

COLEGIO UNIVERSITARIO DE ESTUDIOS
FINANCIEROS

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS (ADE)

TRABAJO FIN DE GRADO



BLOCKCHAIN ¿UNA AMENAZA PARA
LA INDUSTRIA BANCARIA?

Autor: Laoud, Yassine

Tutor: Carbó Valverde, Santiago

Madrid, mayo de 2020

Índice

I.	Resumen	3
II.	Introducción	4
Capítulo 1: La tecnología <i>blockchain</i>		
1.1	Historia de la <i>blockchain</i>	6
1.2	Qué se entiende por tecnología <i>blockchain</i>	7
1.3	Principales características.....	8
1.4	Funcionamiento y principios básicos.....	10
1.5	Tipología	12
Capítulo 2: <i>Blockchain</i> , incursión en los negocios tradicionales		
2.1	<i>DLT (Distributed Ledger Technology)</i>	14
2.2	Modelo Bancario en “ <i>stand-by</i> ”	15
2.3	Principales Desafíos.....	16
Capítulo 3: De la teoría a la práctica		
3.1	<i>Hyperledger</i>	18
3.2	<i>Smart contracts</i>	18
3.3	<i>KYC (Know Your Customer)</i>	20
Capítulo 4: Principales aplicaciones		
4.1	Caso <i>Ripple (XRP)</i>	22
4.2	<i>Corda</i> , el consorcio R3.....	23
Capítulo 5: Nuevos modelos de negocio		
5.1	<i>Blockchain en España</i>	25
5.2	<i>Blockchain a nivel internacional</i>	26
III.	Conclusiones.....	29
IV.	Bibliografía.....	31
V.	Tabla de gráficos.....	33

I. Resumen

Estamos presenciando el progreso de una tecnología disruptiva que ha estado desarrollándose vertiginosamente en la última década, la *blockchain*. Podríamos compararla a un gran registro de almacenamiento de datos en el que se pueden anotar todas las transacciones llevadas a cabo en cualquier lugar del mundo. Dadas sus características, se estima que está dotada de un potencial extraordinario que podría suponer una revolución en todos los ámbitos, especialmente para el sector financiero.

A pesar de haber sido creada hace cerca de tres décadas, está sufriendo un proceso paulatino de integración dentro de la industria financiera, esencialmente en el sector bancario. Si bien se encuentra en una fase de madurez naciente, ya que ha empezado a aplicarse hace relativamente poco tiempo, resulta necesario plantearse si es capaz de garantizar la aportación de una metodología innovadora que supondría la metamorfosis de los prototipos de negocio actuales para evitar su sustitución y lentificar su obsolescencia. Sin embargo, el camino para que las expectativas sean reales es todavía largo, para que todo este potencial se haga realidad, es primordial que las autoridades normalicen su uso mediante su introducción en un marco legal vigente, además de aportar una mayor cantidad de evidencias y estudios exhaustivos que demuestren sus beneficios para su consagración.

Durante la inmersión en el universo de la tecnología de la *blockchain*, la cuestión relativa a las repercusiones que puede suponer con respecto a los servicios ofrecidos por la banca tradicional parecía inevitable. Juntos, descubriremos cómo funciona una cadena de bloques, remarcando sus principios de funcionamiento en general y observaremos el impacto que esta tecnología podría tener en el modelo bancario. Puesto que presenta una amenaza y una oportunidad a la vez para los bancos, apreciaremos la postura sustentada frente a esta supuesta revolución. Por último, conforme a sus utilidades, intentaremos aportar una contestación contundente al dilema que surge en relación con dicha tecnología, es la *blockchain*, ¿un riesgo real para los bancos?

II. Introducción

La *blockchain* se origina en el trabajo visionario y muy avanzado para su tiempo realizado por sus dos fundadores, Stuart Haber y W.Scott Stornetta en el año 1991. Al inicio, esta tecnología se desglosaba en una cadena de bloques encriptada que impedía a cualquiera alterar los documentos emitidos. A raíz de esto, realizaron avances significativos como por ejemplo con la introducción de los árboles de *Merkle*¹, que les permitió agilizar la recopilación de datos en un bloque único protagonizando una mejora de la eficiencia de dicho sistema.

Lo cierto es que la aparición del sistema *blockchain* no estaba diseñado para el uso corporativo en un primer tiempo. Efectivamente, debemos mencionar que, en realidad, el principal objetivo era crear mecanismos capaces de ordenar los archivos registrados de forma única y segura. En los años 1990, este invento representó una solución práctica de gran aceptación para el orden y manejo de documentos digitales con el fin de evitar modificaciones o manipulaciones.

Nadie hubiera imaginado que el descubrimiento de Internet pudiera cambiar nuestra existencia, sin embargo, hoy en día no podríamos considerar un mundo sin él. Quién sabe si pasará lo mismo con la cadena de bloques. La tecnología *blockchain* se está implantando poco a poco al seno de nuestras instituciones y demás, se caracteriza por ser una plataforma segura para la ejecución de transacciones. Estamos viviendo en un contexto dentro del cual la transparencia y la conformidad están siendo primordiales, en relación con este marco, el tránsito del conjunto de las operaciones se realiza con total nitidez, la información está al alcance de todos los miembros de la comunidad ya que carece de un sistema centralizado basando en la intermediación como los conocemos en la actualidad, con los organismos financieros. Estamos cada vez más cerca de presenciar uno de los cambios más significantes en el sector de los servicios financieros dado que está llegando a gran velocidad.

¹ Estructura de datos dividida en varias ramas tomando la forma de un árbol cuya finalidad es la de relacionar cada una de las máquinas que componen la red con una raíz única asociada a los mismos.

Nos estamos enfrentando a un mundo en el que la confianza está siendo la base de toda nuestra sociedad. Pilar básico para la cooperación tanto social como empresarial, es igualmente un problema cíclico al que se tiene que enfrentar el sector financiero dado que la incertidumbre es el enemigo jurado del ser humano. Debido a la crisis mundial del año 2008, las instituciones financieras encargadas de gestionar el dinero se han visto sumamente fragilizadas y sus limitaciones expuestas a todos y para todos. Como bien sabemos, las consecuencias han sido dramáticas y han conllevado a una pérdida de confianza generalizada por parte de los agentes económicos hacia el sistema. Pero entonces, ¿cómo funciona una economía que comporta unos actores económicos que no confían en sus instituciones? El sistema se colapsa.

Considerando este panorama subordinado al pánico, surge el *Bitcoin*, una solución alternativa al problema planteado anteriormente de la confianza, dado el hecho de que evita la intermediación tradicional para expandirse dentro de una cadena de bloques, tecnología que vamos a describir más detenidamente observando sus aportaciones para discernir, precisamente, si va a actuar como un sustituto o un complemento con respecto al sector bancario. Vamos a intentar averiguar si la *blockchain* se caracteriza por ser una solución contra las ineficiencias del banco, o bien, si se va a distinguir como un aliado con el que contar para la mejora de su competitividad.

Capítulo 1: La tecnología blockchain

1.1 Historia de la *blockchain*

Como consecuencia de la crisis mundial de 2008, los agentes económicos han perdido la confianza en las instituciones encargadas de gestionar el dinero, herramienta utilizada como unidad de cuenta, medio de intercambio y reserva de valor. ``La esencia del empresario es su estado de alerta que le permite descubrir en el mercado oportunidades no detectadas hasta entonces`` (Kirzner,I. 1973), así trató de proporcionar Satoshi Nakamoto una solución alternativa a la pérdida de confianza a través de la publicación de un manifiesto titulado: "Bitcoin: *A Peer-to-Peer Electronic Cash System*" en *octubre del 2008*, donde el autor propone una moneda 100% digital: *el bitcoin*. Desde la supuesta desaparición de Nakamoto, el desarrollo de su invento ha sido encargado a nuevos desarrolladores que han ido generando nuevas aplicaciones aportándole mayor utilidad y visibilidad.

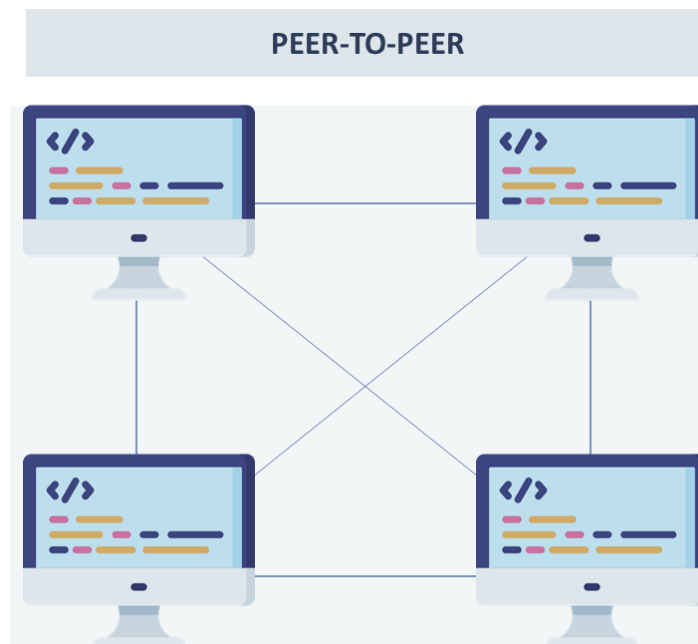
La historia del *blockchain* no es entendible sin la figura del *bitcoin*, ni la intervención de Satoshi Nakamoto que propició aportaciones vitales e innovadoras para el futuro desarrollo de la plataforma. Aunque no se sabe prácticamente nada de este individuo o grupo de personas, lo cierto es que no se le considera como el padre, sino el cerebro de esta tecnología. Su contribución ha supuesto una revolución dada la relevancia que tuvieron las criptomonedas en su auge, que dieron a conocer mundialmente a la *blockchain* ya que se basan en este sistema de registro digital.

Esta criptomoneda no dependería de una entidad o institución reguladora, sino que contaría con el apoyo de un nuevo protocolo de intercambio de información entre pares, liberándose así de la necesidad una autoridad central. Este es el nacimiento de lo que conocemos hoy en día como *Blockchain*, que en definitiva es un libro mayor de acaecimientos digitales que se comparte entre diferentes partes.

1.2 Qué se entiende por tecnología blockchain

La *blockchain*, es conocida igualmente como la cadena de bloques. En este contexto, el bloque refleja la información digital, y la cadena representa el proceso de almacenamiento de los datos digitales en la base de datos que es compartida entre los participantes de la red de manera transparente, por lo que todos pueden acceder a sus contenidos. La gestión de la base de datos se realiza de manera independiente utilizando redes punto a punto (*P2P*) *Peer-to-peer*, que es un tipo de conexión destinada a la comunicación entre aplicaciones. Permite a las participantes distribuir los archivos libremente sin la necesidad de una tercera parte y un servidor *timestamping* ó, de sellado de tiempo, un instrumento online que permite corroborar que una serie de datos han existido y no han sido alterados en un instante específico en el tiempo.

Figura 1: Ilustración de las redes punto a punto



Fuente: Elaboración propia

Cabe destacar que las cadenas de bloques solo pueden ser actualizadas por la aprobación de la mayoría de los integrantes de la red, a los cuales se les denomina nodos y que son en esencia un ordenador dispuesto para tramitar las transacciones de la red. Según Vitalik Buterin, presidente de la criptomoneda *Ethereum*, “la *blockchain* se desarrolla dentro de un

contexto descentralizado (no hay nadie que las controle) y arquitectónicamente descentralizadas (no hay punto central de fallo de infraestructura) pero están lógicamente centralizadas (hay un estado comúnmente acordado y el sistema se comporta como una sola computadora)”. La información proporcionada por dichas transacciones en ningún caso podrá verse alterada y tampoco puede ser borrada, por lo que *blockchain* se presenta como un registro inmutable y permanente.

Al ser una red compartida, donde cada nodo del sistema almacena una copia exacta de la cadena, se garantiza la disponibilidad de la información en todo momento. En caso de que un atacante quisiera provocar una denegación de servicio, debería anular todos los nodos de la red, basta con que al menos un 51% de ellos estén operativos para que la información esté disponible. “El sistema es seguro siempre que los nodos honestos controlan colectivamente más poder de unidad central de proceso que cualquier otro grupo colaborador de nodos atacantes. Si la mayoría de la potencia de la unidad central de proceso está controlada por nodos honestos, la cadena honesta crecerá más rápido y superará a cualquier cadena competidora. Para modificar un bloque anterior, un atacante tendría que rehacer la prueba de trabajo del bloque y todos los bloques posteriores, y luego alcanzar y superar el trabajo de los nodos honestos” (*Nakamoto.S, 2009*)

Estamos frente a una tecnología disruptiva que permite la transferencia segura de datos mediante una codificación muy avanzada y difícil de piratear. Se trata pues, de una especie de libro de registro distribuido punto a punto en el cual están registradas todas las transacciones, que, a diferencia de las operaciones actuales, no requieren la supervisión de un intermediario de confianza que desempeñe la labor de conservar y validar las operaciones.

1.3 Principales características

La cadena de bloques ha existido desde la década de los 90 como hemos comentado anteriormente, es una tecnología que ha sido apartada durante muchos años por lo que nunca se ha podido averiguar su utilidad, aunque en la última década se está intentando involucrarla en diversas actividades, este sistema tiene futuro más allá de la economía y de las finanzas. Podría englobar sectores tales como el sanitario o político, por ejemplo. A continuación,

hablaremos de las principales características enfatizando en ciertos conceptos expuestos en el apartado anterior:

Inmutabilidad: Es indiscutiblemente una de las características fundamentales que compone la tecnología *blockchain*. Cabe recordar la función que realizan los nodos para crear un registro no sin antes verificar su validez. Una vez dicho registro adjuntado, no puede ser cambiado o alterado. Ayuda a garantizar que la tecnología se mantenga como está: una red permanente e inalterable.

Autoridad descentralizada: Al ser una red distribuida, prima por la inexistencia de una autoridad que la supervise o de una persona que la gobierne. Es una característica muy importante que ha dado sus frutos ya que todos los nodos tienen la misma jerarquía en cuanto al control de información, por lo que todos vigilan a todos.

Seguridad: La criptografía se consolida como un aval de cara a la protección de datos por parte de los usuarios. Al ser un algoritmo matemático, toda la información en la *blockchain* se somete a ser cifrada criptográficamente por lo que cualquier dato en la red tiene un valor diferente. En definitiva, se podría considerar como una identificación única para cada documento.

Consenso: Los millones de nodos son los encargados de, entre otras funciones, validar transacciones. Se trata de un proceso de toma de decisiones conjunta para el grupo de nodos activos en la red, en el cual, dado la magnitud de componentes, esta característica es imprescindible para velar sobre el buen funcionamiento de la red. El consenso es el responsable de que no se necesite confianza dentro de la red.

Rapidez: Las características que acabamos de ver propician que la cadena de bloques sea más eficiente en términos de plazos, frente a los sistemas bancarios tradicionales. En este apartado es imperativo tratar de los *Smart Contracts* ó, contratos inteligentes, que permiten realizar acuerdos más rápidos para cualquier tipo de contrato. Este es uno de los mejores beneficios que ofrece la cadena de bloques hasta el día de hoy y que trataremos más detenidamente en el tercer capítulo.

1.4 Funcionamiento y principios básicos

En el fondo, es un registro de transacciones, funciona como un libro de contabilidad tradicional. Estas operaciones se pueden resumir en movimientos de dinero, bienes o datos. Abarcaría operaciones corrientes de uso diario, como podría ser una compra en la farmacia, y operaciones más complejas tales que, por ejemplo, la asignación de un número de identificación para votar en las elecciones. Está diseñado para almacenar información de una manera que hace virtualmente imposible añadir, eliminar o cambiar datos sin ser detectado por los demás usuarios. A continuación, entraremos en más detalle sobre cómo alcanza la cadena de bloques dichos estándares.

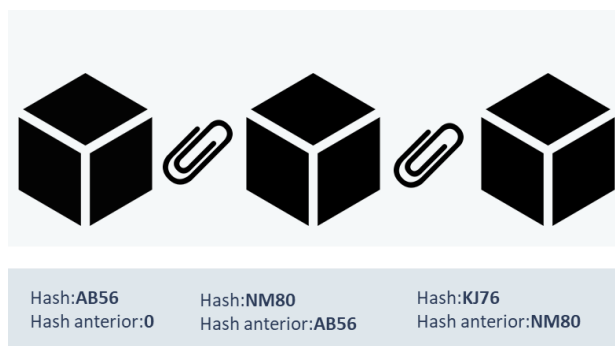
En la actualidad, las transacciones están sometidas a una revisión y aprobación por parte de una institución dentro de un sistema centralizado. Las aplicaciones de cadenas de bloques podrían sustituir estos sistemas centralizados por otros descentralizados, en los que la verificación se realiza, como hemos avanzado anteriormente gracias al consenso que existe entre usuarios heterogéneos. Simplificando, una cadena de bloques necesita hacer dos cosas, básicamente: recopilar datos para ordenarlos en bloques y luego, vincularlos de forma segura usando la criptografía. Supongamos que estamos al seno de una transacción entre dos personas, X e Y, la información de dicha transacción se registra y se comparte con todos los ordenadores que conforman la red de cadenas de bloques. En el seno de la red, el registro se amolda junto con otras operaciones en un bloque dentro de una base de datos en la cual cada transacción está tramitada con fecha y hora. Como toda la información es secuencial, se evitan entradas duplicadas. El bloque completado se envía a través de la red, donde se añade a la cadena. Si se da la casualidad de que otros usuarios de la red están enviando bloques al mismo instante, el *timestamping* hace que se registren de manera coordinada proporcionando igualmente las versiones más recientes de los archivos.

La clave para entender el sistema de seguridad de la cadena de bloques son los denominados *hash*². Es una especie de matemática criptográfica que hace que los vínculos entre los bloques sean virtualmente incorruptibles ya que están compuestos por una cadena única de caracteres. El *hash* de un bloque se añade a los datos del siguiente bloque aportando una evidencia

² Estas funciones tienen como objetivo primordial codificar datos para formar una cadena de caracteres única. Sirven para asegurar la autenticidad de datos, almacenar de forma segura contraseñas, y la firma de documento electrónicos.

rastreada en el nuevo *hash* y así continuamente a lo largo de la cadena. De este modo se consigue reforzar la seguridad ya que, si se hay un intento de pirateo sufrido por un bloque, el *hash* codificado en el siguiente bloque no será válido.

Figura 2: Ilustración de un *hash*



Fuente: Elaboración propia

Como sabemos, todos los participantes están informados acerca de las operaciones que se realizan dentro de la *blockchain* por lo que estarán alertados en el caso de detectar una irregularidad. Los operadores confían en sus registros siempre que los *hashes* coincidan y sean validados a lo largo de toda la cadena.

Es cierto que encontramos en la actualidad ordenadores muy potentes capaces de recalculan millones de *hashes* rápidamente, es por lo que el sistema de la cadena de bloques utiliza algoritmos tales que *PoW (Proof of Work)*³ para calcular los hashes de cada bloque. Aun así, hackear la *blockchain* con éxito es una cuestión que no preocupa a todos los usuarios al tratarse de un proceso muy costoso, se estima que costaría cerca de trescientos mil dólares para conseguir infiltrarse durante unos cincuenta segundos. A parte el gasto en el que se incurriría, no le sería rentable a ninguno intentarlo puesto que será identificado como un intruso cuyo motivo aparente sería el de paralizar las operaciones para conseguir una devaluación de la moneda provocada por una caída del tipo de cambio.

³ “*Proof of work*, coloquialmente conocido como «proceso de minado», que implica la resolución de problemas computacionales complejos para la validación y creación de cada nuevo bloque de la cadena.” (Banco de España, 2018)

1.5 Tipología

Dada la idiosincrasia de la *blockchain*, asumiremos que se pueden formar diversos registros cuyas características divergen. A continuación, expondremos tres tipos de cadenas de bloques que procederemos a explicar.

Blockchain pública

Esta es la opción en la que todos pensamos al hablar de esta tecnología: una cadena de bloques distribuida y accesible para cualquier usuario del mundo, resistente a la censura y la manipulación. Por establecer una semejanza sencilla de interpretar, sería un modelo parecido al de Internet, en el que un solo agente no tiene control sobre todo lo que se produce ya que cada una de las personas y empresas que participan de la Red tienen poder sobre sí mismos y sus propias páginas web.

El procedimiento para acceder es muy simple, se trata de descargarse la aplicación correspondiente y conectarse. A continuación, se exige a un determinado número de nodos de forma automática, la versión más actualizada de la cadena. Una vez el nodo está actualizado, tiene los mismos derechos y deberes que el resto de los participantes a la hora de proponer y validar transacciones (minar)⁴.

En general estas redes son transparentes, los usuarios son anónimos y ningún participante tiene más derechos que los demás, motivo por el cual carece de administradores. Las redes públicas más conocidas son *Bitcoin* y *Bitcoin Cash*.

Blockchain Privada

Las *Blockchains* privadas son establecidas por parte de una empresa o un particular, que será la encargada de gestionar el acceso hacia los registros de las transacciones a determinados usuarios. Para su participación, se requiere una invitación a los operadores, que deberá ser validada a su vez por la red en cuestión. Se trata de una red autorizada que restringe el acceso para quien quiera unirse. Las cadenas de bloques privadas también pueden restringir la

⁴ "Minar bitcoins es el proceso de invertir capacidad de computacional para procesar transacciones, garantizar la seguridad de la red, y conseguir que todos los participantes estén sincronizados" <https://bitcoin.org/en/>

actividad de los usuarios, de modo que ciertas transacciones sólo pueden ser realizadas por unos y no por otros, a pesar del hecho de formar parte de la red.

Este tipo de *blockchain* resultan ser extremadamente útiles cuando se esté trabajando con datos confidenciales tales que las cuentas de la empresa, acuerdos entre entidades, la gestión de carteras...Al fin y al cabo son operaciones que contienen informaciones delicadas por lo que conviene que no estén disponibles para cualquier persona. Esta tipología de cadena de bloques se constituye a partir de un nodo central, en el que recaerá las funciones de supervisión y validación de las operaciones puesto que la red estará completamente sometida a la censura y al dominio que su propietario quiera ejercer, con el objetivo de ajustarse mejor a los estándares de transparencia, seguridad y privacidad exigidos por las autoridades legislativas. Finalmente, las decisiones relativas a su visibilidad y apertura para el público, junto con las tareas de gestión y almacenamiento de los datos, estarán en manos de su propietario.

Blockchain híbrida

Las *blockchains* híbridas están entre medias de los dos modelos expuestos anteriormente, la mejor manera de definirla sería considerarla como una especie de cadena de bloques privada pero un poco pública a la vez. Esta combinación surge como consecuencia de la necesidad de flexibilizar las redes existentes para favorecer su aparición en otros sectores en los que se acopla con mayor naturalidad, puesto que se caracteriza por emitir información en exclusividad tanto para los nodos autorizados como para los no autorizados, y es, al mismo tiempo, una red descentralizada donde varios nodos son los gerentes, por así decirlo. Esto se traduce en la instauración de un consorcio de empresas, dentro del cual el poder no recae en una institución, sino que está gobernada por el liderazgo de una colectividad. Este sistema ofrece la posibilidad de disminuir las posibilidades de manipulación y ser más eficiente en el proceso de validación de las transacciones. Los proyectos basados en esta tecnología que cuentan con mayor visibilidad que los demás podrían ser *Hyperledger* (de la Fundación Linux) y *R3* (un consorcio de bancos internacionales para desarrollar actividades y soluciones bancarias relacionadas con la *blockchain*) que procederemos a explicar en los siguientes capítulos.

Capítulo 2: *Blockchain*, incursión en los negocios tradicionales

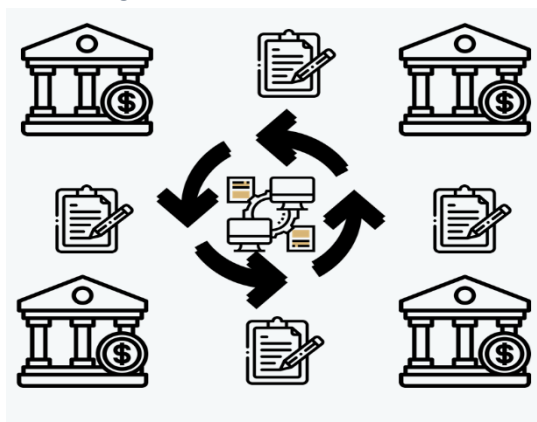
2.1 *DLT (Distributed Ledger Technology)*

Hay una cierta confusión que se ha creado acerca de la *blockchain* y la *DLT (Distributed Ledger Technology)* ya que se tiende a pensar que son, en esencia, la misma tecnología. Digamos que es más sencillo de lo que parece, para simplificar, diremos que la cadena de bloques es un tipo de tecnología de registros distribuidos aclarando que no todas las *DLT* son una *blockchain*.

La tecnología de registros distribuidos está siendo un foco de atención en los últimos años después del auge de las criptomonedas, que acabó atrayendo la atención del sector financiero, tanto por su uso en operaciones con criptoactivos como por el desarrollo de iniciativas que prometen incrementar la eficiencia, transparencia y velocidad de algunos de los procesos que derivan de las transacciones financieras.

Un registro distribuido es una base de datos única y descentralizada que se gestiona a través de todos los participantes. En conclusión, es una base de datos compuesta por múltiples copias idénticas que están distribuidas entre varios participantes y que se actualizan de manera sincronizada.

Figura 3: Ilustración de una *DLT*



Fuente: Elaboración propia

Los *DLTs* pueden ser usados en el sector financiero para crear registros distribuidos que puedan finalizar acuerdos comerciales sobre cualquier activo financiero, supervisadas por una autoridad. Entendemos que, al ser distribuida, no existe confianza total entre las partes por lo que, una figura supervisora será la encargada de distribuir y verificar colectivamente los registros antes de compartirlos.

Podemos afirmar que las *DLTs* proporcionarían una mayor trazabilidad y transparencia de las transacciones, requisito para cualquier entidad legalizada para que pueda llevar a cabo un mejor seguimiento de las operaciones de sus clientes, modalidad que no está siempre disponible en otros sistemas tradicionales. Se le añade a dicha ventaja la posibilidad de que cada uno de los participantes comparta solo aquella información que considere oportuna, usando el método de encriptación o mediante canales alternativos.

Los bancos no tienen más remedio que reaccionar y apropiarse de esta tecnología para no verse superado frente a competidores cada vez más innovadores que pretenden complicar el futuro panorama del sistema bancario tradicional. A continuación, vamos a observar el uso de la *blockchain* en el sector financiero para finalmente observar cómo se han ido preparando los bancos para no estar en una postura desventajada.

2.2 Modelo Bancario en “*stand-by*”

Hemos estado estimando el alcance que va a tener esta tecnología en los próximos años puesto que es una apuesta en la que se nos ofrece más independencia y una forma de libertad. Esta emancipación nos permite ser nuestro propio banco, puesto que cada canal privado está sometido a su propio *token*, ficha en español, es decir, “una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas” (Mougayar.W, 2017)⁵. Por consiguiente, tendríamos la posibilidad de intercambiar cualquier bien, producto o contrato con total normalidad. Esta libertad que se nos ofrece hace que el sistema financiero, particularmente los bancos, se encuentran en una situación incómoda y se ven en la obligación de replicar acaparando esta tecnología para introducirla dentro de su modelo de negociación para evitar que surjan nuevos competidores que podrían ocasionar la pérdida masiva de clientes inventivos que pretenden venir y exponerles ante una situación que podría ser límite el sistema bancario tradicional.

El sector financiero ha destacado por su atracción hacia esta nueva tecnología por lo que ha sido un pionero en adoptarla, en gran parte debido a su potencial que nos permitirá irremediablemente simplificar la ejecución de las operaciones incurriendo en una reducción

⁵ Mougayar, William A Business Guide to Token Usage, Utility and Value (2017)

sustantiva de los costes (operacionales, de transacciones, de riesgo...) al limitar el número de terceros. Con la cadena de bloques, nos aseguramos de que nuestros datos y nuestras operaciones sean tramitadas de manera segura y transparente. `` La cadena de bloques constituye una tecnología innovadora capaz de ayudar a las entidades financieras y otros agentes de la industria a reforzar los criterios de transparencia, divulgación y declaración de información relevante. De una primera valoración, se estima que la aplicación de la *blockchain* puede llegar a suponer un ahorro para las entidades financieras de alrededor \$20 mil millones al año en operaciones de liquidación, pagos transfronterizos y asuntos reglamentarios``. (Fanning & Centers, 2016)

Por otra parte, la tecnología *blockchain* todavía no está sometida a las mismas regulaciones internacionales, existe un vacío legal que puede ser una desventaja para el sector bancario ya que podría verse severamente afectado. Pero por otro lado, si es legalizada, se convertiría en una magnífica oportunidad para abarcar una transición dentro de la transformación del sector de la banca, convirtiéndolo en una industria de cooperación entre instituciones de servicios financieros y empresas de *Fintech*, abarcando la aparición modelos de negocios innovadores evolucionando hacia una banca más competitiva. Sus beneficios con relación al sector bancario son los siguientes:

- Elimina cualquier frontera geográfica
- Ejecuta y tramita las transacciones con mayor rapidez
- Reducción de costes
- Control participativo sobre las transacciones realizadas en el cuadro de una *blockchain* descentralizada.

2.3 Principales Desafíos

Las bases de datos de cadenas de bloques crecen rápidamente en tamaño a medida que se añaden nuevas operaciones. Como consecuencia, existe la preocupación de que se ralentice la velocidad de procesamiento del sistema, lo que deteriora sus aspiraciones de eficiencia con las que fue ideado y concebido. Esta presunta pérdida de rapidez puede transformar la *blockchain* en inapta para ciertas formas de transacciones en las que la velocidad es esencial.

En este sentido, la resistencia de una cadena de bloques es de una importancia capital, especialmente cuando el servicio se utiliza como parte de la capacidad de una institución financiera para cumplir con las obligaciones de negociación y las interacciones con los clientes.

El segundo desafío de la *blockchain* está relacionado con un asunto bastante delicado, la privacidad. Recordemos que una de sus principales características, la inmutabilidad, puede entrar en conflicto con el derecho al olvido y la privacidad, al impedir la actualización o supresión de la información registrada en la cadena de bloques sin un previo acuerdo de las partes implicadas.

El problema radica en las cadenas de bloques de carácter público, aunque se supone que cada uno es propietario de sus propios datos y que las empresas necesitan nuestro consentimiento para hacer uso de ellos, es un concepto que no cabe en dicha tecnología debido a su naturaleza. Surge un riesgo importante en cuanto a la privacidad, si bien no existe nombres, ni un número de identificación con la que estés directamente relacionado, da la casualidad de que todavía pueden rastrear tu dirección *Internet Protocol* y por consiguiente ser identificado en contra de su voluntad con lo que hay un riesgo importante en cuanto a privacidad. Nos enfrentamos a un dilema puesto que los propios procesos que conforman la validación de transacciones efectuadas en la cadena de bloques deben estar disponibles para los participantes de la red o, al menos, para los que se encargan, precisamente, de validar operaciones. De no ser así, el consenso se rompe.

El tercer desafío al que se va a oponer la *blockchain* hace referencia a la falta de comunicación entre plataformas del mismo sistema. Si bien la cadena de bloques puede almacenar millones de datos, existe una diferencia en los lenguajes de programación y codificación entre sus diversos programas lo que supone la falta de interoperabilidad existente en el sistema. Es evidente que, si esta tecnología no se puede acoplar a los sistemas de explotación subyacentes a su sector de actividad, será de poca utilidad. Hace falta una estandarización de las distintas plataformas ya que no existen estándares de mercado, para que las empresas puedan actuar conjuntamente colaborando en nuevos proyectos y el desarrollo de aplicaciones con el fin de alcanzar un mayor grado de competitividad.

Capítulo 3: De la teoría a la práctica...

3.1 *Hyperledger*

Hyperledger fue iniciado en diciembre de 2015 por la Fundación *Lynux* cuyo objetivo es perfeccionar la tecnología de la cadena de bloques para que sea aplicable a múltiples sectores mediante el desarrollo de distintas redes *blockchain*. Es un proyecto de alcance mundial que cuenta con la colaboración de más de 200 compañías (*J.P. Morgan, Intel o Thompson Reuters*) de una gran variedad de sectores tales que el bancario, el tecnológico, la cadena de suministros y los medios de comunicación. El proyecto más conocido, atribuido al sector bancario es el *Hyperledger Fabric*, compuesto de un sistema capaz de procesar más de mil transacciones por segundo. Adicionalmente, está dotado de una mayor utilidad para la creación de aplicaciones dedicadas a las actividades comerciales basadas en la tecnología de cadena de bloques.

La plataforma *Hyperledger Fabric* está basada en una *blockchain* privada y es una implementación de los registros distribuidos (*DLT*) que ofrece seguridad, escalabilidad, confidencialidad y rendimiento de red listos para el uso empresarial. A diferencia de una red pública sin permiso, los participantes no son anónimos y se conocen entre sí. En el caso de que no haya un vínculo de confianza entre ellos, ya que podemos imaginar estar presentes en un escenario en el cual dos empresas que compiten en el mismo sector, la red podría aportar la solución mediante la delegación de la autoridad de control y supervisión a un modelo de gobernanza como consecuencia de un previo consenso para erradicar la falta de certidumbre.

3.2 *SMART CONTRACTS*

Los *Smart Contracts* se caracterizan por ser una de las aportaciones más esperanzadoras de cara a la tecnología de los registros distribuidos (*DLT*). Están redactados en líneas de códigos que se basan en la criptografía y se diferencian de un contrato normal en que se ejecutan de manera automática en el caso de que suceda una acción predeterminada, lo que nos proporciona una mayor eficiencia puesto que perdemos menos tiempo en revisar la información y las cláusulas que conlleva. Estas acciones se deben programar de antemano ya

que el uso de estos contratos está sometidos a una verificación automática basada en una especie de clausulado, "Si sucede A, entonces B". Un ejemplo práctico podría ser el pago de intereses de un préstamo, tanto el prestamista como el prestatario son conscientes que llegada una determinada fecha que ha sido previamente fijada, se garantiza que, llegado al vencimiento, el contrato se liquidará sin la necesidad de ninguna orden, se cederá el importe establecido al deudor.

Entrando en el sector financiero, los contratos inteligentes pueden facilitar la realización en mayor medida de transacciones automáticas, como por ejemplo el pago de intereses, el pago de cupones o dividendo, la liquidación de operaciones, automatización de pagos y donaciones. Todas estas transacciones tendrán lugar en la *blockchain* y se ejecutarán como respuesta a una acción determinada que conlleva la finalización de un contrato inteligente. Su funcionamiento está condicionado ya que está sujeto a la tecnología de la cadena de bloques, para cualquier operación que se realice, su validación será tramitada por el conjunto de nodos que conforman la red como hemos visto anteriormente, es decir, por el consenso de los participantes. Estos nodos serán los encargados de proteger a las *DLT's* actualizando continuamente los bloques ubicándola fuera del alcance de ataques cibernéticos y evitando, de la misma manera, posibles intrusiones. Recordemos que los atributos de la cadena de bloques constituyen su principal aval puesto que una de sus funciones es la de conferir una transparencia extrema a las operaciones, por consiguiente, es de manera simultánea una prueba para la entidad que le permite evidenciar el cumplimiento de ley frente a los instituciones u organismos reguladores.

Si bien los contratos inteligentes han despertado la curiosidad de las grandes empresas, surgen serias dudas acerca de su validez en el futuro, puesto que no está claro si cumple con la definición de "contrato" desde un punto de vista legislativo y jurídico, legislar antes de tiempo puede suponer un avance considerable en este terreno, despejando dudas e incertidumbre, le haríamos un favor muy grande a esta tecnología. En la actualidad, para la realización de un contrato, se necesita el suceso de varios acontecimientos que vienen recogidos en el artículo 1261 del Código Civil, en el cual "se especifica que los contratos celebrados mediante dispositivo automático hay consentimiento desde que se manifiesta aceptación", en el caso de que una de las partes no cumpla con lo pactado, el contrato se

declara como nulo. Se caracteriza igualmente por el hecho de la supresión de la acción declarativa frente a un juez, puesto que esas acciones están automatizadas. En el caso de la celebración de un contrato de compraventa de cualquier bien o activo, si se da la eventualidad de que una de las partes esté en la obligación de cumplir ejecutando el pago de dicho activo, y que la otra parte no cumpla entregando el bien en cuestión, no haría falta acudir frente a un juez puesto que el contrato está programado para llevar a cabo directamente la condena a la parte que se ha negado a cumplir con su parte.

En definitiva, afirmaremos que los contratos inteligentes pueden usarse como un sustituto para ciertas operaciones, por lo que juegan un papel importante en la contribución a la reducción de terceros suponiendo una amenaza para la industria financiera. Sin embargo, representa igualmente una ventaja para dicho sector ya que cabe la posibilidad de que se acaben integrando en el modelo de negocio bancario. Los principales fundamentos sobre los cuales se basarían los agentes a la hora de valorar sus aportaciones, sería la seguridad y exactitud a la hora de ejecutar operaciones, y la reducción drástica en gastos que deriva de un trato *win-win* para todas las partes puesto que, según *Capgemini*, 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. 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”.

3.3 Know Your Customer KYC

Naturalmente, las empresas estarán interesadas en conocer a sus clientes, por una parte, porque les proporcionan un *feedback* sobre el cuál se irán basando para ir mejorando y renovando el conjunto de sus servicios. Por otra parte, este estudio les permite igualmente protegerse de cara a la ley ya que estarían certificando que todo el trabajo realizado al seno de la institución es legal. En relación con el sector financiero, las políticas de *Know Your Customer* o Conoce a tu cliente nunca han sido tan de actualidad como en los últimos años hasta el punto de convertirse en imprescindibles dentro del combate de las autoridades contra

las operaciones de lavado de dinero (*“Anti-Money Laundering” or AML*) que incluyen operaciones tales que la corrupción, la financiación de filiales pertenecientes a células terroristas o la evasión de impuestos.

Sin embargo, debido a la amplia gama de formalidades bajo *KYC*, el protocolo se alarga y se convierte en un proceso realmente cansino e ineficiente para la empresa. Adicionalmente, otro factor importante para tener en cuenta en la ejecución de estos procesos es la experiencia del cliente. Considerando toda la información y documentos certificados que las entidades financieras deben analizar, se hace necesario solicitar continuamente a los clientes que faciliten la misma información. Tampoco deberíamos olvidarnos de abarcar la complejidad de dicha política ya que hace que sea muy costosa, de hecho, según las estimaciones de KPMG, más de 25.000 millones de dólares se destinan a la gestión de riesgos por delitos financieros en el sector bancario, de los cuáles, la mayoría se consumen en los procesos de *KYC*.

No obstante, la tecnología que estamos experimentando intercambia cualquier cosa de valor online de una manera anclada y verificada puede ser fundamental de cara a la aportación de grandes soluciones para los problemas planteados anteriormente ya que el uso de la cadena de bloques para reducir las ineficiencias en el proceso *KYC*. El compartido de información y recursos con el resto de las entidades financieras se realiza con el fin de incluir las identificaciones digitales de todos los clientes lo cual supondría una bajada sustancial en los costes de hasta un 20% evitando que se repita el proceso periódicamente.

Destacamos, por lo tanto, tres funciones esenciales que se realizan en la creación de una identidad digital; se efectúa en primer lugar la recopilación información completa del cliente que es comprobada en la red gracias a sus antecedentes para finalmente llevar a cabo un control sobre sus datos para actualizados en consecuencia. Esta identidad debe ser única, y sólo se entregará al cliente una vez se hayan completado todas las comprobaciones establecidas en el proceso *KYC* para ser añadida después a la *blockchain* y transferida a continuación a todas las instituciones autorizadas que la soliciten. Dado que los bancos tratan con un gran número de clientes de distinto tamaño, con el fin de asegurar el proceso, se adoptó un sistema de base de datos descentralizada, que precisamente es la que nos permite recuperar la información del cliente de fuentes anteriores.

Capítulo 4: Principales aplicaciones

4.1 Caso Ripple (XRP)

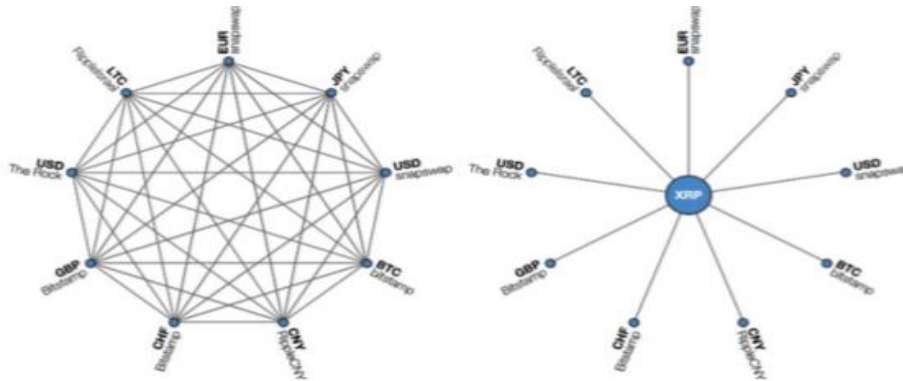
¿Porqué *Ripple* es la aliada perfecta para los bancos? La empresa *Ripple Labs* que conocemos hoy en día fue concebida en 2004, aunque fue descubierta por el mundo casi una década más tarde en el año 2012, en el cual se realiza la introducción de su criptomoneda *ripples* (XRP), una de las más importantes del mercado en la actualidad. En líneas generales se diferencia por ser un prototipo encargado de proveer servicios de pagos y liquidación de distintas divisas, y, además, es una *blockchain* cerrada y creada específicamente para este sector que provee una experiencia óptima para enviar dinero con un alcance mundial ya que *Ripple* conecta bancos y plataformas internacionales de intercambio de activos digitales.

Deducimos que *Ripple* es un sistema de pagos virtual que se basa en una tecnología similar que al resto de las criptomonedas pero con unas ciertas características divergentes que han llamado la atención de la industria financiera, su propuesta de valor se basa en un sistema global integrado por más de 200 usuarios, entre los que figuran entidades financieras como es el caso del Banco Santander y del BBVA en España, de Barclays en Inglaterra, ING en los Países bajos, American Express en EEUU etc...Una de sus principales características es el número de tokens que son emitidos, ya que no existe un proceso de emisión de nuevas monedas a través del minado, como es el caso del *bitcoin*, por ejemplo. Como consecuencia, la cantidad de monedas de *Ripple* está limitada y eso permite que su precio sea más estable, un factor clave para las entidades bancarias, aunque carezca de valor por sí misma ya que según sus creadores, se trata de una “moneda puente” para el intercambio de divisas fiduciarias.

Por otra parte, *Ripple* destaca por la rapidez en la ejecución de operaciones lo que permite a las instituciones financieras recortar costes y liquidar transacciones en menos tiempo en comparación con el sector bancario. Se estima que estas operaciones se pueden liquidar a una velocidad de entre 5 y 15 segundos gracias a esta criptomoneda, sin olvidarnos del gran volumen de negociación de la que es capaz ya que procesa hasta 1.000 operaciones por segundo. Gracias a la cadena de bloques, además de rapidez, esta criptomoneda puede ofrecer los organismos que apuesten por esta tecnología transparencia y seguridad en el desarrollo

de sus actividades, lo que propiciará según un estudio del banco Santander, un ahorro en costes bancarios de hasta 25.000 millones de euros anuales.

Figura 3: Ilustración Ripple



Fuente: <https://ripple.com/>

4.2 Corda, el consorcio R3

El mundo de las finanzas y la industria bancaria se han interesado detenidamente a esta tecnología, dado que los bancos han sido unos pioneros debido a su esfuerzo realizado para entender su operatividad con el fin de incorporarla para aprovecharse de todas las ventajas que presenta. Sus aplicaciones fueron el detonante que convencieron a los bancos para proyectarse mediante su adopción y trabajar en actividades concretas. Con el afán de no ceder parte de su cuota de mercado al ser adelantado por sus competidores con la apropiación y el uso de un segmento de su modelo de negocio, se ha creado *Corda*.

Es una plataforma de código abierto que subyace de las *DLT's (Distributed Ledger Technologies)* creada por el consorcio R3⁶ en el año 2014, para anotar, administrar y unificar acuerdos financieros entre organizaciones legalizadas. A continuación, expondremos sus características que se asemejan con las tecnologías de la *blockchain* privada, aunque cabe reflejar que es un proyecto independiente cuya intención es hacer posible que una amplia gama de aplicaciones interopere en una misma red, con la finalidad de satisfacer las necesidades de los negocios actuales, visto que está siendo especialmente concebida para el

⁶ La R3 (*R3CEV LLC*) es una empresa de investigación financiera y tecnológica ubicada en Nueva York. Lidera el consorcio de más de 70 empresas financieras globales en la esfera de investigación y desarrollo de las tecnologías de la *blockchain* en el sistema financiero. <https://www.r3.com/>

sector financiero. En el caso de que se quiera celebrar un contrato entre dos o más entidades a través de esta plataforma, el contrato no permanecería registrado en un bloque disponible para todos los demás participantes, sino que se trata de un contrato individual. De esta manera, los datos son enviados exclusivamente a las partes interesadas, aunque estén encriptados. Las principales funcionalidades de *Corda* son:

- **Confidencialidad:** El acceso a los datos es restringido, sólo será accesible a aquellas instituciones participantes que han sido legitimadas, la difusión de la totalidad de los datos se realizará hasta alcanzar unos estándares mínimos requeridos para su funcionamiento. El consenso que se logra es entre empresas y a nivel de acuerdos bilaterales o comunes, pero bajo ningún supuesto será regido por algún sistema.
- **Red distribuida:** Al ser una herramienta descentralizada, el flujo de operaciones que se realizan por parte de las diversas empresas es coordinado sin la necesidad de un intermediario o ente central.
- **Estandarizada:** La plataforma está basada en instrumentos derivados de operaciones comunes emprendidas por el mundo de la banca y de la industria financiera en líneas generales, lo que hace que sea compatible con varios mecanismos de consenso.
- **Trazabilidad:** Debido a la configuración peculiar de la plataforma, las labores que nacen de la necesidad de mantener su buen funcionamiento mediante la supervisión y regulación de datos son efectuadas por el conjunto de nodos que forman la red. *Corda* solo permite compartir las operaciones revisadas y está dentro de sus posibilidades el hecho de interpretar la relación directa que se evidencia entre documentos relacionados.
- **Carece de Criptomoneda:** Dado el fin con el que *Corda* se ha creado, no existe la necesidad de desarrollar una criptomoneda nativa porque, hasta prueba de lo contrario, resultaría ser de escasa utilidad.

Podemos concluir este apartado observando que la principal diferencia que existe entre este programa y la *blockchain* (privado y público) reside los procesos de consenso y validación de los datos. En efecto, las características de *Corda* hace que cuente con unos estándares más exigentes que tratan de velar por la privacidad de los acuerdos como contrapartida de la confianza otorgada por parte de las compañías que emplean dicha tecnología.

Capítulo 5: Nuevos modelos de negocio

5.1. La *blockchain* en España

En abril de 2018, Banco Santander anunció el lanzamiento de una nueva plataforma de pago, denominada Santander *One Pay FX*. Dirigido a clientes en España, Reino Unido, Brasil y Polonia, es un nuevo servicio de *blockchain* que utiliza la tecnología de *Ripple* para acelerar la liquidación de las transferencias internacionales de dinero. Un año después, se firmó un acuerdo con IBM para usar sus tecnologías (*blockchain*, inteligencia artificial y *big data*), y se anunció de manera interna el lanzamiento de una extensión de estos servicios para su clientela ubicada en América Latina. Los resultados de esta implantación fueron satisfactorios dado el aumento del volumen de operaciones en la red. Su irrupción dentro del sistema financiero español ha causado una gran repercusión, hasta tal punto ha sido recompensado el premio *“Distribution & Marketing Innovation Awards 2018”* de *Accenture* y *Efma*, con el galardón *‘Silver Award’*.

Además del banco Santander, hablaremos del banco que cuenta con el mayor número de clientes digitales dentro del mercado bancario en España. La Caixa pasó a formar parte de las entidades asociadas a *we.trade*, una plataforma digital creada por nueve bancos: Santander, Deutsche Bank, Unicredit, KBC, Natixis, Rabobank, Nordea, Société Générale y HSBC. Su puesta en marcha se ha realizado en base a la *blockchain* utilizando *Hyperledger Fabric*, es más intuitiva ya que ofrece a los clientes del banco una interfaz de usuario fácil de usar para supervisar las operaciones. El programa *we.trade* se dirige principalmente a las pymes y a las microempresas puesto que proporciona financiación comercial para la cuenta corriente, como el anticipo de facturas, para mejorar el flujo de caja. Los demás servicios provisionados serán el protocolo *KYC*, el cierre de acuerdos comerciales en tiempo real entre dos operadores y el seguimiento y localización en vivo de las transacciones efectuadas.

Trataremos a continuación del proyecto Alastria que nace a mediados del 2017 y que hoy en día cuenta con una multitud de socios ya que podemos encontrar desde entidades financieras, instituciones públicas hasta pymes, por ejemplo. Algunas de estas empresas forman parte del *Ibex35* y resultan ser de suma importancia para la economía española, destacamos Telefónica, BBVA y Banco Sabadell. Es anunciado como un proyecto pionero al plantear la

cooperación entre compañías competidoras, declara su apoyo incondicional para la “democratización de la *blockchain*” contribuyendo mediante la elaboración de informes para que estén al alcance de un mayor colectivo con el fin de dar a conocer las ventajas que ofrece, además de crear plataformas multisectoriales que faciliten su acceso para fomentar su uso por los diversos agentes sociales y económicos. El principal objetivo es de incentivar la economía digital en las pymes, que son vitales para el desarrollo del proyecto puesto que representan el 45% de sus colaboradores. En España, este tipo de empresas juegan un rol capital dentro de la economía que está compuesta en su totalidad por un 98,8% de pymes.

Gracias al potencial de la tecnología *blockchain* en la que se va a basar esta plataforma, los operadores van a beneficiar de la colaboración entre las entidades para crear nuevos modelos de negocio o proyectos de una amplia diversidad con total transparencia y seguridad. Para todo ello, se necesita un proceso estandarizado para que se trabaje a partir de una base común. La red Alastria tendrá un papel muy importante dentro de este protocolo actuando de nexo entre los socios ofreciendo una red para la ejecución de las transacciones, pero se encarga igualmente de legalizar el proyecto ya que la tecnología de la cadena de bloques carece de una regulación específica como hemos dicho anteriormente. En este contexto, la red cuenta con la participación de instituciones jurídicas que anhelan por promulgar una serie de leyes dentro del cuadro de un registro que se somete a la regulación española.

Debido a la magnitud del proyecto, el presidente de Alastria se sinceró diciendo que “No es sencillo que tantas compañías de tanta relevancia decidan apostar juntas por un proyecto desde su mismo nacimiento. Esa es la mejor muestra del increíble potencial que tienen tanto esta tecnología como el consorcio. Debemos sentirnos orgullosos de que un proyecto pionero e inédito en todo el mundo haya nacido en España” (Díaz, 2017).

5.2 La *blockchain* a nivel internacional.

Las instituciones españolas han estado bajo la influencia de las grandes entidades financieras que han estado llevando a cabo pruebas acerca de la cadena de bloques publicando sus resultados. Como consecuencia, el número de bancos que van adoptando esta tecnología es

cada vez mayor. A continuación, hablaremos de los bancos pioneros que han decidido invertir en esta tecnología y que, hoy en día, son una referencia para el resto de las entidades del sector.

En febrero del 2019, *J.P. Morgan* se ha adjudicado el premio del primer banco en Estados Unidos en originar y emitir una moneda digital que pasó a denominarse *JPM coin*. Se trata de una *stablecoin*⁷ simbolizado por un *token* digital respaldado en los dólares estadounidenses que son propiedad de la entidad *J.P. Morgan Chase*, provocando que sus valores sean idénticos. Su utilidad principal es la de liquidar transacciones asociadas a la transferencia de fondos momentáneamente entre los clientes autorizados de *J.P. Morgan*, puesto que se dirige fundamentalmente a clientes institucionales tales que bancos, fondos soberanos y fondos de pensiones, que van a ser capacitados para canjear sus *JPM Coins* en el banco para recibir dólares estadounidenses en cualquier momento. Cabe mencionar que este proyecto ha sido concebido en el cuadro de un estudio y la puesta en marcha de la tecnología de las cadenas de bloques aplicada a los procesos bancarios para comprobar su alcance en primera persona, lo que en última instancia se ha traducido en una reducción de los costes para la entidad como para sus clientes y en un aumento considerable de la eficiencia en relación con la ejecución de operaciones.

The Hong Kong and Shanghai Banking Corporation, el banco multinacional conocido con sus siglas HSBC, llevó a cabo la realización de una plataforma digital, llamada *eTrade Connect* dirigida hacia el financiamiento vía la cadena de bloques en colaboración con decenas de bancos relevantes, como *Crédit Suisse* o *BNP Paribas*. El tiempo medio para la concesión de un préstamo comercial se sitúa entre treinta y cuarenta horas, mientras que con este nuevo sistema se tardará menos de cuatro horas en finalizar una operación entre el banco y el cliente. Por otra parte, para demostrar su compromiso hacia esta tecnología, "HSBC anunció la intención de traspasar activos con valor de veinte mil millones de dólares a *Digital Vault*, una nueva herramienta segura basada en *blockchain*. Con esto, el banco con sede en Reino Unido estaría asignando cerca del 40% de sus activos en la cadena de bloques; una

⁷ Es un tipo de criptomoneda que busca reducir la volatilidad proporcionando una mayor estabilidad de precio. Para ello, irá acompañado por una especie de colateral, que podría ser una moneda fiduciaria (esencialmente en dólar) o un activo en bolsa,

cifra que supondría un inmenso paso de un gran banco mundial en el área de la *blockchain*". (Reuters, 2018). Adicionalmente, han estimado haber procesado cerca de dos millones de operaciones a través de una cadena bloques privada, *FX Everywhere*.

En el continente asiático, es el banco nipón *Mitsubishi UFJ Financial Group* quien se demarcó por su pronto interés en esta tecnología, remontando en el año 2016, anunció por primera vez la creación de su propia criptomoneda, denominada *MUFG coin*, que no prosperó. Actualmente, la famosa institución bancaria lanzará su nueva red privada, *Global Open Network*, junto con la emisión de una nueva moneda local, que será aceptada como medio de pago por empresas que actúen en dicho territorio, multinacionales y hasta instituciones públicas, como por ejemplo la compañía ferroviaria *Kintetsu*.

III. Conclusiones

Hemos iniciado este trabajo tratando de entender la *blockchain*. En un primer tiempo, nos hemos centrado en su historia intentando aportar los antecedentes para poder analizar los principales fundamentos sobre las que se basa, explicando sus características y describiendo su tipología. Simultáneamente, hemos observado el creciente interés del sector bancario en adquirir conocimiento acerca de esta tecnología que tiene todas las chances de modificar el sistema tradicional tal como lo conocemos actualmente. Como pudimos observar, el uso de la cadena de bloques en la banca ya no está en una fase de observación y deducción teórica, muchas compañías bancarias ya han realizado pruebas e implementado esta tecnología en su infraestructura. Descubrimos la reacción de los bancos frente al desafío y a la oportunidad que representa, con un propósito en particular, ser aptos en aportar una respuesta a la siguiente pregunta, *blockchain*, ¿un riesgo real para el sector bancario?

Nuestra réplica se va a basar en gran parte en descifrar la postura de los bancos frente a esta tecnología que, hoy en día, podemos asegurar que no representa una revolución, sino una evolución, que está presenciando un cambio importante sobre todo en el sector financiero. Cabe resaltar los numerosos aportes y el enorme potencial que el *blockchain* representa para los bancos, aunque en la actualidad, sería muy difícil pensar que remplazaría al sistema bancario. Pensamos que pasará a formar parte de sus actividades garantizando la agilización del sistema para emprender de forma instantánea, transparente y segura el registro y la validación de operaciones cuya trazabilidad permite tener una visión del conjunto de los datos en cualquier momento, lo que da la esperanza de que el blanqueo de capitales se acabe extinguiendo. Aunque sea una tecnología que sigue sembrando dudas, lo cierto es que ha permitido que los bancos se unan mediante la creación de consorcios como hemos visto anteriormente (R3 y Alastria). Frente a la insurrección masiva de nuevos competidores que irrumpieron con fuerza en el escenario mundial, se han creado sinergias entre los servicios existentes y la nueva tecnología para plantar cara a estos nuevos modelos de negocio que mitigan el rol de la banca.

Sin embargo, hemos comentado la existencia de un vacío legal que gira alrededor de la cadena de bloques puesto que seguimos sin ponernos de acuerdo sobre la determinación de

su centro de actuación. A todo esto, se hace notar la necesidad de una institución legalizada cuya función principal sería la de regulador y supervisar los servidores que van a ser emprendidos por los bancos para tramitar sus transacciones. Las cuestiones relativas a la regulación crean desconfianza en cuanto a su evolución dentro del mercado. Es, por lo tanto, imprescindible regir unas normas a nivel internacional que servirán de referencia para cualquier entidad o empresa que haga uso de ella. En el caso de que la regulación sea establecida por los participantes de la asociación financiera, no podríamos tener ninguna garantía de que la red en cuestión es totalmente legal dado que podría autorizar prácticas que no han sido aprobadas por la legislación vigente. Teniendo en cuenta las características del *blockchain*, el objetivo desde el punto de vista legal será el de encontrar un equilibrio entre la privacidad de los participantes y el control que se pretenderá realizar sobre las transacciones que se realizan, puesto que, sin regulación, no se le puede garantizar a los agentes sociales y económicos su seguridad. La dificultad será reside en encontrar el límite entre una regulación exhaustiva que pretende violar la intimidad de los ciudadanos y recortarles sus derechos, frente a una regulación razonablemente moderada que permita la expansión de la cadena de bloques. Si se produce el siguiente escenario, esta tecnología alcanzará la prosperidad dado que será gratamente aceptada por la totalidad de las instituciones.

Concluiremos este trabajo con dos convicciones, asumimos que el futuro es una incógnita mayúscula, no sabemos con precisión cómo esta tecnología pretende desarrollarse y peor todavía, tampoco sabemos lo que le depara la humanidad. Asumimos igualmente que hoy en día, la *blockchain* ha pasado de ser temida y considerada como una amenaza, hasta ser parcialmente domada para pasar a formar parte del abanico de servicios financieros en el mercado, y percibida como una oportunidad de mercado, que produjo una rápida reacción por parte de los bancos que se plantearon evolucionar a la par con los avances globales en materia de transformación digital. Quien sabe, quizás la *blockchain* se convierta en el nuevo libro contable universal en el que se procesa cualquier operación en el planeta, más pronto que tarde.

IV. Bibliografía

- A. Preuskschat, Los Tipos de Blockchain (2017), <https://www.iecisa.com/es/blog/Post/Los-tipos-de-Blockchain-publicas-privadas-e-hibridas-y-II/>
- B. Nogales, El uso de la blockchain para la banca (2018), <https://bitcoin.es/actualidad/blockchain-para-los-bancos-usos-beneficios-e-inconvenientes/>
Bheemaiah, K. The Blockchain alternative: rethinking macroeconomic policy and economic theory (2017).
- Brands, S.: Electronic Cash on the Internet. In: Proceedings of the Symposium on the Network and Distributed System Security (1995)
- B. Cant, “Smart Contracts in financial services: Getting from Hype to reality” (2016), Consorcio de bancos r3, definición y concepto, <https://www.r3.com/corda-network/>
- E. Díaz, Zuñiga La tecnología Blockchain en las instituciones financieras (2018) , <https://www.ig.com/es/estrategias-de-trading/la-tecnologia-blockchain-en-las-instituciones-financieras-181224#information-banner-dismiss>
- E. Sereno, La limitación de la blockchain y sus desafíos (2019), <https://www.eleconomista.es/aragon/noticias/10122376/10/19/Blockchain-los-tres-desafios-que-esta-tecnologia-tiene-ante-si.html>
- J. Chen, Protocolo *Know your Client* (2019), <https://www.investopedia.com/terms/k/knowyourclient.asp>
- McLeay Y, M., “Money creation in the modern economy” (2014).
- N, Mantoni La banca y el blockchain (2018), <https://dailyhodl.com/2018/12/19/which-banks-have-already-integrated-blockchain-technology/>
- N. Rodríguez, Blockchain y su historia (2018), <https://101blockchains.com/es/historia-de-la-blockchain/>
- N. Rodríguez, Comparación entre *Hyperledger* y *Corda*, (2018) , <https://101blockchains.com/es/hyperledger-vs-corda-r3-vs-ethereum-la-guia/>

- N. Rodríguez, Tecnología del Registro distribuido (*DLT*), (2019), <https://101blockchains.com/es/tecnologia-de-registro-distribuido-dlt/>
- Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2009).
- Pessoa, M., Williams, M.J.: Government cash management: relationship between the treasury and the Central Bank. Int. Monetary Fund (2013).
- Petrasic, K., & Bornfreund, M. Beyond Bitcoin: The blockchain revolution in financial services (2016).
- Reid, F., Harrigan, M.: An Analysis of Anonymity in the Bitcoin System (2011).
- Szabo, N. Formalizing and securing relationships on public networks (1997).
- V. Butarin, La historia de la cadena de bloques (2013), <https://www.binance.vision/fr/blockchain/history-of-blockchain>

V. Índice de Figuras

Figura 1: Red <i>Peer-to-Peer</i>	7
Figura 2: Operatividad de un <i>hash</i>	11
Figura 3: Ilustración de una <i>DLT</i>	14
Figura 4: Funcionamiento de <i>Ripple</i>	23