos acostumbrados y el código de Smart contract o contrato inteligente.

Básicamente, podemos ver que, aunque algunas de sus características se asemejan con las de tecnología blockchain tanto en la función como en la infraestructura del registro distribuido, mucho apunta a que las diferencias son mayores. Finalmente, a principios del año 2017 los directivos de las empresas que forman parte de R3 han afirmado que Corda “no es una blockchain”, sino un proyecto independiente inspirado en ella, pero construido desde cero con la intención de cumplir las necesidades de los negocios financieros actuales (Rutter, 2017). La blockchain, según R3, no puede ser aplicada ciegamente a los mercados financieros sin considerar la aplicación de ciertos cambios necesarios para cumplir las normas de protección de datos, las cuestiones reglamentarias y solucionar problemas de escalabilidad. Por otro lado, en comparación con la blockchain de Bitcoin, por ejemplo, donde toda la historia de todas las transacciones está distribuida entre todos los nodos, Corda solo permite compartir las operaciones revisadas, y rechaza la idea de que los datos tienen que estar copiados para todos los participantes, aunque estén encriptados.

La prueba de concepto más reciente de R3 fue para los préstamos sindicados. A través de la combinación de tecnología de contratos inteligentes y los procesos de negocios, el sistema es capaz de ofrecer a los inversores acceso directo a un sistema de registro de datos de préstamos sindicados. Eso genera ahorros inmediatos ya que reduce las revisiones manuales, la reentrada de datos y la reconciliación de sistemas.

A pesar de los éxitos conseguidos en la implementación de sistemas blockchain o inspirados en la blockchain por las asociaciones de empresas, existen ciertas dudas acerca de la necesidad de los consorcios grandes. En concreto, los expertos opinan que el modelo demuestra varias limitaciones. A finales del año 2016, algunos de los grandes bancos incluido Goldman Sachs entre otros han anunciado que van a dejar el consorcio R3CEV después de que la organización “no haya podido proveer ningún tipo de implementación comercial de la tecnología”. En abril del 2017 otra de las organizaciones fundadoras del consorcio R3, J.P. Morgan Chase, ha anunciado su salida definitiva. Después de este acontecimiento es difícil predecir el futuro de este consorcio, ya que, por un lado, nadie descarta la posibilidad de salida de consorcio de otros miembros, pero, por otro lado, después de lanzamiento de Corda se espera la aparición de otros productos comerciales.

La salida de los jugadores clave de R3CEV y la reorganización del sistema de socios de este tipo de consorcios ha provocado una ola de otras empresas que salen de los consorcios grandes y dedican su esfuerzo a crear mini-consorcios con 2 o 3 bancos u otro tipo de intermediarios. Según estas empresas, es importante en primer lugar crear un “ecosistema mínimo viable” con un pequeño subconjunto de actores clave en

principio. Es muy probable que si las asociaciones más sectoriales se centraran en las pruebas de concepto puedieran alcanzar la producción a corto plazo y resolver de esta manera necesidades concretas.

4.1.2. Hyperledger Project

Otro proyecto en esta área es Hyperledger, que fue iniciado en diciembre de 2015 por la Fundación Linux, y a principio de 2016 ya ha empezado a desarrollar las primeras propuestas. Es un proyecto de código abierto que tiene como objetivo avanzar en el uso de la tecnología blockchain en distintos sectores. Es una colaboración global que incluye líderes en las áreas como finanzas, banca, IoT (por sus siglas en inglés "Internet of Things" o internet de las cosas), cadena de suministro, producción y tecnología. El objetivo principal de esta colaboración es desarrollo de una variedad de blockchains con diferentes modelos de consenso, almacenamiento de datos, gestión de acceso y servicios de identificación, y su consiguiente salida a mercado.

Entre los participantes del proyecto Hyperledger están tanto las organizaciones especializadas en la protección de la propiedad intelectual, medios de comunicación, empresas informáticas, como las compañías especializadas en las soluciones blockchain que se dedican a la creación y el intercambio de criptodivisas. La lista de los miembros incluye más de 122 organizaciones, entre ellos tan conocidos como J.P. Morgan, Intel, CISCO, Panasonic, SAP, Thompson Reuters, Accenture, SWIFT o IBM.

Como ejemplo de los proyectos que están llevando a cabo ahora mismo en Hyperledger está Sawtooth Lake, una plataforma para creación y explotación de registros distribuidos y contratos inteligentes. Las aplicaciones de esta plataforma pueden ser muy amplias, desde la liquidación de bonos y activos en el sector financiero hasta la trazabilidad de la cadena de suministro de pescado y marisco. Otro ejemplo es Hyperledger Fabric – un sistema operativo para IBM Blockchain, que tiene mayor funcionalidad para la creación de aplicaciones comerciales basadas en la tecnología de cadena de bloques y es capaz de procesar más de mil transacciones por segundo.

4.1.3. R3 y Hyperledger: colaboración o competencia

A pesar de que ambos proyectos se desarrollan en la misma área y con la utilización de la misma tecnología, su enfoque es diferente.

El consorcio R3 expresa intereses de grandes capitales, es mucho más cerrado y enfocado en el desarrollo en el mundo de las finanzas. Fundamentalmente, los grupos del consorcio están trabajando en los objetivos concretos, y para la solución de los problemas relacionados no les importa menoscabar los principios en las que se basaba la idea de la blockchain desde sus comienzos, ya que su principal objetivo es conseguir rapidez, seguridad y la gestión adecuada de los flujos de transacciones financieras. Además, la fundación de R3 fue un primer intento de las organizaciones en reunirse para investigar juntos las oportunidades que brinda la tecnología blockchain. Este consorcio no está liderado por un banco en concreto, mientras que las instituciones interbancarias suelen desarrollarse con una intervención activa de un banco-líder.

Mientras Hyperledger está formado principalmente por las empresas del sector tecnológico. Es más abierto e incluye la variedad de pequeños startups. Como tarea prioritaria se declara la estandarización tecnológica y el desarrollo de la solución universal que puede servir de base a una amplia gama de productos. Este proyecto intenta abordar un mayor alcance de aplicación de la tecnología blockchain que incluye, entre otros, IoT.

Todavía es pronto para hablar de una competencia entre estos dos proyectos, además que muchas de las empresas han decidido formar parte de los dos consorcios a la vez. No obstante, las ambiciones del R3 que ha lanzado la plataforma Corda, que compite

claramente con las “blockchain tradicionales”, y entre ellos con Sawtooth Lake de Hyperledger, en su aplicación a finanzas, pueden permitir que la competencia entre estos dos consorcios sea posible. Sobre todo, si esos dos conglomerados no se pongan de acuerdo en su cooperación y el desarrollo de los estándares comunes, o por lo menos dividan esferas de influencia.

4.2. Ethereum Enterprise Alliance (EEA)

Ethereum Enterprise Alliance o alianza empresarial Ethereum es un consorcio fundado a principios de 2017 por un grupo de startups, empresas innovadoras y entidades financieras interesadas en la tecnología blockchain para, por un lado, desarrollar y, por otro lado, promocionar y apoyar los nuevos proyectos a base de Ethereum. Las empresas que entraron en esta nueva alianza son, entre otros, Intel, J.P. Morgan, Microsoft, ConsenSys y Banco Santander. Además, han creado su propia infraestructura con nombre EntEth 1.0.

Ethereum es una blockchain pública, lo que supone que puede ser utilizada por cualquiera. Para algunas de las aplicaciones es una ventaja muy grande, pero en el caso de otras puede suponer incluso un inconveniente. Por eso, las instituciones financieras y los negocios a gran escala copian el código fuente de la blockchain Ethereum para lanzar sus propias iniciativas en vez de utilizar el código inicial. Aun así, Ethereum es una solución muy prometedora en el mundo de soluciones empresariales en la blockchain, y uno de los objetivos de EEA es mejorarlo para que sea más adecuado para los estándares bancarios y útil para varias industrias. Eso supone evitar protocolos aislados y un entendimiento que no sea colectivo. Por otra parte, el propósito del consorcio no es entrar en el ámbito de la blockchain privadas, ni crear una criptomoneda, sino aprovechar la plataforma que ya existe para potenciar la gestión de pagos.

Siendo un consorcio recién creado, todavía no ha lanzado propuestas concretas de su utilización, sin embargo, después de la noticia sobre su creación el precio de Ether (moneda digital de Ethereum) ha subido desde 13,5 dólares (precio al 25.02.17 según coingecko.com) hasta el máximo histórico de 73 dólares el 28.04.17, en otras palabras, el valor de la criptodivisa se ha incremento un 441%.

4.3. Otros tipos de colaboraciones

Aparte de organizar un consorcio formal, existen otras formas de colaboración y alianzas entre las instituciones financieras y las empresas que promueven la utilización de la blockchain. Dos ejemplos muy claros de estas colaboraciones son casos de Digital Asset Holdings y Ripple.

4.3.1. Digital Asset Holdings

Digital Asset Holdings (DAH) es una empresa de software que desarrolla las soluciones para el sector financiero basadas en la blockchain. Su software vincula la lógica empresarial y los procesos jurídicos con las firmas (signaturas) criptográficas, y permite la fijación de las transacciones en los registros distribuidos públicos o privados dependiendo de los requisitos concretos en cada caso.

Aunque en este caso no estamos hablando de un consorcio tradicional, entre los patrocinadores de DAH están las compañías como Goldman Sachs, J.P. Morgan, BNP Paribas, IBM, Deutsche Borse entre otros. En la primera ronda de inversión, han conseguido recadar unos 7,2 millones de dólares, y en la segunda 60 millones de dólares, pero la principal función de DAH fue la adquisición de proyectos existentes en la blockchain. En el año 2016 han adquirido Elevance Digital Finance, anteriormente compraron también startups como Blockstack.io y Bits of Proof.

Aunque la propuesta principal de la empresa es utilizando la tecnología blockchain disminuir el tiempo de operaciones de compensación y liquidación, a día de hoy el fundamento de su tecnología es una recopilación de soluciones conseguidos a través de absorción de pequeñas startups, por lo que es, obviamente, criticada, y lo que le causó ciertas dificultades a la hora de buscar financiación, según el periódico "The New York Times" (Popper, 2015).

4.3.2. Ripple

Ya hemos analizado la propuesta y la tecnología que ofrece Ripple en el capítulo anterior, pues esta empresa también se diferencia por la forma de colaborar con otras organizaciones. En el caso de Ripple, se crean conglomerados regionales, como por ejemplo el conglomerado RC Cloud de los bancos japoneses con 56 bancos participantes (representan casi un 40% de todos los bancos en Japón), que llevaron a cabo dos pruebas de la tecnología Ripple en transacciones interbancarias. En este caso fue SBI Ripple Asia (la empresa conjunta con una firma de servicios financieros basada en Tokio SBI Holdings) quien participó por parte de Ripple. Según los datos de SBI, el 60% de SBI Ripple Asia pertenece a los bancos, y el 40% de Ripple (Rizzo, 2017).

Aparte, en la lista de los inversores de Ripple podemos ver Banco Santander, Accenture, Google Ventures y Andreessen Horowitz entre otros, pero el número de los bancos con los que trabaja en diferentes fases Ripple llega a más de 90. El BBVA, por ejemplo, ha realizado pruebas con la tecnología Ripple, las infraestructuras de BBVA y el dinero fiduciario para hacer un pago entre España y México que tardó tan solo segundos en ser realizado (Robinson, 2017). Con la tecnología que se utiliza a día de hoy, esa misma transferencia tarda 4 días en procesarse. El siguiente paso por parte de BBVA sería ofrecer probar esta tecnología a un grupo seleccionado de sus clientes durante 2 semanas, y en función de resultados tomar la decisión final acerca de la implementación. Este tipo de experiencias de pruebas exitosas pueden abrir puertas a más colaboraciones de los bancos con las empresas que utilizan la blockchain.

4.3.3. Similitudes y diferencias entre los consorcios

Vamos a comparar los cuatro consorcios analizados para definir lo que tienen en común y en qué se diferencian entre sí.

Criterio	R3CEV	Hyperledger	Digital Assets Holdings	Ripple
Sistema de afiliación	Afiliación simple	Tres niveles: miembros premier, miembros ordinarios y miembros asociados	Venta de software a los bancos, organizaciones de compensación y liquidación entre otros	Conglomerados regionales, por ejemplo, RC Cloud en Japón
Las cuotas	Una tarifa fija por servicio de consultoría	250 mil dólares para los miembros premier, 5-50 mil para los miembros ordenarios y gratis para los asociados	Se determina en cada caso particular	Se determina en cada caso particular

Criterio	R3CEV	Hyperledger	Digital Assets Holdings	Ripple
Ámbitos principales del trabajo	Operaciones y acuerdos financieros tradicionales	Blockchain con propósitos generales	Mercados de capitales, asentamientos posteriores a la negociación (post-trading)	Las transacciones (principalmente interbancarias y/o internacionales)
Productos clave	Corda – un registro distribuido para la fijación y gestión de acuerdos financieros	Tres estructuras: IBM-Fabric, Soramitsu-Iroha y Intel-Sawtooth Lake	Plataforma de activos digitales que utiliza la tecnología de registro distribuido para el intercambio sincronizado de datos de mercados y procesos financieros entre miembros particulares	Integración de los servicios para los pagos corporativos y transferencias aisladas
Inversiones	Los miembros que financian el proyecto reciben una parte en una empresa subsidiaria que controla Corda	Un proyecto colectivo de código abierto financiado a través de las cuotas de los miembros	Patrocinado por J.P. Morgan, Goldman Sach, Deutsche Borse, ABN, AMOR, IBM, BNP Paribas entre otros	Patrocinado por Santander Innoventures, Standard Chartered Bank, Accenture, Digital Currency Group entre otros

Tabla 3. Similitudes y diferencias entre los consorcios R3CEV, Hyperledger, Digital Assets Holding y Ripple

Fuente: Elaboración propia

En la Tabla 3 podemos observar que, en cuanto a formas de afiliación, los consorcios más grandes como R3 o Hyperledger suelen utilizar el sistema de membresía más transparente, para unirse al consorcio las organizaciones pagan una cuota en función de privilegios que desean recibir como parte del consorcio. En el caso de Hyperledger el precio de la afiliación Premium puede llegar a unos 250 mil dólares. En el caso de consorcios más pequeños, la cuota se define individualmente, ya que es el precio de las soluciones que ofrecen las empresas principales. Los productos ofrecidos por los consorcios se diferencian en función de la parte de mercado al que van dirigidos, mientras que los miembros a menudo se repiten en distintas asociaciones. Por ejemplo, el banco BBVA a la vez está en el consorcio Hyperledger, además de ser socio fundador de R3 y Enterprise Ethereum Alliance, mientras que hace pruebas con la tecnología Ripple en transacciones internacionales. Los J.P. Morgan y Goldman Sachs también repiten de consorcios, así que es una situación más bien común que solamente demuestra el interés de las instituciones por la implementación de la tecnología blockchain, sea cual sea el consorcio que lo consiga primero.

Las previsiones acerca del futuro de los consorcios son diversas. Hay expertos que opinan que van a seguir creciendo como forma de colaboración entre bancos y empresas de la forma en que colaboran hoy en día, mientras que otros defienden la idea de que van a aparecer distintas formas de asociaciones. En primer lugar, son consorcios de los Bancos Centrales, por ejemplo, lo que podemos ver en Gran Bretaña con el proyecto de Banco de Inglaterra. Es evidente que los reguladores

financieros van a tener que implementar la nueva tecnología financiera de forma centralizada, desde arriba. Asimismo, la banca comercial va a tener que aceptar e integrar esas soluciones.

4.4. PRUEBAS EN LOS BANCOS (BBVA, Santander, JP Morgan, Banco Sabadell)

En este apartado, vamos a analizar otras iniciativas particulares de los bancos y organizaciones financieras y las pruebas ya realizadas no en forma de consorcio, sino por vías propias. Generalmente, se trata de actividades como creación de monedas virtuales propias, innovaciones en mercados de valores y capitales privados o mejoras en transacciones interbancarias e internacionales, entre otras.

Una amplia variedad de instituciones financieras ya ha puesto en marcha esfuerzos para explorar el potencial de las oportunidades que blockchain puede ofrecer a su negocio. Algunos como USAA Bank y BBVA han invertido millones de dólares en proveedores de servicios Bitcoin como Coinbase y Circle para estudiar aplicaciones en la blockchain. Otros, como Barclays y Sabadell, han creado aceleradoras o han patrocinado hackatones (encuentros de programadores informáticos con el objetivo de desarrollo colaborativo de software) para proporcionar espacio para los startups y también para aprender de ellos. Otros, como Citi o Nasdaq, todavía están en la fase de pruebas beta de los sistemas construidas sobre la base de tecnología blockchain y analizar posibles enfoques prácticos. Goldman Sachs, aparte de participar en varios consorcios y financiar distintas startups del sector, a finales del 2015 también ha presentado una solicitud de patente para un sistema de liquidación de valores con criptomonedas basado en una nueva criptomoneda llamada SETLcoin.

La segunda bolsa de valores electrónica y automatizada más grande de los Estados Unidos Nasdaq se ha unido a la transformación blockchain con el lanzamiento de una plataforma Nasdaq Linq que soluciona el problema de manejo manual y en papel de certificados de acciones, concesión de opciones y notas convertibles rápidamente que se desactualizan. Nasdaq Linq pretende establecer este proceso en el registro distribuido digital para permitir una gestión más eficiente y segura de esta actividad. Es un producto orientado a los empresarios e inversores de capital de riesgo con una interfaz intuitiva y sencilla, y está formada en parte por la plataforma Nasdaq Private Market, que básicamente es un paquete de servicios financieros que ha servido a Nasdaq para salir al mercado secundario de compraventa de acciones de las empresas que todavía no han tenido un IPO. A través de Linq se puede consultar el precio de las acciones, la cantidad recaudada en cada una de las rondas de inversión y el porcentaje de las opciones existentes, es decir, los datos y la información de las operaciones se visualiza de forma clara y fácil. Además, permite determinar proporción correspondiente a cada inversor en la empresa. Los datos de los inversores, como identificadores de transacciones, por un lado, garantizan la transparencia de todo el proceso de negociaciones, permitiendo seguir el proceso de una determinada empresa, y, por otro lado, es un sistema de registro distribuido hace hincapié en la innovación de toda la tecnología en la que se basa la plataforma.

La primera empresa que ha hecho un acuerdo con las acciones lanzadas en la plataforma blockchain para el mercado de capital privado Linq ha sido una startup con nombre Chain. Esta startup fue financiada por Visa, Citi, Orange y Nasdaq, y su propuesta es ofrecer soluciones de blockchain para las empresas principalmente en el sector financiero. Están convencidos de que todos los activos del futuro serán instrumentos digitales que funcionarán en múltiples blockchains.

El grupo ING que proporciona servicios financieros de banca, seguros e inversiones lleva desarrollando una estrategia basada en blockchain desde el año 2015, y a día de

hoy ha realizado 27 pruebas de concepto en seis áreas de negocio, entre las cuales están los pagos, los mercados financieros, tesorería bancaria, préstamos, protección y verificación de identidad, entre otros. Los resultados de estas pruebas en gran parte son internos y no se conocen públicamente, pero lo que sí han anunciado es que han conseguido, por ejemplo, reducir los tiempos y los costes del proceso de recolección de datos de los clientes. En el caso de las finanzas comerciales, la blockchain ha ayudado a disminuir los costes operacionales entre un 10 y un 15%.

Otra línea de investigación que está llamando la atención de los bancos es la de la creación de sus propias criptomonedas basadas en la blockchain. Por ejemplo, los bancos Santander, Deutsche Bank, UBS y BNY Mellon están intentando promover el uso del dinero digital con el objetivo de hacer posible la transaccionalidad de activos reales como euros o dólares entre bancos centrales e instituciones financieras. La moneda se llamará “Utility Settlement Coin” (USC), y su objetivo principal será el de facilitar pagos y liquidaciones de manera rápida, segura y eficiente. Será una moneda que funcionará en un registro distribuido compartido entre varias entidades financieras, por lo que es convertible en paralelo a un depósito de su correspondiente divisa, lo que permite su intercambio eficiente entre entidades. A diferencia de otras criptodivisas, USC cumple con todos los requisitos regulatorios, lo que podría facilitar su implementación masiva en un futuro.

La creación de una criptomoneda propia es una tarea pendiente para el Banco Popular de China. Los sistemas de pagos móviles están en auge en este país, y, por otro lado, China es uno de los lugares donde más interés generan las criptodivisas, y donde más “granjas” de mineros de Bitcoin y más negociaciones con esta criptodivisa hay a nivel mundial. En diciembre de 2016 las autoridades chinas han realizado pruebas de intercambio bancario usando la moneda que han desarrollado. Aunque basada en la tecnología de cadenas de bloques, la moneda digital china tendría un respaldo del Gobierno y ayudaría principalmente a combatir la evasión fiscal, el lavado de dinero y transacciones ilegales, bajando a la vez el coste de transacción.

El Banco de Canadá también es un ejemplo de la apertura de las instituciones hacia la blockchain. En 2016 ha empezado el experimento con un proyecto llamado “Jasper”, con el fin de superar el Sistema de Transferencias de Grandes Valores que actualmente se utiliza en Canadá para transferencias electrónicas de grandes cantidades de dinero, y, por otro lado, explorar la posibilidad de emitir, transferir y liquidar los activos emitidos por el banco central en la red de registros distribuidos. Las cuestiones que iba a resolver este experimento eran varias. Por ejemplo, si puede o no un proyecto basado en la blockchain satisfacer los Principios sobre Infraestructuras de los Mercados Financieros (PFMIs por sus siglas en inglés), reducir costes y las barreras de entrada para participación directa, o si es capaz o no mejorar la seguridad y gestión de garantías, aumentar la flexibilidad, accesibilidad y transparencia (Hendry, 2016). Según la vicedirectora del Banco de Canadá Carolyn Wilkins, este experimento ha proporcionado mayor conocimiento de cómo el sector privado podría interactuar con un sistema de este tipo e incluso adaptarla. Han obtenido también unas ideas importantes que serán relevantes para este tipo de aplicación de registro distribuido en los negocios.

En primer lugar, han concluido que es poco probable que la mayoría de ahorros de costes venga en el sistema central, sino que vienen de la reducción de los esfuerzos de reconciliación bancaria. En segundo lugar, existe la posibilidad de obtener más ahorros si se pudieran construir otras aplicaciones sobre blockchain (por ejemplo, compensación y liquidación de activos financieros o financiación comercial). Además, si bien el sistema de registro distribuido podría tener como objetivo reducir la concentración del riesgo, se requeriría una cantidad considerable de centralización (por ejemplo, autorización de nodos y establecimiento de normas operacionales) si se

aplica a los sistemas de pagos mayoristas. En términos más generales, el experimento Jasper ha ayudado a Banco de Canadá, como admiten sus directivos, a entender mejor el imperativo comercial de quienes proporcionan y utilizan los servicios financieros. Es crucial que las instituciones financieras, los nuevos participantes y los encargados de formular políticas trabajen juntos para aprovechar todo el potencial de fintech (Wilkins, 2017).

Existen también ejemplos de la implementación de la tecnología blockchain y en concreto los contratos inteligentes en sector de finanzas corporativas. Por ejemplo, a finales de 2016 un banco ruso Alfa Bank ha utilizado los Smart contracts y la tecnología blockchain en las transacciones con carta de crédito (también llamado crédito documentario, es un instrumento de pago que se rige bajo normas internacionales y se utiliza cuando cuando se desea indicarle a un banco que concrete un pago a un tercero, siempre y cuando se cumplan todos los requisitos y las condiciones estipuladas para la mencionada transacción). Esta vez la prueba no ha sido interna, sino que involucraba a una empresa real – la aerolínea rusa S7 Airlines – como otra parte de la transacción. Las acciones han sido las siguientes. Primero, se ha creado un contrato inteligente acordado por las partes con antelación, luego los movimientos del banco relacionados con la apertura y la ejecución del crédito documentario han sido registrados en la blockchain, a través de un contrato inteligente. La información registrada en este caso fue el contenido y los términos de la carta de crédito. Asimismo, las etapas principales de la transacción han sido registradas a base de contratos inteligentes en el sistema Ethereum. La particularidad de esta transacción es la utilización de dos contratos inteligentes a la vez: uno solo para la apertura y otro para el cierre de la carta de crédito. Los contratos interconectados entre sí permiten disminuir la posibilidad de errores en el código, protegiendo a la vez los intereses de ambas partes y aumentando la transparencia de la transacción.

Pero no solo los bancos y las entidades financieras están mostrando entusiasmo a la hora de investigar la blockchain. En abril de 2017 se produjo el primer encuentro del grupo asesor de Fintech de alto nivel (High Level Advisory Group on Fintech) del Fondo Monetario Internacional, el grupo que cuenta con importantes ejecutivos del sector (Del Castillo, 2017). Aunque la reunión no era pública, solo el hecho de su celebración demuestra un fuerte interés por parte del Fondo Monetario Internacional en investigar las posibilidades de la blockchain. Asimismo, los encuentros de este tipo pueden ayudar a encontrar beneficios de esta tecnología para el FMI, como ayudar a los reguladores a considerar los posibles riesgos que puede llevar su implementación masiva.

4.5. PAÍSES QUE ESTÉN EMPEZANDO A UTILIZAR LA TECHNOLOGÍA DE CADENA DE BLOQUES

Los gobiernos más avanzados ya están trabajando en el área de la blockchain, ya que esta tecnología podría beneficiar la sociedad en varios aspectos, como, por ejemplo, los servicios públicos o la identidad digital, entre otros.

Una de las áreas muy importantes para el gobierno es la prevención de fraude. Por ejemplo, después de que en 2014 uno de los bancos más grandes de Hong-Kong “Standard Chartered” ha perdido casi 200 millones de dólares como consecuencia de un fraude con los préstamos garantizados con la carga en el puerto chino de Qingdao, el gobierno de Singapur ha decidido utilizar la blockchain para prevenir las prácticas financieras engañosas. Los estafadores utilizaron duplicados de las facturas para la misma mercancía para recibir dinero de los bancos, por eso el gobierno de Singapur junto a los bancos locales ha desarrollado un código criptográfico único para cada factura. Así, los bancos traspasan este código único, y no los datos primarios. Si otro banco intenta registrar una factura con los mismos datos, salta una alerta. En cuanto a

la aceptación de criptodivisas existentes, en Singapur son totalmente legales, y a partir de 2014 las operaciones con Bitcoin equivalen a transacciones sujetas a impuestos sobre bienes y servicios de cara a las autoridades fiscales.

En otro país asiático, China, la blockchain ya está en la lista de las tecnologías avanzadas que ha sido promovida en el 13 Plan Quinquenal (un documento de planificación económica gubernamental utilizado en la República Popular de China) para ayudar a mejorar las industrias nacionales y a combatir fraudes financieros. Además, mientras cuatro bancos chinos están en el ranking de los cinco más grandes en el mundo en capitales, muchos de ellos siguen utilizando fax o sellos tradicionales para verificar los documentos (Tham, 2017). Lo mismo sucede en muchos otros sectores, y es inaceptable para un país que intenta promover el uso de tecnologías disruptivas. Por el contrario, Japón es uno de los líderes de innovaciones en el sector fintech, y es uno de los países que más avances han conseguido – es el primer país que reconoce el Bitcoin como un sistema de pago legal.

En Estonia la utilización de la tecnología blockchain, sin embargo, es diferente y no se centra solamente en el sector financiero. Conocido como un país con uno de los gobiernos más progresivos digitalmente, Estonia permite tener un sistema de residencia electrónica (o “e-Residency”) a los extranjeros. Esta identidad digital permite a los extranjeros que pueden incluso vivir en otros países distintos registrar empresas en Estonia, utilizar la banca digital y la firma electrónica. El funcionamiento de este sistema es posible gracias a la tecnología blockchain, en la que se puede gestionar, registrar y almacenar incluso la información más sensible como los datos personales de forma segura y protegida. Aparte de e-Residency, Estonia está haciendo pruebas junto con Nasdaq Tallinn para implementar el sistema de votación electrónica (e-voting) como la siguiente etapa (DeMarinis, Uustalu, & Voss, 2017). En España el ayuntamiento de Barcelona también ha manifestado su interés en la tecnología, cuando ha decidido implementar blockchain para el manejo de las identidades digitales (Proyecto Decode).

Por otra parte, la blockchain y su sistema de registro distribuido impiden la corrupción pues como sabemos los registros son inmutables y constantes, y están protegidos criptográficamente. Muchos países están desarrollando formas para aprovechar esa funcionalidad en la lucha contra la corrupción. Por ejemplo, el registro catastral de tierras basado en la blockchain ya está siendo implementado en Georgia, Grecia y Honduras. Algo similar están desarrollando en Gana, África Occidental, donde la blockchain va a permitir garantizar transparencia en las operaciones con inmuebles y sentar bases para la atracción de inversión extranjera.

En Ucrania también piensan combatir la corrupción y la burocracia con los avances tecnológicos. Entre los proyectos que ya se están probando están eAuction 3.0, un sistema de subasta electrónica para alquiler o venta de bienes de estado basado en la blockchain, o e-Vox, un proyecto que permitiría organizar votaciones totalmente transparentes. El último avance en este campo ha sido un acuerdo fundamental entre el Gobierno de Ucrania y la startup Bitfury para crear aplicaciones en plataforma distribuida de gobernanza digital que va a incluir varios aspectos. En primer lugar, se desarrollará un programa piloto para la introducción de la tecnología en procesos actuales de la plataforma del gobierno de Ucrania. Las áreas que se van a incluir son registros públicos, seguridad social, energía y salud. La segunda fase va a incluir también servicios de ciberseguridad. El objetivo principal de esa innovación es proteger los datos del estado, pero también reducir costes para los ciudadanos, impulsar la inversión extranjera, y, obviamente, reducir niveles de corrupción.

Aunque no solo los países emergentes están tomando este camino. Suecia está desarrollando un proyecto que permitiría concertar transacciones inmobiliarias de forma que todas las contrapartes – los bancos, los agentes, los compradores y vendedores – puedan tener la oportunidad de seguir el proceso de la implementación del acuerdo después de su finalización, lo que permitiría autenticar las transacciones

instantáneamente. Gran Bretaña, en su lugar, está considerando las posibilidades de utilizar el registro distribuido para la gestión de asignación de subvenciones. Como el control y el seguimiento de las subvenciones concedidas es bastante complejo y muchas veces su uso indebido y el abuso es algo común, la tecnología blockchain podría ofrecer la mejor solución para este problema, ya que está disponible para todas las partes implicadas (Mougayar, 2016a). En cuanto a Estados Unidos, por ejemplo, el gobernador del estado Delaware Jack Markell ha anunciado en 2016 el desarrollo de dos iniciativas basadas en la blockchain. La primera se centra en la circulación de los archivos gubernamentales en el registro distribuido, y la otra permite a cualquier empresa privada registrada en Delaware hacer el seguimiento a las acciones y los derechos de los accionistas.

En resumen, las principales aplicaciones que ofrece la tecnología blockchain en el sector gubernamental y servicios públicos pueden ser los siguientes:

- Verificación

Por ejemplo, de licencias, registros, entradas, operaciones, procesos o eventos. Una vez registrados en la blockchain, estos acontecimientos no pueden ser cambiados o eliminados por un intruso. Por otra parte, siendo registro distribuido, se vuelve prácticamente inaccesible para los virus o cualquier malware informáticos, una gran ventaja frente a bases de datos convencionales (no distribuidos).

- Movimiento de activos

Las transferencias monetarias de una entidad jurídica a otra, sobre todo si se trata de la distribución de fondos del Estado. En este caso, la utilización de contratos inteligentes puede ser muy conveniente, ya que no es necesario un intermediario, la transacción puede procesarse automáticamente en cuanto se cumplen los requisitos predefinidos, y un uso indebido de recursos se vuelve prácticamente imposible, ya que la operación queda gravada en el registro distribuido. Lo mismo pasa con el presupuesto nacional, regional o municipal – blockchain podría permitir a cualquier ciudadano averiguar cómo fue gastado y dónde han acabado sus impuestos.

- Propiedad

Registros de tierras, títulos de propiedad y cualquier tipo de propiedad inmobiliaria. La cadena de bloques es un perfecto guardián de la cadena de custodia para cualquier activo físico.

- Identidad y datos personales

El gobierno puede emitir documentos de identidad digital para sus ciudadanos a través de la blockchain, lo que les permitiría utilizar de forma segura algunos servicios públicos o realizar sus derechos, como el derecho a voto, de forma totalmente segura.

Para realizar todas esas funciones aprovechando la nueva tecnología, los líderes de los gobiernos deberían tomar algunos pasos importantes, que son los siguientes:

1) Investigar la capacidad y estudiar las posibilidades que brinda la blockchain.
2) Crear equipos responsables del desarrollo de la tecnología en cara a los servicios públicos, con el fin de adoptar, finalmente, una estrategia de desarrollo.
3) Empezar a experimentar con la tecnología a través de pruebas de conceptos y proyectos, en principio a pequeña escala. Hay que mencionar también, que incluso en ciudades muy pequeñas existen varias posibilidades para adoptar la innovación, mientras que ponerla en práctica sería mucho más accesible ahí que en ciudades con millones de habitantes.
4) Desarrollar nuevas ideas progresistas y ambiciosas para las necesidades cotidianas de los ciudadanos.
5) Facilitar la introducción de las soluciones basadas en la blockchain que reducen costes y ofrecen a los ciudadanos servicios públicos y gubernamentales rápidos, asequibles y de calidad.

Como podemos ver, son muchos los países donde estas prácticas ya se están llevando a cabo, y se espera que cada vez sean más. De esta manera, podríamos ver una diferencia significativa en la prestación de servicios públicos, y, por lo tanto, un claro beneficio para la sociedad y para los ciudadanos.

4.6. REGULACIÓN Y LIMITACIONES

Como en el caso de cualquier tecnología nueva y en fase temprana, la regulación de la blockchain es un tema pendiente para las instituciones reguladoras nacionales e internacionales. A día de hoy, no existe ninguna regulación básica de la tecnología blockchain, sino que varía mucho según la región, el estado y el país. En términos generales, la mayoría de las normas aplicables son las que regulan los sectores en que se aplica esta tecnología. Por ejemplo, a las empresas del ámbito de la criptodivisa bitcoin habitualmente se les aplican las normas financieras tradicionales. Asimismo, en el caso de las empresas que operan en el sector sanitario, igualmente se les aplicarían las normas de dicho sector (Jiménez & Pierce, 2017).

No obstante, al igual que otras innovaciones digitales, la blockchain tendrá que encontrar formas de cómo hacer frente y adaptarse a las regulaciones que varían en grado y complejidad. En abril de 2016, la Cámara de Comercio Digital, la organización comercial líder mundial en representación de la industria de activos digitales y cadenas de bloques, junto a otras organizaciones principales en el sector blockchain han lanzado un evento con nombre Global Blockchain Forum (Foro Global de la Blockchain), cuyo objetivo es ayudar a formar regulaciones para dicha tecnología. Se espera que las regulaciones se ponen en marcha pronto, especialmente como la tecnología siga avanzando a este ritmo. Ciertos países y estados pueden tener más facilidad a la hora de cosechar los beneficios de la blockchain, ya que las regulaciones y la experiencia con ella varían dependiendo de la zona.

En cuanto al estatus legal de Bitcoin, esta criptomoneda suele ser tratada en algunos países como un bien o un activo de inversión a efectos fiscales está sujeto a la legislación pertinente. A veces es reconocida como una unidad monetaria (por ejemplo, en Alemania), en otros países (por ejemplo, Japón), el Bitcoin es un medio legal de pago con el impuesto sobre la compra. También hay países (como China) donde las transacciones con Bitcoin están prohibidas para los bancos, pero permitidas para las personas físicas, mientras que China es un líder en el campo de la minería debido a la presencia de grandes capacidades de producción. Uno de los países más favorables hacia Bitcoin es Suiza, donde a la criptomoneda se aplican las mismas reglas como en una moneda extranjera. Además, la legislación suiza favorece a las startups en este ámbito y las blockchain públicas. Hay que mencionar, que a otras criptodivisas que no sean Bitcoin (Ethereum, Litecoin, Zcash etc.) la regulación les aplica las mismas normas, por eso cuando mencionamos el Bitcoin en este contexto, nos referimos a todas monedas digitales criptográficas.

En general, si hablamos del sector financiero, la regulación preventiva puede ser poco eficiente, y la sobrerregulación, hasta perjudicante. Por eso, en el contexto regulador mundial, por parte de entidades financieras la mejor opción es seguir controlando la nueva tecnología, más bien en forma de supervisión, pero a su vez dejando que las empresas fintech se desarrollen y la tecnología madure. Aparte, es necesario educar a los usuarios y explicarles el significado de la revolución blockchain y sus posibles beneficios. Por último, la modernización de las instituciones tradicionales tiene que ir de la mano con la generación de un ecosistema competitivo y potente.

4.6.1. Blockchain y criptodivisas en España

España es uno de los primeros países que más rápido ha colocado la atención en sector de las criptodivisas en el aspecto legal, siendo un país impulsor ante las autoridades de la Unión Europea.

En el año 2013 el Instituto de Contabilidad y Auditoría de Cuentas que forma parte de Hacienda consideraba Bitcoin como existencias, no como una moneda, aunque después en varias consultas vinculantes la nombraba “un medio de pago” que es legal en España y se consideraba libre de IVA. Con la inclusión del Tribunal de Justicia de la Unión Europea a Bitcoin en la categoría de divisas tradicionales y otros medios de pago en el 2015 como divisa virtual o electrónica, el pago con Bitcoin se declaró equivalente a un pago en cualquier divisa fiduciaria en toda Europa.

Por otro lado, en España se intenta controlar la actividad de los mineros de Bitcoin. Las personas que se dedican a esta actividad deben registrarse en Hacienda y en la Seguridad social como trabajadores autónomos. Sin embargo, Hacienda acepta la creación de divisas digitales y declara que la actividad no sujeta a Impuesto de Valor Añadido (IVA), el que tampoco se cobrará por las ventas de divisas virtuales en España. La instalación de los cajeros físicos de Bitcoin (que actualmente son 22 y están distribuidos por todo el país) está apoyada por Hacienda que ha definido incluso un marco legal para este tipo de actividades. A su vez, la Oficina Nacional de Investigación del Fraude (ONIF) está investigando a las empresas españolas que usan Bitcoin y otras criptodivisas para poder garantizar que no cometan fraude o cualquier otra actividad ilícita de esta forma.

Una de las primeras empesas que comenzó a investigar sobre el tema de legalidad para el Bitcoin y la blockchain en España es el despacho de abogados especializados en Derecho Tecnológico Abanlex. Pero los avances existen no solo en el marco legislativo. Los bancos españoles como Santander y BBVA han sido pioneros en la adopción de la tecnología blockchain en el sector financiero. Ambos forman parte de los consorcios internacionales más grandes que investigan en este ámbito, como R3CEV o Hyperledger, y están haciendo pruebas continuamente. Otro banco español, Sabadell, ha organizado varios eventos y hackatons para promover esta tecnología y crear nuevos conceptos al respecto, y ha destinado más de 96 millones de euros para financiar las startups. Además, existen empresas a gran escala, como la mayor compañía eléctrica de España Endesa, que está apostando a investigar cómo podría mejorar sus servicios el uso de la blockchain con las aplicaciones para la industria (Das, 2016). Para ello ha creado un laboratorio centrado especialmente en diseñar soluciones basadas en la blockchain enfocados en el sector energético.

Al mismo tiempo, están apareciendo nuevas startups españolas que basan sus soluciones en la blockchain, como la startup barcelonesa con nombre Aragon. Esta empresa, que pretende revolucionar la gestión y administración de empresas usando la tecnología blockchain y las ventajas que brindan los contratos inteligentes, ya han tenido una inversión de 150 mil dólares, y en mayo-junio de 2017 tiene planeado lanzar su campaña de ICO. Por otra parte, están apareciendo cada vez más programas educativos que pretenden dar de conocer las posibilidades de la blockchain a los estudiantes, emprendedores y empresarios españoles, desde los cursos presenciales (por ejemplo, los que ofrece la Universidad de León), hasta varios cursos y clases sobre el tema en línea disponibles a cualquiera interesado en el tema. De hecho, el siguiente congreso mundial de blockchain, Blockchain World Forum tendrá lugar en Barcelona en octubre de 2017.

Evidentemente, todas estas actividades acercan España a convertirse en un ecosistema del conocimiento blockchain. Aunque todavía faltan muchos obstáculos por superar en el camino de implementar la tecnología blockchain en diferentes ámbitos sociales y dar de conocer sus ventajas, España parece pisar fuerte en esta dirección.

4.6.2. ¿Por qué todavía no utilizamos ampliamente la Blockchain?

Cuando en 2008 en medio de la crisis económica mundial y la pérdida de confianza a las instituciones financieras globales apareció la primera criptodivisa Bitcoin, fue un acontecimiento excepcional. Aunque el foco estaba puesto en esta moneda digital

descentralizada, transparente y libre de control superior e intermediarios, y no en la infraestructura que permite su funcionamiento – la tecnología de cadena de bloques o blockchain.

Sin embargo, el protocolo inventado por Satoshi en realidad tenía muchas posibilidades de revolucionar casi todas las áreas económicas y sociales, transformando radicalmente nuestra forma de entender los conceptos tan básicos como la confianza o el derecho de propiedad. Por eso, para el año 2015 los discursos sobre el potencial de la blockchain han saltado a popularidad convirtiéndose en corrientes dominantes ya no solo para un pequeño grupo de criptoanarquistas, ingenieros y matemáticos, sino que ha llegado al público en general. No obstante, el uso de las criptodivisas sigue siendo complejo para un usuario común, y actualmente los esfuerzos de las instituciones financieras y grandes empresas de poner en funcionamiento la blockchain para sus necesidades acaban solo en experimentos y pruebas en esta dirección.

Las investigaciones llevadas a cabo por la Universidad de Harvard al respecto proponen una multitud de usos que puede ofrecer la blockchain, pero también admiten que existen algunas razones por los que todavía no está ampliamente utilizado en las industrias (Iansiti & Lakhani, 2017). ¿Cuáles son, entonces, las razones de poca popularización actual de esta tecnología?

1) Falta de confianza

En primer lugar, es imprescindible ganar confianza de los usuarios y darles de entender en qué se diferencia la tecnología blockchain, por qué es más segura y más rápida, cuál es su propuesta de valor para un cliente particular y por qué debe ser elegida. Desgraciadamente, en muchos casos la información que se puede encontrar sobre el tema en medios de comunicación o internet carece de claridad y está orientada más bien a profesionales que a gran público. Lógicamente, ganar confianza de usuario de la tecnología (como de cualquier producto) lleva tiempo y esfuerzo.

2) Novedad

No debemos olvidar que la tecnología Blockchain está en su fase temprana. Ya sabemos y entendemos las ventajas que teóricamente aportará, pero todavía faltan tanto investigaciones académicas y estudios de casos prácticos en este aspecto, como recursos humanos altamente profesionales y cualificados para llevar esta tecnología a las empresas y “a la calle”. Existen muchos ejemplos de cuando un error humano en el código podía causar varios problemas (por ejemplo, el caso de TheDAO, cuando por una falta en programación se ha podido atacar la red y robar los fondos, aunque finalmente ha sido devuelto a sus dueños). Este tipo de situaciones suceden por falta de profesionales en el sector tan joven, pero a la vez afectan negativamente en toda la comunidad, ya que los usuarios empiezan a pensar que la blockchain puede ser hackeada, cuando en realidad los errores humanos en el código no significan vulnerabilidad del sistema como tal.

3) La disrupción que ofrece

Mientas que muchas industrias ven a blockchain como una forma de reducir costes y superar rápidamente a las empresas establecidas, reuniendo un modelo comercial tradicional con la rapidez y costes mucho más bajos, el verdadero valor que ofrece esta tecnología es la posibilidad de crear nuevos modelos de negocio y apoyar la infraestructura económica, social y empresarial. Pero para conseguirlo, como hemos dicho antes, hacen falta muchos profesionales dispuestos a estudiar esa posibilidad, y, por otro lado, los inversores dispuestos a lanzar capital de riesgo en los proyectos con un modelo de negocio totalmente nueva.

4) Adopción

A día de hoy, los que más han abrazado a la blockchain han sido los bancos y las entidades financieras – esos intermediarios centralizados contra los que lucharon primeros adeptos de Bitcoin. Son estas instituciones las que más promueven la

utilización de esta tecnología, ya que les permite ahorrar los gastos y mejorar el servicio. Mientras, en otros sectores esa adopción puede tardar años por falta de legislación, por asuntos burocráticos o simplemente por falta de interés por parte de los gobernantes y directivos.

Si nos fijamos en el sector financiero en concreto, en el año 2016 Morgan Stanley en su informe ha publicado un mapa de implementación de la blockchain (*Global Insight: Blockchain in Banking: Disruptive Threat or Tool?*, 2016). Esta hoja de ruta afirma que las instituciones financieras tardarán entre 5 y 10 años en implementar esta tecnología.

Según Morgan Stanley, entre 2016 y 2018 los bancos y las corporaciones van a realizar pruebas de concepto de esta tecnología, con el objetivo de evaluar si la blockchain puede ser escalable y reducir los costes de manera eficaz. Entre 2017 y 2020, veremos cómo va a aparecer una infraestructura compartida, con activos que han sido probados más allá de la etapa inicial de prueba de concepto. Finalmente, entre 2021 y 2025 aún más activos se trasladarán en la cadena de bloques, como la eficiencia ya habrá sido demostrada. Por ahora, las predicciones se están cumpliendo, ya que las pruebas se están realizando y la atención puesta en esta tecnología crece cada vez más.

Aunque la tecnología blockchain tiene el potencial para ofrecer muchos beneficios a la industria financiera, todavía existen obstáculos clave que habrá que superar antes de que la implementación blockchain se convierta en una realidad.

1) **La relación entre coste y beneficio**

La blockchain puede hacer que las transacciones financieras se procesen más rápidamente, pero la velocidad no siempre significa ganancias. Teniendo en cuenta el coste elevado del desarrollo de la infraestructura nueva, cada uso propuesto tiene que tener un impacto positivo en el capital invertido.

2) **Mutualización de costes**

Si la blockchain compartida funcionara como una herramienta interoperable de la industria, los bancos deberían compartir costes de la construcción de esta infraestructura. Sin embargo, eso puede ser desafiante, teniendo en cuenta una amplia variación de los tamaños de los bancos y su necesidad de adaptación.

3) **Alineamiento de incentivos**

En el caso de blockchain compartidas, entidades diferentes pueden tener prioridades conflictivas. Pero sin grandes grupos de usuarios, la tecnología no tendrá éxito.

4) **Evolución de los estándares**

Los usuarios quieren determinar un estándar antes de cualquier inversión material, y la existencia de demasiadas opciones en este campo podría retrasar la adopción.

5) **Mantenimiento de escalabilidad**

Una blockchain debe escalar eficazmente de la prueba de concepto para tener éxito, y es una razón clave por qué la mayoría de propuestas nuevas de la blockchain está mirando hacia un amplio rango de reglas, incluido las que restringen usuarios o los centralizan, total o parcialmente. Sin ellos, los gastos de energía más altos podrían eliminar los beneficios de los costes de personal más bajo.

6) **Dirección y gestión**

Va a hacer falta un órgano directivo para tomar la decisión sobre a quién permitir acceso a la blockchain y quién gestiona su mantenimiento.

7) **Regulación**

Debería abordarse también el desafío de regular las identidades digitales y las normas transfronterizas para un funcionamiento eficaz.

8) **Riesgos legales**

Los usuarios de los sistemas de cadenas de bloques en servicios financieros tienen que ser entidades identificables. Los reguladores van a exigir las políticas KYC (por sus siglas en ingés “Know your customer”, en castellano – conoce a tu consumidor) y AML (por sus siglas en inglés, “Anti-Money Laundering” – contra lavado de capitales), independientemente del protocolo de software.

9) Seguridad

Los bancos tendrán que realizar una extensa investigación para asegurarse de que cualquier cadena de bloques que se va a implementar sea al menos tan resistente ante un ataque informático como su infraestructura actual.

10) Simplicidad

Las soluciones basadas en la blockchain deben ser sencillas y fáciles de entender. También tienen que interactuar sin problemas con otras partes de la cadena tecnológica, lo que permite que el proceso de configuración, formación y fijación sea más rápido.

Si todos los desafíos nombrados anteriormente se solucionen y el sector financiero pueda llevar la tecnología blockchain a sus consumidores, es muy probable que todos los componentes se podrán beneficiar de los cambios que llevará.

4.6.3. Los desafíos y limitaciones de las criptodivisas

El uso de criptodivisas tampoco está en su auge. Aunque sus beneficios frente a las divisas fiduciarias son evidentes (rapidez de transacciones, transparencia y seguridad, por ejemplo), todavía no se han convertido en una parte de nuestro día a día. Para esa falta de adopción hay varios motivos, pero el más crítico es la altísima volatilidad en precio de criptodivisas (Haran, 2017). Los precios de monedas digitales fluctúan por fuerte movimiento especulativo. La estabilidad es esencial no solo para una criptomoneda, sino también para cualquier divisa que pretende cumplir función de medio de intercambio de confianza. En caso de fluctuaciones continuas, los usuarios van a tener miedo de que su dinero pierda todo el valor, por lo cual no lo ven como una moneda real. Peor aún, la imprevisibilidad de los precios causa estragos en los servicios monetarios regulares, como el envío de transferencias, la conversión de divisas y el uso de cajeros automáticos. Con el fin de utilizar criptomonedas, las empresas tienen que cubrir sus riesgos mediante el cobro de tasas exorbitantes (en el caso de cajeros automáticos, puede llegar a un 15%), lo que elimina por completo una de las principales ventajas que ofrecen frente las monedas fiduciarias. Por esta razón, la mayoría de las personas que utilizan criptodivisas las ven como un instrumento de inversión de alto riesgo más que como un medio de pago o una moneda.

Para no permitir una inestabilidad tan alta, la única forma es prever la demanda que va a tener la nueva criptomoneda. El problema de predecir la demanda, sin embargo, es la existencia de especuladores que crean demanda artificial, ya que así su precio no refleja el uso de la moneda ni la demanda real. Tradicionalmente, la solución a este problema ha sido el banco central, pero las criptodivisas, descentralizadas por definición, tendrán que encontrar un enfoque totalmente nuevo a la hora de disminuir el rango de volatilidad, preferiblemente sin comprometer la libertad de usuarios ni recurrir a la inflación. Con la especulación, la infusión de capital es necesaria para mantener la moneda estable, lo que puede ser una tarea importante. Por ejemplo, Bitcoin: con la capitalización de mercado de aproximadamente 20 mil millones de dólares, necesitaría una enorme cantidad de capital para ser más o menos estable.

Una de las estrategias es centrarse en la creación de valor con productos y servicios únicos que están asociados con la moneda. De esta manera, se podría decir que la moneda está respaldada por algo que la gente realmente quiere, y no solo movimientos especulativos de los traders en búsqueda de alta rentabilidad. Otra forma es establecer primero una base de usuarios y luego introducir la criptomoneda.

Por último, la solución a este problema no se ha encontrado todavía, pero es la única manera de que criptomonedas se vuelvan más competitivas frente a las fiduciarias.

CAPÍTULO 5. CONCLUSIONES

Cuando en el año 2008 apareció por primera vez la criptomoneda Bitcoin, muchos la veían como un cambio total de paradigma y el comienzo de un Nuevo Mundo descentralizado, donde los intermediarios no van a existir y los bancos desaparecerán. Todavía hay los que piensan así, pero la realidad ha demostrado que por ahora no es posible, teniendo en cuenta varios inconvenientes y aspectos por mejorar y perfeccionar que caracterizan esa tecnología, desde la altísima volatilidad que tienen las monedas digitales hasta la falta de conocimiento por parte de usuarios finales. No debemos olvidar que tanto el concepto de criptodivisas, como la de la blockchain son muy jóvenes, se trata de una tecnología que todavía está en su primera versión "alfa", y no ha demostrado su efectividad al cien por cien.

Quizás a día de hoy no estamos en una revolución, pero claramente estamos al borde de un cambio importante, sobre todo en el sector bancario y financiero. El poder de realizar transacciones transfronterizas de forma casi inmediata, la transparencia de servicios financieros y bancarios, la posibilidad de financiación de pequeñas empresas y grandes proyectos independientemente y de forma descentralizada y abierta, la privacidad para el usuario y la disminución de costes para las instituciones – son solo algunas de las ventajas que puede ofrecer la tecnología blockchain. Pero la pregunta es, si se podrá utilizar las ventajas que brinda para beneficiar realmente a la sociedad. Y eso depende de los que van a estar detrás de los cambios – de los mismos bancos, instituciones financieras y los gobiernos. Ellos van a ser responsables de resolver un dilema importante: cómo encontrar el equilibrio entre la privacidad de los usuarios y el control de actividades ilícitas, la regulación que sirve para proteger a los ciudadanos y la sobrerregulación que recorta sus derechos. Por otro lado, la regulación no debe anteceder la innovación, sino que ir en un conjunto orgánico con ella.

El sector financiero tiene un desafío por delante que se trata, por un lado, de digitalización y mejora del servicio a cara de los usuarios y clientes finales, y, por otro lado, la reducción de costes y el alcance de alta rentabilidad. La clave está en que la blockchain sea capaz de ofrecérselo. A día de hoy, esta tecnología todavía no se está utilizando en el sector de forma generalizada, pero se realizan cada vez más pruebas de concepto, que acercan el momento de su implementación masiva. Aun así, es evidente que blockchain ha venido para quedarse. Durante los meses de realización de este trabajo, los principales periódicos de gran impacto en el mundo económico y financiero no paraban de publicar noticias sobre los experimentos con esta tecnología de los bancos y las grandes expectativas que tienen ellos al respecto, lo que demuestra un gran interés hacia la blockchain. Aunque la "fiebre" de la blockchain a veces parece exagerar, el volumen de la inversión de las instituciones demuestra que la blockchain ya no es percibida como una amenaza, sino como una oportunidad que los bancos tienen que aprovechar para no quedar atrás en el proceso global de transformación digital.

En mi opinión, todavía no se puede hablar de la implementación masiva de la blockchain, pero los próximos años serán la clave para esta tecnología. Si la blockchain demuestra su poder de evolucionar desde los escenarios de prueba a poder ofrecer soluciones reales, rentables y escalables, logrando a la vez entregar el valor percibido y mejorar los procesos, será abrazada por las instituciones.

BIBLIOGRAFÍA

Armknecht, F., Karame, G. O., Mandal, A., Youssef, F., & Zenner, E. (n.d.). Ripple: Overview and Outlook. Retrieved from http://www.ghassankarame.com/ripple.pdf

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. Retrieved from http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

Bheemaiah, K. (2017). *The Blockchain alternative : rethinking macroeconomic policy and economic theory*. Paris, France. Retrieved from https://books.google.es/books?id=M5o7DgAAQBAJ&pg=PA82&lpg=PA82&dq=ILP+Ledger+qué+es&source=bl&ots=fDzM1ui8XZ&sig=TXwR3zoVhaIfFDWeUIjERWI_mdk&hl=es&sa=X&ved=0ahUKEwjl34CGnKTTAhVCKsAKHeYxDNMQ6AEITDAF#v=onepage&q&f=false

Blair, D. (2016). *Ripple vs SWIFT: Payment (r)evolution*. Retrieved from http://www.atc.asia/articles/170105/aca161124ripple.pdf

Buterin, V. (2014). Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform. *Bitcoin Magazine*. Retrieved from https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/

Byström, H. (2016). *Blockchains, Real-Time Accounting and the Future of Credit Risk Modeling*. Retrieved from http://www.the-blockchain.com/docs/Blockchains, Real-Time Accounting and the Future of Credit Risk Modeling.pdf

Cant, B., Khadikar, A., Ruiter, A., Bolgen Bronnebakk, J., Coumaros, J., Buvat, J., & Gupta, A. (2016). *Smart Contracts in Financial Services: Getting from Hype to Reality*. Retrieved from https://www.capgemini-consulting.com/resource-file-access/resource/pdf/smart-contracts.pdf

Cearley, D. W., Walker, M., & Burke, B. (2016). *The Top 10 Strategic Technology Trends for 2017*. *Gartner*.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. In *Advances in Cryptology* (pp. 199–203). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4757-0602-4_18

Dai, W. (1998). B-Money. Retrieved from http://www.weidai.com/bmoney.txt

Das, S. (2016). Spanish Electricity Giant Endesa is Harnessing Blockchain Tech. Retrieved May 3, 2017, from https://www.cryptocoinsnews.com/spanish-electricity-giant-endesa-looks-harness-blockchain-tech/

Del Castillo, M. (2017). The IMF Just Finished its First “High Level” Meeting on Blockchain. Retrieved April 30, 2017, from http://www.coindesk.com/imf-just-finished-first-high-level-meeting-blockchain/

DeMarinis, R., Uustalu, H., & Voss, F. (2017). Is Blockchain the Answer to E-voting? Nasdaq Believes So. Retrieved May 2, 2017, from http://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html

Demirgüç-Kunt, A., Klapper, L., Singer, D., & Van Oudheusden, P. (2015). *The Global Findex Database 2014: Measuring Financial Inclusion around the World*. *World Bank Policy Research Working Paper 7255*. https://doi.org/10.1596/1813-9450-7255

Fernández, J. G. (2016). ¿Cuánto puede ahorrarle el “blockchain” a los clientes de banca? Retrieved April 16, 2017, from http://www.expansion.com/economia-digital/innovacion/2016/10/27/5811f12a468aebb3078b464b.html

Fernández Espinosa, L. (2016). Smart Contracts: los contratos basados en blockchain que no necesitan abogados. Retrieved April 16, 2017, from https://www.bbva.com/es/noticias/economia/computacion/transformacion-digital/smart-contracts-los-contratos-basados-blockchain-no-necesitan-abogados/

Fortnum, D., Mead, W., Pollari, I., Hughes, B., & Speier, A. (2017). *The Pulse of Fintech Q4 2016: Global analysis of investment in fintech*. Retrieved from https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/pulse-of-fintech-q4-2016.pdf

Global Insight: Blockchain in Banking: Disruptive Threat or Tool? (2016). Retrieved from http://www.morganstanley.com/ideas/big-banks-try-to-harness-blockchain

Gorjón, S. (2014). Divisas o Monedas Virtual: El caso de Bitcoin. Retrieved from http://www.bde.es/f/webpcb/RCL/canales/home/menu-botonera/noticias/2014/Enero/pdf/Nota_informativa_Bitcoin_enero2014.pdf

Haferkorn, M., & Quintana Diaz, J. M. (2015). Seasonality and Interconnectivity Within Cryptocurrencies - An Analysis on the Basis of Bitcoin, Litecoin and Namecoin (pp. 106–120). Springer, Cham. https://doi.org/10.1007/978-3-319-28151-3_8

Haran, N. (2017). What's keeping cryptocurrencies from mass adoption? Retrieved May 4, 2017, from https://techcrunch.com/2017/04/20/whats-keeping-cryptocurrencies-from-mass-adoption/

Hendry, S. (2016). *The Bank of Canada's Blockchain Experiment*. Retrieved from http://chicagopaymentssymposium.org/wp-content/uploads/2016/10/101316-intl-lessons-learned-hendry.pdf

Hetherington, R., & Schiebs, H. (2016). Can Blockchain support enterprise size banking? Retrieved April 20, 2017, from http://www.globalbankingandfinance.com/can-blockchain-support-enterprise-size-banking/

Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. *Harvard Business Review*, 118–127. Retrieved from https://hbr.org/2017/01/the-truth-about-blockchain

Jiménez, M., & Pierce, B. (2017). Bitcoin: Brock Pierce: "Habrá empresas de 'blockchain' tan importantes como Google o Facebook." Retrieved May 3, 2017, from http://retina.elpais.com/retina/2017/04/20/tendencias/1492718244_153098.html

Kashyap, M., Garfinkel, H., & Shipman, J. (2016). *Blurred lines: How Fintech is shaping Financial Services*. Retrieved from http://www.pwc.es/es/publicaciones/financiero-seguros/assets/pwc-fintech-global-report-2016.pdf

Kastelein, R. (2017). Blockchain Capital Closes ICO - $10 Million in Six Hours Raised in Record Time. Retrieved April 22, 2017, from http://www.the-blockchain.com/2017/04/11/blockchain-capital-closes-ico-10-million-in-six-hours-raised-in-record-time/

Leising, M. (2015). The Blockchain Revolution Gets Endorsement in Wall Street Survey - Bloomberg. Retrieved April 20, 2017, from https://www.bloomberg.com/news/articles/2015-07-22/the-blockchain-revolution-gets-endorsement-in-wall-street-survey

Levine, M. (2016). Blockchain Company Wants to Reinvent Companies. Retrieved April 22, 2017, from https://www.bloomberg.com/view/articles/2016-05-17/blockchain-company-wants-to-reinvent-companies

Mankiw, N. G. (2006). Principles of Microeconomics. *Cengage Learning*, 533. https://doi.org/10.4324/9780203333716

McDonald, T. (2016). R3 brings eleven major global financial institutions together on a cloud based distributed ledger — R3. Retrieved April 28, 2017, from http://www.r3cev.com/press/2016/1/20/r3-brings-eleven-major-global-financial-institutions-together-on-a-cloud-based-distributed-ledger

Meijer, C. R. W. (2017). Towards smaller and more focused blockchain consortia. Retrieved April 25, 2017, from https://www.finextra.com/blogposting/13760/towards-smaller-and-more-focused-blockchain-consortia

Montes de Oca, J. (2017). Cotización. Retrieved May 4, 2017, from http://economipedia.com/definiciones/cotizacion.html

Mougayar, W. (2016a). The Blockchain is Perfect for Government Services. Retrieved May 3, 2017, from http://www.coindesk.com/blockchain-perfect-government-services-heres-blueprint/

Mougayar, W. (2016b). *The business blockchain : promise, practice, and application of the next Internet technology*. Retrieved from https://books.google.es/books/about/The_Business_Blockchain.html?id=X8oXDAAAQBAJ&redir_esc=y

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, 9. https://doi.org/10.1007/s10838-008-9062-0

Pérez-Soì, C., & Herrera-Joancomartí, J. (2014). Bitcoins y el problema de los generales bizantinos. *RECSI 2014*. Retrieved from https://web.ua.es/en/recsi2014/documentos/papers/bitcoins-y-el-problema-de-los-generales-bizantinos.pdf

Petrasic, K., & Bornfreund, M. (2016). Beyond Bitcoin: The blockchain revolution in financial services. Retrieved April 18, 2017, from https://www.whitecase.com/publications/insight/beyond-bitcoin-blockchain-revolution-financial-services

Popper, N. (2015). Cash Call for a New Technology. *The New York Times*. New York. Retrieved from https://www.nytimes.com/2015/12/29/business/dealbook/cash-call-for-a-new-technology.html?_r=0

Preukschat, A. (2017). ¿Qué es un ICO? Así se gesta la salida al mercado de una criptomoneda. Retrieved April 22, 2017, from http://www.eleconomista.es/tecnologia/noticias/8070336/01/17/Que-es-un-ICO-Asi-se-gesta-la-salida-al-mercado-de-una-criptomoneda.html

Rizzo, P. (2017). 47 Banks Complete DLT Cloud Pilot With Ripple Tech. Retrieved April 29, 2017, from http://www.coindesk.com/47-banks-blockchain-complete-dlt-cloud-pilot-ripple-tech/

Robinson, E. (2017). BBVA Taps Blockchain to Make International Payments in Seconds. Retrieved April 29, 2017, from https://www.bloomberg.com/news/articles/2017-04-20/bbva-taps-blockchain-to-make-international-payments-in-seconds

Rutter, D. (2017). When is a blockchain not a blockchain? Retrieved April 29, 2017, from http://www.r3cev.com/blog/2017/2/24/when-is-a-blockchain-not-a-blockchain

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Tapscott, D., Salmerón Arjona, J. M., & Tapscott, A. (2017). *La revolución blockchain : Descubre cómo esta nueva tecnología transformará la economía global*. Retrieved from https://books.google.es/books/about/La_revolución_blockchain.html?id=TJ4ADgAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q

&f=false

Tham, E. (2017). China turns to blockchain to make markets clearer and cleaner. Retrieved May 2, 2017, from http://www.reuters.com/article/us-china-fintech-blockchain-idUSKBN15A368

Wilkins, C. (2017). Project Jasper: Lessons From Bank of Canada's First Blockchain Project. Retrieved May 1, 2017, from http://www.coindesk.com/project-jasper-lessons-bank-of-canada-blockchain-project/