Master Universitario en Derecho de Telecomunicaciones,
Protección de datos, Audiovisual y Sociedad de la información.

Curso académico 2016-2017

Trabajo Fin de Máster

"LAS IMPLICACIONES JURIDICAS DEL BLOCKCHAIN EN EL SECTOR FINANCIERO"

Rubén Jurado Villarreal

Tutor:

Agustín Eugenio de Asís Roig

Madrid,

A 6 de Julio de 2017

INDICE

INDICE DE FIGURAS

Resumen

Blockchain ha llegado y está suponiendo una revolución para todos los ámbitos, especialmente para el sector financiero. Resulta evidente que se trata de una tecnología muy temprana pero que se está desarrollando rápidamente, en especial por su aplicación real en la contratación. Sin embargo, no quedan claras las implicaciones jurídicas que pueden derivarse de su implementación. Hasta el momento, diferentes entidades financieras han puesto en marcha distintos proyectos basados en blockchain, y de cara al futuro es necesario la regulación y control a nivel mundial o regional de esta tecnología.

Abstract

Blockchain has come and it is being a revolution in all areas, specially in the financial sector. It is obvious that blockchain is an early technology, but it is developing quickly, specially due to its actual application to contracts. Nevertheless, the legal implications that may be derived from its implementation are not clear. Thus far several financial institutions have launched different projects based on Blockchain. Looking forward it is necessary to establish a regulation and control of this technology at a global and regional level.

Palabras clave**:** Blockchain, Smart-Contracts, consenso, privacidad, cifrado, cumplimiento, regulación, sector financiero, bancos.

Key words: Blockchain, Smart-Contracts, consensus, privacy, cryptography, compliance, regulation, financial markets, Banks.

Introducción

Blockchain es una tecnología creada a finales de 2008 por Satoshi Nakamoto a través de un artículo titulado “Bitcoin: A Peer-to-Peer Electronic Cash System”. El artículo hace referencia al funcionamiento del bitcoin, una criptomoneda, que utiliza el blockchain como sistema para llevar a cabo transacciones.

La revolución que trajo consigo esta publicación fue la definición de un sistema que permite asegurar la integridad de las transacciones sin la necesidad de contar con un tercero de confianza.

A partir de entonces, se ha buscado otros usos para esta tecnología, y el sector financiero ha puesto sus ojos detrás del blockchain, debido a sus características. Tanto ha sido el interés que se han dado casos de la utilización de esta tecnología en el ámbito bancario.

A continuación, se expondrá una primera aproximación jurídica de lo que el blockchain puede implicar para el sector financiero.

1. ¿Qué son el Blockchain y los Smart-contracts?

1.1 Concepto de blockchain

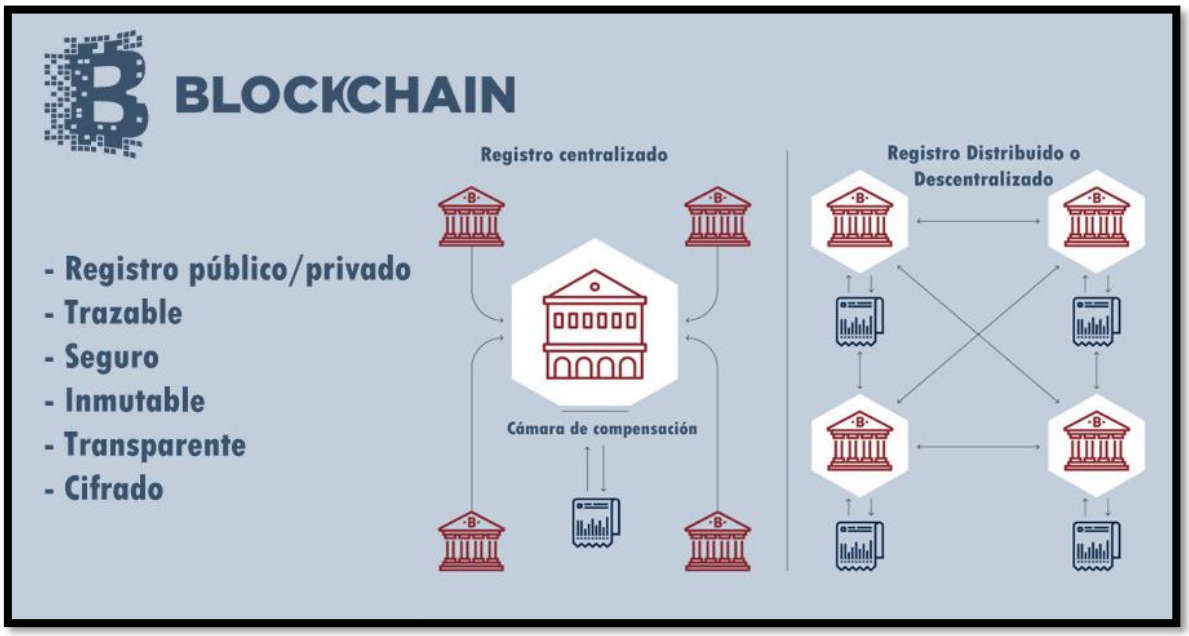
Blockchain es un protocolo de consenso para la creación de una única base de datos distribuida entre un número de usuarios. Es decir, todos los usuarios comparten una única verdad publicada en una base de datos[1].

Consta de tres componentes fundamentales: una transacción, un registro de transacciones y un sistema que verifica y almacena la transacción. En las transacciones tradicionales, como las transferencias de dinero o de divisas, normalmente hay un intermediario o una entidad centralizada que registra la transmisión de dinero o de divisas y que existe de forma independiente[2]. No obstante, lo verdaderamente interesante del blockchain es que todo esto sirve para poder llevar a cabo transacciones sin un tercero de confianza (por ejemplo, un notario), ya que la propia tecnología, una vez que la transacción este validada, permite que esa información sea de confianza por si sola al ser imposible alterarla.

Cuando hacemos referencia a bloques, pueden entenderse como meras transacciones, que, en la práctica, pueden convertirse en una transferencia bancaria de dinero, un contrato de compraventa, un arrendamiento o una hipoteca, un préstamo bancario...etc. De tal manera, que se trata de una tecnología que permite, que esas transacciones tengan las características que he mencionado anteriormente y que se muestran en la figura siguiente.

[1] Definición extraída de: IEB. Blockchain, La disrupción en el sector financiero
[2] *Vid.* BBVA Research, Bitcoin: A Chapter in Digital Currency Adoption. Disponible en: https://www.bbvaresearch.com/wp-content/uploads/migrados/130731_EconomicWatchEEUU_Bitcoin_tcm348-398292.pdf

Figura 1. Características del Blockchain



Fuente: elaboración propia

La gran particularidad del blockchain, o, mejor dicho, la clave para que esta tecnología pueda aplicarse, es el **consenso**. Esto es, bien sea una blockchain de acceso privado o público[3], la forma para validar los bloques de la cadena es, a través del consenso entre los agentes, es decir, un protocolo común que verifica y confirma las transacciones realizadas. En este sentido, la primera blockchain[4] tenía al consenso del 51% como una de sus principales características, sin embargo, y como veremos posteriormente, la forma de validación consensuada cambia fundamentalmente dependiendo del tipo de blockchain y también por cuestiones técnicas, como, por ejemplo, el tipo de algoritmo utilizado, por ejemplo, se puede hacer un algoritmo que permita que solo unas entidades determinadas sean las que puedan consensuar sobre la validez de una transacción.

Para terminar con esta breve explicación conceptual de la tecnología, una de las características que permiten el funcionamiento de la cadena de bloques, es la

[3] En el caso de blockchain accesibles al público, los nodos (usuarios) validan la transacción por mayoría (51%). Las blockchain privadas se basan en un consenso en el que los usuarios no participan, son las instituciones financieras (en caso de ser un blockchain financiero) las que establecen un algoritmo de consenso en base a sus intereses. Por ej. Si es una transferencia de dinero entre dos bancos, serán solo esos dos bancos los que participan en la validación.

[4] Con Satoshi Nakamoto, apareció la primera blockchain para permitir el funcionamiento de la criptomoneda, Bitcoin.

criptografía o cifrado. *Por tal entendemos un procedimiento que, utilizando un algoritmo con clave (clave de cifrado), transforma un mensaje sin atender a su estructura lingüística o significada de tal forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo empleado. En la blockchain, la criptografía tiene la responsabilidad de proveer un mecanismo infalible para la codificación segura de las reglas del protocolo que rigen el sistema. Es también fundamental para evitar la manipulación, hurto o introducción errónea de información en la cadena de bloques, así como la responsable de generar firmas e identidades digitales encriptadas*[5].

1.2 Modalidades de blockchain

Dada las particularidades que tiene blockchain, es posible que se puedan formar registros con diferentes características. En este sentido, podemos encontrar en la práctica, tres tipos bien diferenciados:

1.2.1. Blockchain de acceso público, abiertos y descentralizados

La blockchain de acceso público está basada en la tecnología que utiliza bitcoin para su funcionamiento. Se trata de sistemas descentralizados y abiertos, donde no existe ninguna autoridad que tenga el poder y todos los usuarios tienen acceso a la información y de forma replicada. De tal manera que, cada usuario posee una copia del registro y puede leer, enviar transacciones y participar en el proceso de verificación y validación de transacciones (minería en bitcoin[6]).

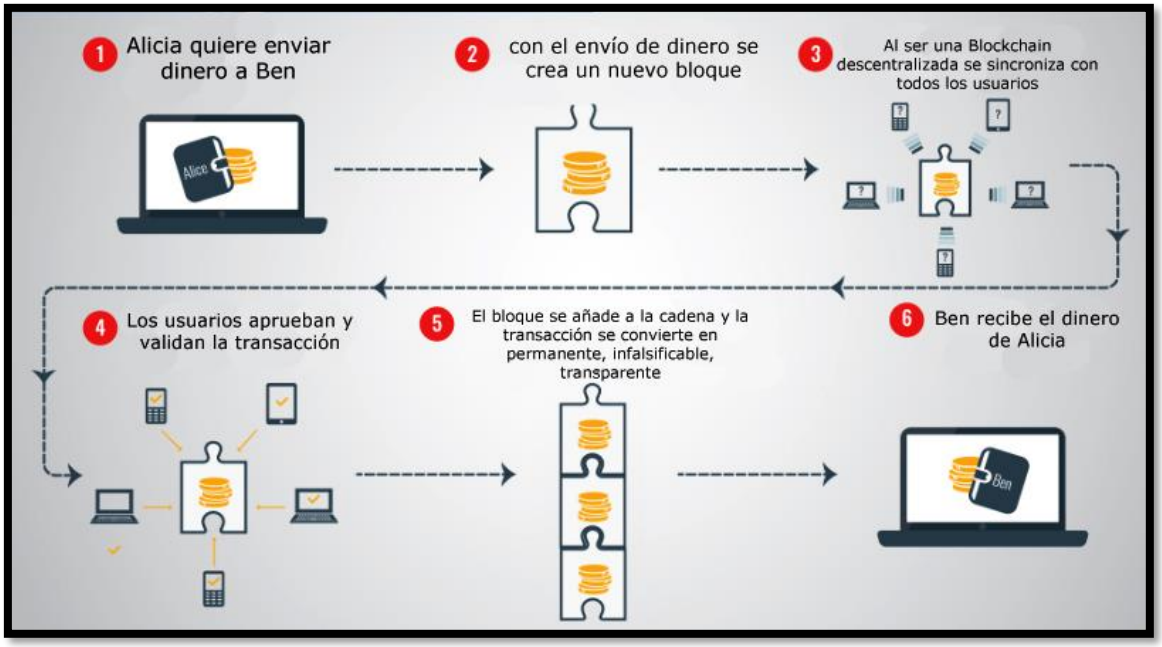
Al tratarse de una red de acceso público, la blockchain está construida para agregar información y no es posible modificar o eliminar los registros históricos (superiores a un día), es decir, se puede añadir información, pero nunca borrar, ya que uno de los requisitos para que el bloque pueda añadirse a la cadena sin generar una transacción corrupta, es que debe de cumplir con un registro anterior validado y duplicado por todos

[5] Definición de Criptografía. PREUKSCHAT, A.: "Blockchain: La revolución industrial de Internet", Barcelona, Centro Libros, 2017, p. 26.

[6] 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. Podría describirse como el centro de datos de Bitcoin, excepto que este ha sido diseñado para ser completamente descentralizado con mineros operando en todos los países y sin que nadie tenga el control absoluto sobre la red. Definición extraída de la web oficial de bitcoin sin ánimo de lucro: bitcoin.org/es/faq

los usuarios[7]. Para poder eliminar una transacción sería necesario eliminarla de todas las copias que los usuarios tienen en sus manos, algo virtualmente imposible.

Figura 2. ¿Cómo funciona una blockchain publica?



Fuente: Elaboración propia.

1.2.2. Blockchain privados, cerrados y centralizados.

Es un sistema centralizado, donde los permisos y/o privilegios son determinados por una única entidad o institución que aglutina todo el poder. En este supuesto, solo los usuarios con permiso[8] pueden participar y acceder al registro, ya sea para leer o editar. Los permisos pueden obtenerse, bien a través de una lista blanca que te autoriza a participar, o bien a través de una lista negra te restringen el acceso. Se trata de registros que no aprovechan del todo la capacidad de esta tecnología, en lo que respecta a la

[7] Una explicación más sencilla del funcionamiento de una transacción en una blockchain publica seria: los usuarios validan las transacciones por consenso, pero solo aquellas que no muestren conflicto con otras anteriores, por ejemplo, si A tiene 5 y paga 4 a B, se crea un bloque, pero si A vuelve a pagar 4 a C, entraría en conflicto con el anterior bloque, ya que A no tiene suficiente dinero en base a esa transacción.

[8] Definition of a permissioned blockchain: A permissioned blockchain restricts the actors who can contribute to the consensus of the system state. In a permissioned blockchain, only a restricted set of users have the rights to validate the block transactions. Una traducción aproximada seria: Un blockchain bajo permiso o cerrado restringe el número de usuarios que pueden contribuir al consenso del sistema. En un blockchain cerrado, solo un número determinado de usuarios tienen derecho a validar las transacciones

inmutabilidad de las transacciones. En un registro con pocos agentes, sería fácil obtener el consenso por una transacción no real.

1.2.3. Blockchain híbridos o consorciados, cerrados parcialmente y distribuidos

Este último tipo de blockchain es el que más nos interesa. El blockchain hibrido o consorciados son registros distribuidos, de manera que el registro está controlado por un consorcio de empresas o instituciones. En este sentido, son esas empresas las que se encargan de validar las transacciones cuando alcanzan la mayoría y de esta manera, se añaden al registro.

Estos registros pueden ser abiertos, de manera que cualquier usuario puede acceder a la información o bien, pueden ser cerrados, necesitando un permiso. De tal manera que sólo los participantes en el consorcio podrán escribir en la blockchain.

Como se ha dicho anteriormente, al tratarse de una red híbrida, la blockchain puede modificarse o eliminar sus registros siempre que haya consenso entre los participantes (la cuestión de la inmutabilidad o inalterabilidad de los registros se verá comprometida más adelante). Normalmente la información está cifrada para que solo algunos usuarios puedan tener acceso a la misma.

El consorcio puede exigir la identificación de los usuarios, con fines de cumplimiento normativo, como por ejemplo el Know Your Customer (KYC), para ello, y como veremos más adelante, se fijan unos estándares de firma electrónica y obligaciones de transparencia para la identificación de los usuarios.

Una de las razones manifestadas por el sector financiero para el desarrollo de las blockchain consorciadas o hibridas ha sido la imposibilidad de compartir, por razones regulatorias o de confidencialidad, sus bases de datos de forma abierta.

Normalmente, al contar con DLT (Distributed Ledger Technology), se trata de un registro que se distribuye entre varios nodos (agentes o miembros del blockchain) y siguen las normas de una figura dominante. Un ejemplo sería los casos de blockchain híbridas financieras que veremos más adelante, la red Corda del consorcio R3.

Actualmente, dado que muchas entidades financieras están investigando esta tecnología, los requisitos de entrada y salida son muy flexibles y tan solo requieren que las instituciones sean entidades financieras y que aporten una determinada cantidad para la financiación de la plataforma. Sin embargo, hay que tener en cuenta cómo va a ser la suscripción de los bancos a estos consorcios, ya que, por otro lado, es necesaria la interoperabilidad entre las entidades para poder usar esta tecnología. Quizás en el futuro, se imponga, de la mano del Banco Central Europeo, la entrada de las entidades para facilitar esa interoperabilidad.

Figura 3. Ventajas y desventajas de los tipos de blockchain

Pública	✓ Red neutral, independiente, abierta y pública ✓ Efecto red: al ser abierto posibilita el aumento de usuarios que lo utilicen para intercambiar activos y la creación de nuevas aplicaciones / usos ✓ Permissionless innovation: tecnología abierta a los desarrolladores sin pagos de tasas, fomenta la innovación ✓ Transparencia ✓ Inmutable	~ Transparencia: no todas las públicas ofrecen la privacidad requerida por las entidades financieras, aunque están trabajando en ello ~ Imposibilidad de anular transacciones (p.ej. entidades financieras) ~ Coste de los incentivos económicos para la red ~ Coste de la infraestructura: electricidad, hardware, etc. ~ Escalabilidad: en desarrollo varias propuestas ~ Pseudo-anonimato: reto regulatorio ~ Consenso para realizar cambios en el protocolo
Consorciada o híbrida	✓ Privacidad ✓ Encriptación de la información ✓ Escalabilidad consensuada con mayor rapidez ✓ No es necesario proporcionar incentivos a la red	~ Número limitado de usuarios, pierde el efecto red ~ Consenso: requiere el consenso de todos los participantes, siendo un reto poner los intereses y prioridades de todos de forma efectiva

Fuente: IEB. Blockchain, La disrupción en el sector financiero

1.3 El Blockchain en el sector financiero

Después de analizar el concepto y las tipologías de blockchain que existen en la actualidad, es necesario explicar cuál sería, o está siendo, la implementación del blockchain en el sector financiero. En este sentido, las principales iniciativas de blockchain en el sector bancario han sido a través de DLT, es decir, registros distribuidos entre las diferentes entidades y que en la mayoría de casos se han creado siendo privados pero que tienden a ser híbridos o consorciados (véase el caso de Corda de R3[9]).

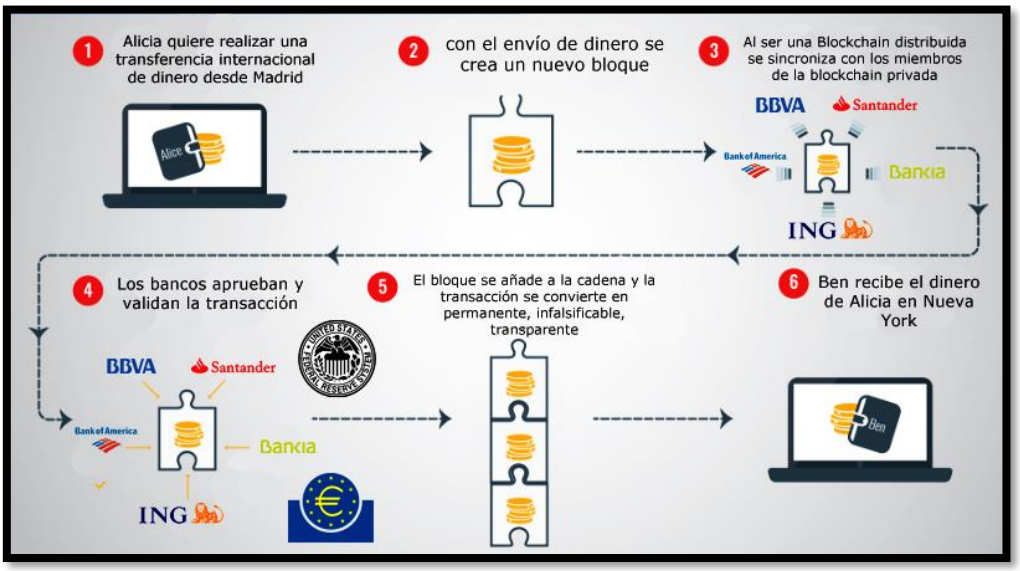
[9] Para más información: HEARN, M. (2016), "*Corda: A distributed ledger*". Extraído de: [url] https://docs.corda.net/_static/corda-technical-whitepaper.pdf

Los anteriormente mencionados DLTs, permiten a los usuarios modificar registros en una base de datos distribuida (entre los usuarios), sin necesitar un centro de validación que imponga sus propios estándares y procedimientos. Ahora bien, al ser distribuida, existe una autoridad que es la que distribuye dicha base de datos entre los participantes, y en principio, bajo unas reglas de consenso y, en algunos casos, de cifrado, con la finalidad de que todo funcione automáticamente. De esta manera, los DLTs pueden ser usados en el sector financiero para crear registros distribuidos que puedan sellar acuerdos comerciales sobre activos financieros y gobernados por una autoridad.

Otro de los factores por los que el sector financiero ha optado por un registro hibrido y distribuido es por la posibilidad de poder alterar los "bloques". La inmutabilidad de la que gozan los registros de blockchain públicos se ha expuesto al riesgo del error humano. Un ejemplo reciente fue una persona de un país nórdico que subió 2,5 megabytes de información pornográfica ilegal en una blockchain pública hace 5 años, hoy en día, sigue estando ahí por su inmutabilidad[10]. Otro de los problemas se da cuando el error humano supone la equivocación de la contra parte en un contrato o en la cantidad que supone la transacción. Por consiguiente, se hace imperativo en esta tecnología la necesidad de establecer un gestor de cumplimiento o riesgos que monitoricen los movimientos y gestionen las comunicaciones entre las partes y poder editar o eliminar los movimientos cuando sea necesario.

[10] Otro ejemplo del poder de la inmutabilidad del blockchain sucedió con el *disclosure* de información clasificada de diplomáticos estadounidenses por wikileaks, alrededor de 250.000 documentos que siguen en la blockchain hasta la actualidad.

Figura 4. ¿Cómo funciona una DLT? (simple)



Fuente: Elaboración propia

1.3.1 Las Transacciones financieras como Smart-Contracts (de la contratación clásica a la contratación inteligente)

Una de las ventajas que nos permite los DLTs es la posibilidad de celebrar Smart-contracts, o contratos inteligentes. El principal objetivo que tienen los contratos inteligentes es que te permiten contratar con otra persona desconocida con total confianza y a través de internet, ya que no sería necesario un tercero de confianza al automatizarse el proceso de contratación[11]. Un ejemplo de este tipo de contratos se puede dar en el supuesto de un partido de futbol para el cual compras una entrada, y solo en caso de cancelación del partido, la entrada será reembolsable. Para ello, se lleva a cabo un Smart-Contract con diferentes clausulas auto ejecutivas, y una de ellas ejecuta el reembolso en caso de cancelación del partido, de manera que, en el caso de suspenderse, el propio código depositado en la blockchain se ejecuta y se reembolsa el dinero sin necesidad de reclamar la devolución a cualquier agencia o tercero.

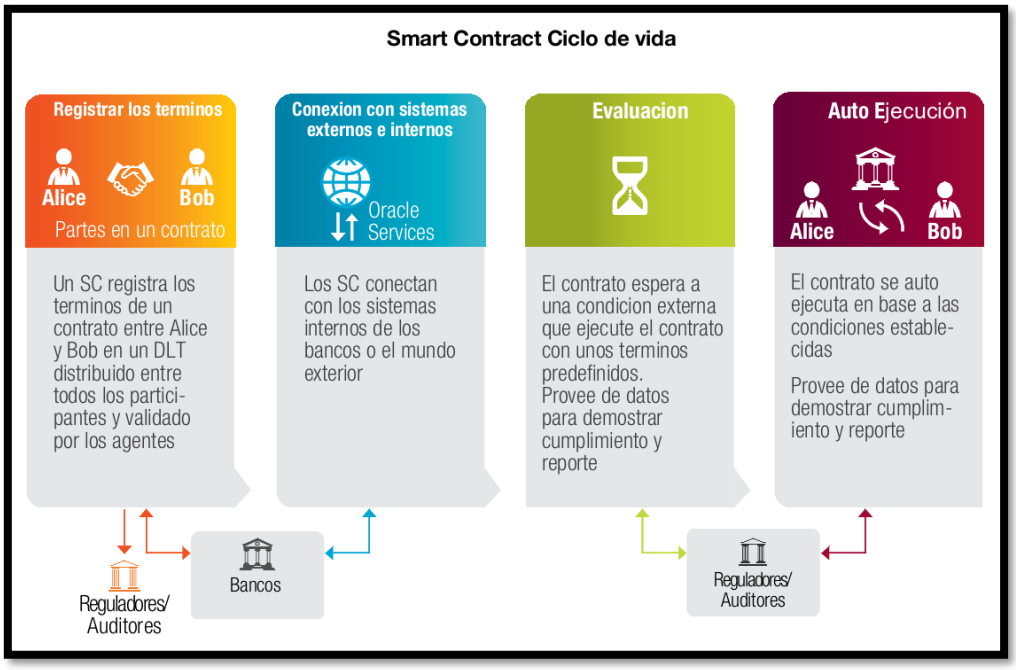
Por consiguiente, una de las principales características de este tipo de contrato es que se elimina la posibilidad de acción declarativa o ejecutiva ante un juez, al automatizarse esas acciones. Esto puede ocurrir en el supuesto de una compraventa de una cosa

[11] SZABO, N., (1997), "Formalizing and Securing Relationships on Public Networks", First Monday. Disponible en: [url] http://journals.uic.edu/ojs/index.php/fm/article/view/548/469

determinada, de manera que, una de las partes se obliga a cumplir con el pago del precio de la cosa, pero la otra parte no cumple con la entrega de la misma, en este sentido, si se trata de un contrato inteligente, el contrato ejecutaría directamente la condena a la parte incumplidora en caso de establecer en el contrato penas convencionales.

Entrando en el terreno de la contratación en el ordenamiento jurídico español, en la actualidad, para la celebración de un contrato, necesitamos que concurran al mismo tiempo varios requisitos. Estos requisitos vienen establecidos en el artículo 1261 del Código Civil, esto es, el consentimiento de los que contratan, el objeto sobre el cual se contrata, y la causa de la obligación que se establezca. De tal manera, que, si no se dan estos requisitos, el contrato será nulo al ir en contra de un mandato imperativo.

Figura 5. Smart-Contract. Ciclo de vida



Fuente: Capgemini Consulting Analysis. Traducción propia

En primer lugar, el contrato inteligente se lleva a cabo entre dos o más partes, es decir, un acuerdo de voluntades, y para que sea válido, es necesario que esas partes tengan capacidad de obrar. En este sentido, y como hemos mencionado anteriormente, un registro como el blockchain permite cifrar las transacciones y al mismo tiempo, que las partes puedan ser identificadas gracias a la firma electrónica. En principio no es necesario, para contratar por internet, la firma electrónica, no obstante, cuando reúne ciertas características otorga al documento de credibilidad y seguridad, que dota al

documento de una fuerza probatoria superior[12] lo que unido al estar registrado en una red distribuida puede ser susceptible de validez frente a terceros. De esta forma, una vez que se preste el consentimiento, se acepta el contrato y por tanto, puede que se cumpla la condición por una de las partes, y se perfecciona, o bien se incumple y por tanto se auto ejecuta[13].

Dicha auto ejecución encaja con la figura de los contratos sometidos a una condición, ya sea suspensiva o bien como resolutoria. El problema que se plantea en algunos casos es la imposibilidad de la condición, es por ello que resultaría contrario a las buenas costumbres y, en definitiva, prohibido por ley.

Por otro lado, la libertad de forma recogida en el Código civil[14] permite que, los contratantes puedan decidir como contratan, con quien y cuál es la regulación de la relación contractual. El principio de libertad de forma va ligado al de autonomía de la voluntad para contratar, de manera que permite la contratación sin ir en contra de las leyes, la moral o el orden público. Cabe destacar que la forma no es un elemento esencial de los contratos con carácter general, lo mismo recoge el artículo 51 del Código de Comercio que manifiesta que «serán válidos y producirán obligación y acción en juicio los contratos mercantiles, cualesquiera que sean la forma y el idioma en que se celebren, la clase a que correspondan y la cantidad que tengan por objeto, con tal que conste su existencia por alguno de los medios que el Derecho civil tenga establecidos». De manera que, la regla general es que cualquiera que sea la forma en la que se contrate, incluso la verbal, produce plenos efectos entre las partes, otra cosa sería el valor probatorio frente a terceros, que la forma de los contratos inteligentes lo garantizan.

Sin embargo, en el mismo Código Civil, se regula una excepción a dicha libertad de forma, los contratos celebrados con el otorgamiento de escritura pública[15]. En este

[12] FERNANDEZ, R., "*Forma de prestación del consentimiento electrónico: referencia a la firma electrónica y a la prueba de la existencia del contrato*" pp. 305-330

[13] Artículo 1262 del Código Civil: "En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación." Un ejemplo claro de que estos contratos automáticos existían previamente, es el contrato celebrado con una máquina expendedora de refrescos.

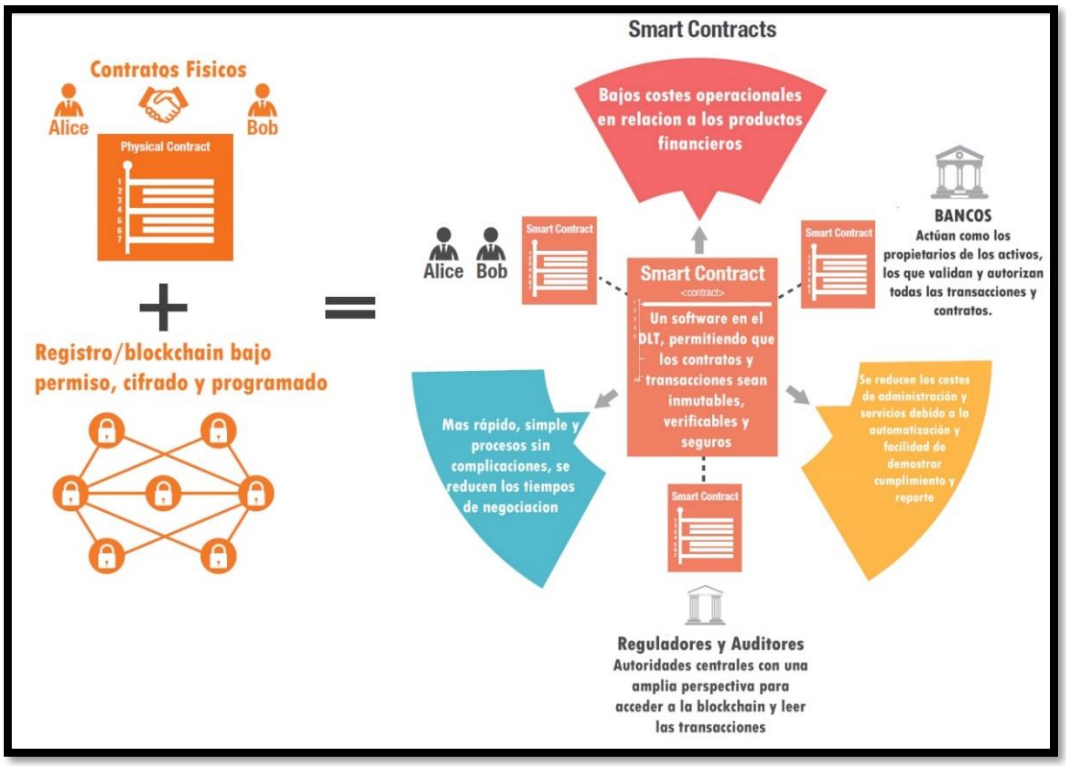
[14] Artículo 1278 del Código Civil: "Los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez."

[15] Artículo 1279 del Código Civil: "Si la ley exigiere el otorgamiento de escritura u otra forma especial para hacer efectivas las obligaciones propias de un contrato, los contratantes podrán compelerse

sentido, algunos de los contratos de tracto sucesivo en el sector financiero requieren de esta especifica norma. Un ejemplo sería el de contrato de hipoteca, que debería otorgarse bajo escritura pública. Resulta interesante considerar la posibilidad de salvar esta forma contractual, sobre todo en el caso de las hipotecas donde es un requisito *ad solemnitaten* y constitutivo para el contrato, a través del blockchain. No obstante, será una cuestión que se mencionará más adelante.

Básicamente, con DLT, los Smart-Contracts pueden usarse para llevar a cabo transacciones basadas en un clausulado consistente en "Si se da la situación A, entonces ocurre B" y, por tanto, en el caso de una compraventa, la propiedad del bien, servicio o cualquier objeto puede ser transferida automáticamente, o bien, en caso de incumplimiento por una de las partes, la posibilidad de fijar penas convencionales o sanciones en el contrato y auto ejecutarse. Los términos del contrato están escritos en lenguaje de código, y, por ende, es como tener un contrato de papel que puede leerse a si mismo y llevar a cabo los términos pactados y cuando vienen a tener efecto.

Figura 6. Como los SC funcionan en un blockchain bajo permiso o cerrado



Fuente: Capgemini Consulting Analysis. Traducción propia

recíprocamente a llenar aquella forma desde que hubiere intervenido el consentimiento y demás requisitos necesarios para su validez."

En el ámbito financiero, los contratos inteligentes pueden proporcionar transacciones automáticas, (como acreditar un pago de dividendos o cupones, reaccionar a ajustes de márgenes en bolsa de valores u optimizar el uso de garantías), y que tengan lugar en el registro de blockchain en respuesta a una acción corporativa específica o un evento que ha sucedido en el mercado (dependiendo del código del SC). Además, dado que los contratos inteligentes están escritos en la blockchain, la validación de su ejecución sigue el mismo procedimiento que cualquier otra transacción, es decir, por el consenso de los agentes participantes. Asimismo, si un DLT es capaz de asegurar que las actualizaciones en el registro sean a prueba de ataques cibernéticos, la ejecución de sus contratos inteligentes también está protegida de forma similar a esos ataques.

Los servicios financieros se encuentran en un sector que está muy regulado, y es necesario licencias específicas y aprobaciones, que perfectamente pueden trasladarse a un registro distribuido. Por otro lado, las características de la blockchain permiten la total transparencia en las transacciones, por lo que, el uso de los Smart-Contracts por parte de las entidades financieras permiten demostrar el cumplimiento con los organismos y autoridades reguladoras. No obstante, la legalidad de los SC financieros está todavía por ver, y en los próximos epígrafes se llevará a cabo una primera aproximación de los problemas legales que pueden entrañar.

1.3.2 El uso de los contratos inteligentes en el sector financiero.

Una vez expuestos los diferentes argumentos de cómo se puede implementar el uso de la blockchain en el sector financiero a través del uso de Smart-Contracts, es necesario dilucidar las diferentes finalidades que tiene este tipo de contratos inteligentes y la tecnología que utiliza para el sector financiero. En este sentido, son varias las finalidades que pueden distinguirse dentro del sector financiero.

- **Financiación de las PYMES (pequeñas y medianas empresas) a través de préstamos**: las empresas pueden acceder como participantes del blockchain para disfrutar de inversores de todo el mundo, debido a la facilidad y rapidez en el proceso de las transacciones. De esta manera, es posible expandir las oportunidades de financiación de este tipo de empresas. Este tipo de préstamos son posibles dado que podría aparejarse la garantía al préstamo en el mismo SC,

de manera que en el supuesto de que el deudor incurra en mora automáticamente el contrato inteligente proceda a la ejecución de la garantía, bien revocando las claves digitales que dan acceso al deudor a las mismas, bien transfiriendo directamente la garantía al acreedor.

- **Movimiento internacional de dinero**: gracias al blockchain cualquier movimiento de dinero a nivel internacional es posible en tiempo real a muy bajo coste. Por otro lado, esto permitiría cualquier pago de nóminas a nivel internacional eliminando cualquier tarifa y retraso asociado. Este aspecto es muy importante, ya que se garantiza una trazabilidad de la operación y, por tanto, la transparencia de cara a los reguladores. Por ejemplo, una persona que quiere enviar dinero desde su sucursal en España a una sucursal en Australia.

- **Facilidad en el trazado de la propiedad de activos**: como se menciona anteriormente, los activos financieros se podrían simplificar si se plasman en el registro de manera que es posible mantener una trazabilidad de la propiedad. Nos da la posibilidad de prevenir el blanqueo de capitales y operaciones encubiertas.

- **Eliminación de las fases de negociación e intermediarios**: tener a los bancos en el mismo registro distribuido contribuye a mejorar la eficiencia, de manera que las fases de la negociación se acortaran y el número de intermediarios se reduciría. Por otro lado, se optimizan los procesos de conciliación, ya que los registros se actualizan automáticamente, por lo que ayuda al ahorro de costes. Un ejemplo claro se da en el mercado de valores con la emisión de bonos inteligentes.

- **La posibilidad de utilizar blockchain como depósito de garantías en las operaciones bancarias**: la eliminación de las fases de negociación va a contribuir a disminuir la cantidad de garantías necesarias para la negociación. Además, la garantía depositada se liberará más rápido de lo normal, ya que una vez transferida la propiedad del vendedor al comprador, el contrato tiene la orden automática de liberar los fondos de garantía al vendedor.

- **Capacidad de demostrar el cumplimiento ante los organismos regulatorios**: debido a que toda la información está registrada y en principio, inmutable, las entidades financieras podrían dar cumplimiento a las obligaciones regulatorias impuestas por las autoridades a través de reportes de manera más eficiente. Como veremos posteriormente, los reguladores podrían tener un acceso de sólo lectura, casi en tiempo real, al registro distribuido de las entidades financieras. Esto les permitiría jugar un papel más proactivo y analizar información en tiempo real. En otras palabras, esto los acerca a convertirse en participantes en el proceso, en lugar de clientes del proceso. Tal cambio podría reducir drásticamente el tiempo y el esfuerzo (y por lo tanto el costo) que las entidades financieras gastan en la presentación de informes reglamentarios, así como mejorar la calidad, la precisión y la confianza del proceso.

- **Identidad digital:** es posible la utilización de servicios de identidad digital, como la firma electrónica, para garantizar la personalidad en las transacciones, prevenir el fraude, y mejorar la experiencia total del cliente. Blockchain elimina la posibilidad de que una de las partes falsee su dirección email, numero de la seguridad social, o incluso el número de teléfono, lo que ayuda a proteger a las demás partes de robos de identidad. También elimina el riesgo de que una identidad digital para un individuo pueda ser diferente en cada ubicación donde se utiliza.

2. Casos reales en la actualidad

2.1 Ripple

Se trata de una de las primeras plataformas, creadas por entidades financieras, basada en la tecnología blockchain. Ripple fue creada en 2013, como un prototipo, convirtiéndose en un proveedor de servicios de pagos y liquidación multi-divisa, y, además, es una blockchain cerrada y creada específicamente para este sector.

Básicamente, gracias a Ripple, las instituciones financieras pueden llevar a cabo pagos cross-border, a nivel internacional, mediante una conexión directa banco a banco.

El asiento y compensación de la transacción es el resultado del consenso, de manera que las entidades financieras que componen Ripple autorizan a un grupo de contrapartes para validar las transacciones en la blockchain. Con esta contabilidad común, los bancos pueden procesar y liquidar transacciones continuamente (365 días, las 24 horas) y en tiempo real (cada 5 segundos aproximadamente).

Cabe destacar, que Ripple traslada el modelo bitcoin al ámbito privado, ya que utiliza una criptomoneda, pero solo a efectos de utilizarla como "moneda puente"[16], ya que lo normal es que la mayoría de usuarios hagan sus pagos en dólares o euros sin mantener esta moneda (XRP).

Entidades como UniCredit, Bank of America, Santander, UBS o BBVA, participan en Ripple actualmente, y llevan a cabo transacciones a nivel internacional en cuestión de segundos.

Un ejemplo dentro de Ripple, sería una transferencia por parte de una persona en España hacia una persona en Australia. Si los bancos de ambas partes utilizan Ripple, en solo 5 segundo se llevaría a cabo el contrato inteligente de enviar el dinero. Esto supone que, en un periodo de 5 a 10 segundos, se hacen las comprobaciones de blanqueo de capitales, conflictos de riesgos, se cifra la información, se automatizan las comisiones para los bancos que envían y reciben el dinero y, efectivamente, se realiza la transferencia, actualizando los registros de ambos bancos.

2.2 Corda de R3CEV

Corda se trata de una plataforma realizada por el consorcio bancario R3CEV, para registrar, gestionar y sincronizar acuerdos financieros entre instituciones reguladas. Está inspirada en la tecnología blockchain, pero cuenta con muchas diferencias con respecto a las blockchain tradicionales o públicas como la de bitcoin o Ripple, especialmente en

[16] *XRP en la moneda nativa de la blockchain de Ripple. Es un activo digital que existe exclusivamente en esta red y está limitada a 100 mil millones de unidades. El valor de XRP fluctúa libremente contra otras monedas dentro de la blockchain, al igual que lo hace por ejemplo el euro contra el dólar. XRP no tiene un valor intrínseco, es sólo el valor que alguien está dispuesto a pagar por él. No es necesario que los usuarios adopten XRP como depósito de valor o medio de cambio.* Fuente: IEB. Blockchain, La disrupción en el sector financiero

los procesos de consenso y validación, con el objetivo de velar por la privacidad de las transacciones.

Básicamente se trata de un registro distribuido que no funciona en base a una cadena de bloques, de manera que un bloque valida el anterior y así sucesivamente, y no todo el mundo mantiene una copia de ese registro. De esta manera, si se quiere realizar un contrato entre dos partes a través de Corda, el contrato no se queda en un bloque como tal, y todo el mundo puede verlo, sino que se trata de un contrato individual y, de esta manera se envían los datos sobre el contrato solo a aquellos que necesitan saber esa información, ya sea ambas partes, ya sea un servicio externo que certifique y que valide la transacción o bien reguladores que sean exigidos por la normativa.

Las principales funcionalidades de Corda son:

- Privacidad: sólo aquellas entidades participantes que tengan una necesidad legítima de acceder a la información pueden ver los datos dentro de un acuerdo.
- Distribuida: realiza el flujo de trabajo directamente entre las entidades sin un ente central.
- Trazabilidad: el diseño de Corda permite nodos de observación directa por parte de reguladores y supervisores.
- Estandarización: está desarrollado sobre herramientas estándar de la industria y será open source una vez la solución esté madura.
- Criptomoneda: no usa una criptomoneda nativa.

3. Implicaciones jurídicas en el uso de blockchain por entidades financieras. Principales problemas identificados.

Durante los últimos años, los diferentes reguladores han estado intentando dar con la clave en lo que respecta a una regulación del Blockchain, y hasta el momento, no se planteaba una regulación a corto plazo, debido a que no existía una plataforma que usara blockchain y fuera operativa, y por otro lado, todavía no está suficientemente

claro cómo debería cambiar la regulación en antelación al desarrollo tecnológico, ya que, bien es sabido, que cualquier regulación prematura resulta insuficiente a posteriori sobre la tecnología en la práctica, ya que, en la mayoría de veces, la tecnología supera al derecho.

Figura 7. Posición de las autoridades sobre los DLTs.

Posicion de las autoridades sobre los Registros distribuidos				
Autoridad	**Localizacion**	**Posicion**	**Pronunciamiento**	**Resumen**
Parlamento Europeo	UE	Neutral hacia positivo	Informe/ Grupo de trabajo	Acercamiento liberal para la regulación de la tecnología de blockchain. Creación de un grupo de trabajo para analizarla
Comision Europea	UE	Neutral	Grupo de trabajo FT	Regulación de la DLT a través del grupo de trabajo Tecnológico financiero
BCE	UE	Positivo	Informe/ Declaración	Beneficios potenciales en el uso de Registros distribuidos en las actividades posteriores al comercio (cumplimiento). Y ha comenzado un proyecto conjunto con el Banco de Japón para analizar el uso potencial de DLTs.
Bancos Centrales	Varios paises	Positivo	Declaracion/ Informe del BoE	Un gran numero de bancos centrales han mostrado un serio interes en la emison de sus criptomonedas. El Banco de Inglaterra ha publicado un informe sobre este tema

Fuente: BBVA Research. Traducción propia

No obstante, sí que existen algunas regulaciones actuales que pueden aplicarse a servicios basados en blockchain. Un ejemplo de esto, son los Smart-Contract, que como decíamos anteriormente, van a tener que cumplir al menos, con la regulación en materia de contratos en el ámbito civil y mercantil.

De esta manera, dependiendo de qué tipos de servicios financieros se ofrecen en la blockchain (pagos, préstamos, inversiones, etc.), habrá que aplicar la regulación de estos servicios.

De cualquier manera, y como veremos posteriormente, una estrecha colaboración con los reguladores y supervisores desde el principio es necesario para adaptar y desarrollar normas coherentes sobre las tecnologías de blockchain.

En este sentido, se van a exponer los principales problemas que pueden derivarse de la utilización de esta tecnología, fundamentalmente, en el aspecto de los Smart-Contracts y en la modalidad de un Registro distribuido y consorciado entre las entidades financieras.

3.1 Autoridad reguladora gubernamental

Uno de los principales retos y problemas que se plantean, es en relación al tipo de entidades o autoridades legales que operaran en estos registros distribuidos y como los consorcios de bancos que establecen esos DLTs colaborarán con los reguladores.

En este sentido, están surgiendo diferentes DLTs, como por ejemplo R3 o Ripple, que tienen una actuación global y no está del todo clara su territorialidad, ya que, por naturaleza los registro distribuidos no están ligados a una territorialidad especifica. Sin embargo, los requisitos regulatorios, en la mayoría de casos, tienen un componente local. Sería necesario una autoridad global que regulase este tipo de registros[17].

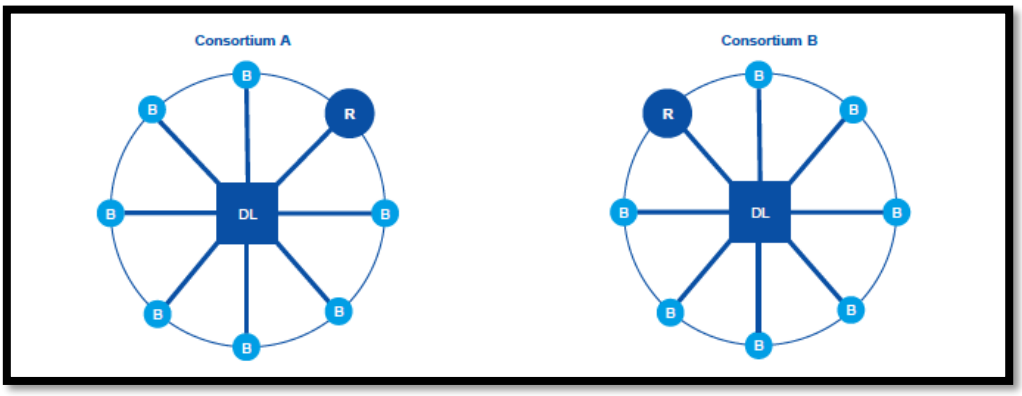
Por otro lado, la autoridad reguladora o supervisora debería velar por el desarrollo de las operaciones llevadas a cabo. A fin de conseguir este objetivo, es necesario que se fijen unas medidas o estándares comunes ("*reglas del juego*"), en lo que respecta a la seguridad de la información, transparencia, cumplimiento y, en definitiva, el procedimiento de contratación en la plataforma.

3.1.1. La creación de un supra-regulador.

Una de las opciones que puede darse en cuanto al rol de regulador seria la creación de un supra regulador. Este regulador tendría una territorialidad global y se reservaría un nodo dentro de cada registro distribuido en el sector financiero. En este sentido, el regulador tendría acceso ilimitado a toda la información relevante que necesite para evaluar los riesgos del sistema. Estaríamos hablando del mismo regulador en cada tipo de registro. Un ejemplo asimilable en la actualidad puede ser la OMPI, y podría contribuir a la armonización de las legislaciones nacionales, facilitar la resolución de controversias a través del arbitraje, entre otras medidas.

[17] Un ejemplo de esta autoridad global puede ser la OMPI. Organismo especializado del Sistema de Naciones Unidas, para fomentar el uso y la protección de las obras del intelecto humano, que dispone de un centro de arbitraje y mediación para la solución de controversias.

Figura 8. Supra-regulador en blockchain



Fuente: BBVA Research

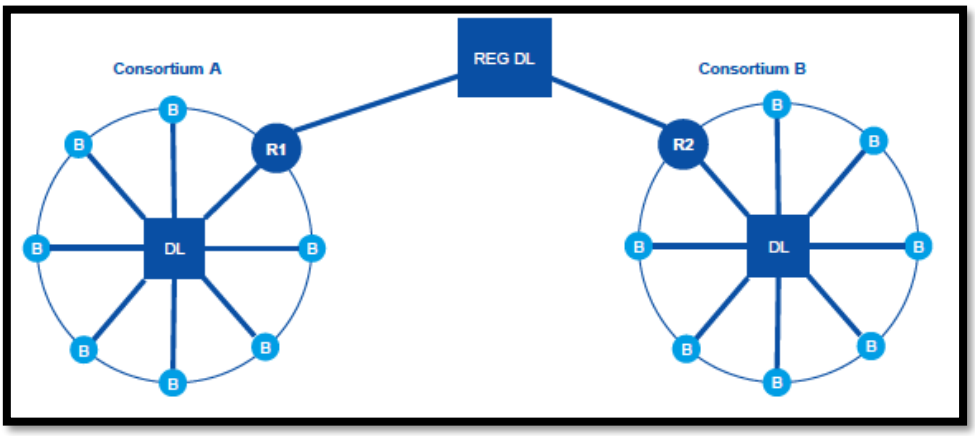
No obstante, es muy improbable que este tipo de aproximación resulte exitosa y se convierta en realidad. Hay que tener en cuenta que, en el sector financiero, existen regulaciones con un componente geográfico muy marcado, por ejemplo, en Europa con el BCE, y, por tanto, son regulaciones locales y regionales que deben tenerse en consideración a la hora de crear una autoridad reguladora.

3.1.2. La creación de un regulador regional y un registro privado regional

La segunda opción planteable puede ser la creación de reguladores regionales para cada registro en diferentes regiones (EEUU, Europa, China), de tal manera que cada regulador regional tendrá su nodo en el registro regional, pero a su vez, participarían de otro registro privado, formado por autoridades regulatorias regionales. Esto supondría que los propios reguladores regionales podrían compartir la información en tiempo real a través de su propio registro distribuido creado a tal efecto. Este caso sería similar al funcionamiento del BCE con el resto de bancos centrales nacionales. En este sentido y de acuerdo al artículo 127.2 del Tratado de Funcionamiento de la Unión Europea[18], dentro de sus funciones se encuentra la definición de la política monetaria de la zona del euro, o promover el buen funcionamiento de los sistemas de pago. De esta manera, los bancos centrales nacionales actuarían como nodos dentro de este tipo de registros de transacciones financieras y luego reportarían al BCE.

[18] El articulo 127 apartado 2 del Tratado de Funcionamiento de la Unión Europea recoge las funciones básicas que se llevaran a cabo a través del SEBC.

Figura 9. Reguladores regionales compartiendo la información en un registro privado.



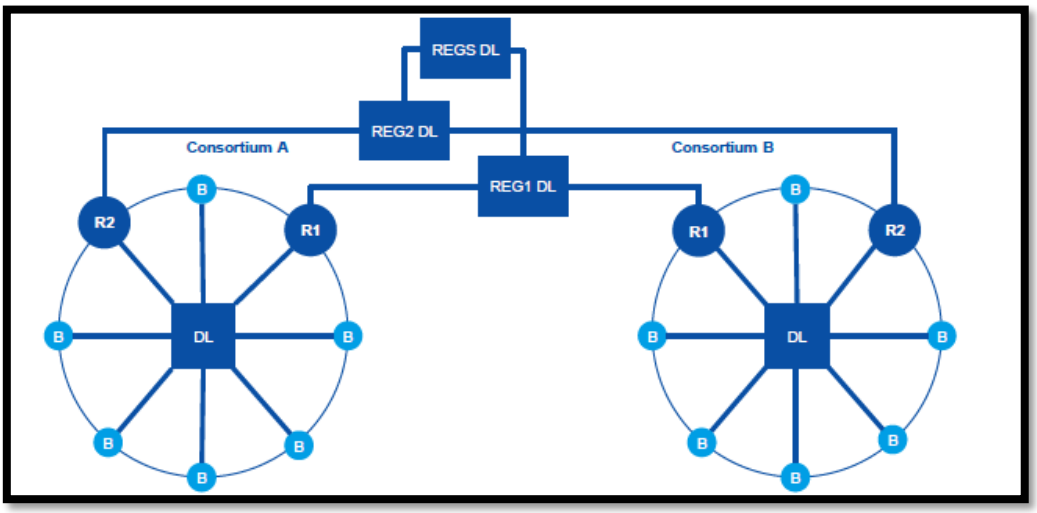
Fuente: BBVA Research

Visto desde este prisma, resulta muy interesante esta segunda opción, sobre todo, en relación a la aplicabilidad del derecho de la UE en este tipo de plataformas. No obstante, hay autores que critican esta forma de organización debido a que se trata de un enfoque muy regional, y que la dirección, en la que se mueve el blockchain financiero en estos momentos, es global.

3.1.3. Reguladores por niveles geográficos.

Esta última opción se basa en una estructura de reguladores de diferentes localizaciones con una presencia en cada consorcio financiero global, de manera que acceden únicamente a la información necesaria para llevar a cabo las actividades de supervisión sobre aquellas entidades que están bajo su paraguas de jurisdicción. Una vez que obtienen la información necesaria para llevar a cabo esa supervisión, cada regulador lo comparte en un registro privado individual, que a su vez forman una red global, donde todos los registros privados de autoridades, combinan la información y monitorizan el sistema global.

Figura 10. Autoridades reguladoras por niveles



Fuente: BBVA research

Para las entidades financieras, está la opción a seguir, debido a que asegura una proyección más globalizada, en la que la regulación local y regional se va diluyendo cada vez más. no obstante, la posición argumentada en este punto, comprende el establecimiento de una organización mundial que regule en última instancia dicho registro, algo que parece incierto en estos momentos.

3.1.4. Estandarización de normas y títulos habilitantes.

Blockchain es una tecnología muy difícilmente regulable, sin embargo, las actividades que se llevan a cabo sobre esta tecnología si pueden ser regulables. De hecho, y como se ha mencionado anteriormente, los Smart-contracts son contratos, al fin y al cabo, por lo que les resulta aplicable la normativa civil y mercantil en esos casos. Por otro lado, dependiendo del contrato que se lleve a cabo en dicha plataforma le será de aplicación una regulación u otra. En este sentido, en el ámbito financiero, y en el caso europeo, será de aplicación toda la normativa de prevención contra el fraude, blanqueo de capitales, regulación del mercado de capitales, etc.

Ahora bien, en el ámbito europeo, se ha puesto en marcha una Directiva que puede poner cerco a los servicios llevados a cabo en la tecnología blockchain. Estamos hablando de la Directiva MiFID II[19], que viene a reforzar las actuales normas europeas

[19] Directiva 2014/65/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 que armoniza la regulación sobre los mercados de valores, los instrumentos financieros que en ellos se negocian, la

sobre los mercados de valores, garantizando que el comercio organizado se realice en plataformas reguladas, introduciendo normas sobre algoritmos y transacciones de alta frecuencia (High frecuency trading[20]) que mejoren la transparencia y la supervisión de los mercados financieros, así como las condiciones de competencia en la negociación y compensación de instrumentos financieros.

En este sentido, resulta fundamental que, a partir de esta nueva directiva, aplicable en 2018, se elabore un Reglamento que tenga en cuenta al blockchain como un factor a considerar en el mercado financiero. Otra de las propuestas, pueden pasar por la estandarización de funciones regulares de código clasificadas en librerías[21] para su uso, así como el mantenimiento de una biblioteca de Smart-contracts aprobados.

Otro de los problemas surge en cuanto a la responsabilidad, porque no podría haber un responsable último por el funcionamiento del registro consorciado, y por la información que está dentro de él. En este caso, la responsabilidad dependería de que el propio consorcio tenga algún tipo de entidad jurídica subyacente o no. Una empresa ad-hoc o una entidad legal creada para administrar el registro aliviaría estos problemas de responsabilidad.

Finalmente, sería conveniente la necesidad de obtener de la autoridad reguladora competente, una licencia o título habilitante, para poder operar como entidad financiera en este tipo de plataformas. Un ejemplo claro se encuentra en el Estado de Nueva York en EEUU, donde es preciso obtener una BitLicense, esto es, una autorización emitida por el departamento de servicios financieros del Estado y poder actuar como agente que realizan actividades empresariales en divisas virtuales.

---

organización y relación con los clientes de las entidades financieras que prestan servicios de inversión y protección al inversor

[20] Se trata de un tipo de transacción que usa software avanzado para realizar operaciones a gran velocidad usando datos financieros rápidamente actualizables. En este concepto, podría encajar Blockchain. Summary of: Directive 2014/65/EU on markets in financial instruments. Extraído de: [url]: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32014L0065

[21] Definición de librería, extraída de Wikipedia: En informática, una librería (del inglés library) es un conjunto de implementaciones funcionales, codificadas en un lenguaje de programación, que ofrece una interfaz bien definida para la funcionalidad que se invoca

3.2 Identificación y Medidas de seguridad de la información personal

Una de las virtudes del blockchain, como se ha mencionado anteriormente, es la capacidad de contener información cifrada e inmutable gracias al funcionamiento intrínseco del registro. Por otro lado, a la hora de celebrar Smart-contracts, es necesario garantizar la autenticidad de la transacción. Para ello, a continuación, se explicarán varios elementos que hacen de los Smart-contracts, contratos con verdadera seguridad jurídica.

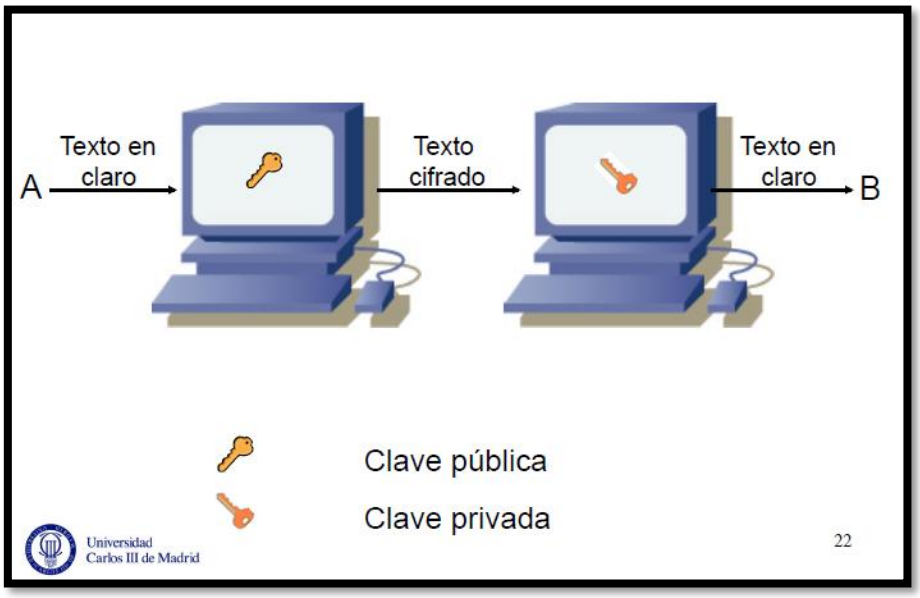
3.2.1. Identificación de las partes e integridad de la transacción

A la hora de contratar dentro de un registro de este tipo (DLTs), es necesario acreditar la identidad de cada una de las partes, ya que, uno de los requisitos del contrato es el consentimiento valido. Por consiguiente, la identificación de las partes, permiten que las mismas en el contrato puedan celebrarlo, de esta manera, las partes garantizan que son mayores de edad y plenamente capaces para su celebración y que, por tanto, el consentimiento no esté viciado y el contrato no sea nulo.

Siguiendo con esta misma línea, la integridad del contrato debe acreditarse de la misma manera, de manera que se pueda probar que el contenido del mismo no pueda haber sido alterado con posterioridad a su celebración.

Gracias a las características del blockchain, esta acreditación es posible, de manera que cabe la posibilidad de mantener inalterable la transacción e identificar a las partes en un contrato. En este sentido, entra en juego la *criptografía* o cifrado al que se someten estas transacciones. Este sistema consiste en un cifrado asimétrico o de clave pública, de manera que utiliza dos claves, una publica y otra privada que se crean y se conectan entre si a través de una función especial. Dicha función es capaz de generar una clave pública a partir de una clave privada (que es la original). Esto permite el cifrado de cualquier transacción con una clave que es publica, y que posteriormente se descifra con la clave privada. Este sistema garantiza dos cosas; por un lado, la integridad del contrato y por otro la confidencialidad del mismo.

Figura 11. Cifrado asimetrico o de clave publica.



Fuente: Presentación Régimen Jurídico de la sociedad de la información. Ribagorda, A.

Cabe destacar que el cifrado asimétrico no garantiza la disponibilidad del contrato ya que por mucho que tengas acceso a la clave pública del contrato, la única manera de acceder al mismo es con una clave privada.

Además, se podría acreditar la identidad de cada contratante a través de la firma electrónica, la cual utiliza el mismo tipo de cifrado (asimétrico), de manera que nos encontraríamos ante una transacción certificada, segura, y autenticada.

Figura 12. Certificación del cifrado asimétrico

Fuente: Presentación Régimen Jurídico de la sociedad de la información. Ribagorda, A.

Otra de las características de este cifrado es el sello del tiempo (tamper-proof), que junto a la firma electrónica son medios que nos validan la transacción en tanto en cuanto garantizan la integridad y no repudio de la misma.

Ahora bien, actualmente para que en Europa sean reconocibles estos medios de autenticación como válidos, son necesarios que se estructuren de conformidad con el nuevo Reglamento eIDAS[22], en donde se establecen los requisitos que debe reunir estos medios para ser válidos[23].

A día de hoy, no está claro si las plataformas blockchain consorciadas encajan dentro de esta regulación o si podrían llegar a ser reconocidas por los reguladores o por los tribunales como entidades de certificación cualificada. No obstante, hay que tener en cuenta el artículo 43 del Reglamento eIDAS, que dice lo siguiente: "*A los datos enviados y recibidos mediante un servicio de entrega electrónica* ***no se les denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales*** *por el mero hecho de que estén en formato electrónico o no cumplan los requisitos de servicio cualificado de entrega electrónica certificada.*". Mientras que si el sistema es cualificado: "*disfrutaran de la presunción de la integridad de los datos, el envío de dichos datos por el remitente identificado, la recepción (…) la fecha (…)"*

3.2.2. Seguridad

Uno de los problemas que despierta mayor preocupación, son los ataques de denegación de servicio que puede ocurrir en este tipo de plataformas, sobre todo, por la naturaleza del registro. Por ejemplo, en el caso de que un hacker decida emitir un gran número de transacciones a la red, podría causar una denegación del servicio disminuyendo el tiempo de procesamiento y a su vez, los diferentes nodos estarían validando transacciones fraudulentas. Esto puede afectar a la seguridad jurídica de contratar en este tipo de plataformas y que puedan ser una alternativa de hecho a los registros tradicionales en cuanto a la validez frente a terceros.

Ahora bien, dentro de un DLT, sería posible que los nodos (bancos) acordaran ignorar o incluso bloquear al emisor de tales transacciones de spam. Sin embargo, si un atacante es capaz de controlar un gran número de clientes, es posible que puedan interrumpir

[22] REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

[23] Artículo 44 del Reglamento eIDAS establece los requisitos de los servicios cualificados de entrega electrónica certificada.

gravemente la red emitiendo grandes volúmenes de transacciones irrelevantes[24]. Esto es, puede darse el caso de que se den "consensus hijacks" que vienen a ser ataques donde se secuestra el consenso. Esto es especialmente relevante en los registros distribuidos como los que quieren establecer las entidades financieras. En este tipo de blockchain, los ataques dependen del número de participantes.

La misma naturaleza distribuida de la arquitectura Blockchain pone de manifiesto la perspectiva de que sería difícil contener un programa malicioso, lo cual hace replantearse la utilización de las mismas. En el apartado de cumplimiento, se profundizará sobre la posibilidad de mutar esas transacciones de manera legal y cuáles son las consecuencias.

Aun así, con las capacidades de los nuevos protocolos que ofrecen almacenamiento de datos y computación, sería posible almacenar datos maliciosos dentro de la red Blockchain y ocasionar daños o inestabilidad al sistema. Además, un hacker podría reasignar el control del Smart-Contract a voluntad, aprovechando la naturaleza de Blockchain para comprar y vender malware entre claves criptográficas[25]. Finalmente, otro de los retos viene de la mano de las penalizaciones derivadas de los protocolos de consenso para los participantes, que básicamente, no existen. De esta manera para un usuario sería más fácil de atacar.

3.2.3. Privacidad y derecho al olvido

En materia de privacidad surgen dudas y cuestiones acerca de cómo podrá aplicarse la normativa europea de protección de datos, y es que, se señala varios problemas relacionados con la identificación del encargado del tratamiento, los riesgos de realizar transferencias internacionales de datos sin cumplir con las exigencias legales o satisfacer el derecho al olvido debido al carácter de inmutable que denota el blockchain.

[24] LAMPORT, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982): 382-401

[25] D. Roffel, C. Garrett, A novel approach for computer worm control using decentralised data structures, December 13th 2014

Por consiguiente, se puede afirmar que la inmutabilidad del blockchain puede representar un problema cuando entra en colisión con los derechos reconocidos en el Reglamento europeo de protección de datos[26].

En este sentido, a la hora de celebrar Smart-contracts que contengan datos de carácter personal, se tiene que tener en mente que, a priori, la información permanece inalterable. Algunas de las soluciones que se han propuesto[27], pasan por la sustitución del derecho al olvido por un derecho a la imposibilidad de uso o acceso por parte de otros agentes en la blockchain, algo que resultaría, por un lado, costoso técnicamente, y por otro, la necesidad de reformular la ley.

Por otro lado, Accenture ha anunciado patentes sobre blockchain editables, a través de un algoritmo especial llamado Camaleón, el cual permitiría editar una transacción e ir "marcha atrás" en la cadena de bloques. No obstante, este tipo de blockchain va a ser analizado más adelante en el epígrafe relativo al cumplimiento normativo.

En definitiva, la tecnología blockchain y los contratos inteligentes son tan flexibles que permitirían una modalidad que garantizara el derecho al olvido. Podrían agregar granularidad a los datos personales y codificar permisos, condiciones y restricciones para su uso. También podrían permitir la portabilidad de datos y proporcionar una pista fácilmente auditable con pruebas de consentimiento. Pero esto hace que surja otra problemática, el hecho de que la regulación europea en protección de datos sea la peor enemiga del blockchain en el sentido de que la posibilidad de entregar a los consumidores el poder de su información personal podría chocar con la característica de inmutable del registro distribuido y hacer extremadamente difícil el uso de esta tecnología en cumplimiento de la ley.

[26] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[27] CERMEÑO, J., *"Blockchain in financial services:Regulatory landscape and future challenges for its commercial application"* working paper extraído de: [url]: https://www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf

3.3 Validez contractual en el Blockchain.

3.3.1. Seguridad jurídica de los DLTs. Validez frente a terceros

Entrando a valorar la validez contractual de los Smart-contracts en una red distribuida, se vuelve al concepto de contrato y que se entiende por el mismo en nuestra legislación civil. Al margen de los requerimientos civiles para la validez del contrato[28], es necesario pararse en la forma del contrato, y es que, la libertad de forma contractual recogida en el código civil tiene como excepción aquellos contratos, que, para su validez, son necesarios que se otorguen bajo documento público. En este sentido, se nos plantea la primera cuestión para con el blockchain, la capacidad de esta tecnología para contratar, por ejemplo, una hipoteca, bajo documento público para así, hacer efectivas las obligaciones propias del contrato.

En el artículo 1216 CC, se establece que "Son documentos públicos los autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la ley.", de tal manera, que nos indica que es necesario un fedatario público para el otorgamiento de escritura pública. ¿Es posible otorgar escritura pública mediante la contratación por una red distribuida?

Se ha discutido durante los últimos años sobre la seguridad jurídica de contratar a través de este tipo de registro distribuidos, y la respuesta frente al otorgamiento en escritura pública es que no existe en blockchain porque, directamente, no se necesita, es decir, un registro de esta naturaleza permite la contratación Inter partes con la posibilidad de hacer valer los efectos del mismo contrato ante terceros, ya que, se presume un conocimiento público[29] de ese contrato y además, en seguridad de la información se presume el no repudio tanto en origen como en destino[30].

Esto supone un cambio en la forma de contratar, no solo en el aspecto logístico (tiempo, costes…) sino también en el aspecto jurídico. Los documentos en la blockchain

[28] Nos referimos al art. 1261 del CC, consentimiento, causa y objeto.

[29] Se trata de una presunción *iure et de iure,* de manera que no cabe prueba en contrario

[30] No Repudio de origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros.
No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente.

realmente podrían ser usados como prueba de su existencia o propiedad. Otra cosa diferente seria que los jueces y tribunales reconozcan algo así. Hay que tener en cuenta que no existe jurisprudencia en este sentido.

3.3.2. El problema de la nulidad retroactiva

El elemento de inmutabilidad del blockchain puede suponer una ventaja para acreditar derechos frente a terceros, pero también supone discrepancias a la hora de la nulidad de un contrato. Por ejemplo, el hecho de que un contrato sea inmutable implica, a priori, que en el caso de que la nulidad contractual tenga efectos retroactivos, no podría tener lugar con los Smart-contracts. Los efectos retroactivos en la nulidad de un contrato suponen que las acciones objeto del contrato vuelvan al estado en el que se encontraban en el momento anterior a la contratación. Por tanto, que será necesario confeccionar suficientemente bien el Smart-Contract para contemplar todas las posibles soluciones.

La legislación financiera está cambiando constantemente. Los nuevos reglamentos entran en vigor cada día, y el derecho internacional se actualiza constantemente. En el mundo inmutable e irrevocable de Blockchain, es probable que cause graves trasformaciones. Es necesario llegar a una solución acerca de cómo deberá adaptarse blockchain a la nueva regulación.

3.3.3. Desaparición de intermediarios en el proceso.

Como se ha mencionado anteriormente, blockchain tiene el poder de actuar como un "notario virtual". En este sentido, utilizando contratos inteligentes, solo pueden ser consumados cuando las condiciones estipuladas se cumplen. Además, cada transacción es visible, trazable, verificable, y segura. Tal como se observa, blockchain supone la solución que todos buscan; no existe modo alguno de que un contrato se llegue a consumar hasta que se hayan completado las condiciones estipuladas. En este contexto, los notarios como fedatarios públicos deben verificar tres aspectos: Que dicha firma se corresponde con la del que dice ser el firmante; Que dicho firmante goza de capacidad jurídica; y que el documento firmado se ajusta a la ley. De esta manera, dentro del Ordenamiento jurídico español, sería necesario que el blockchain se recoja legislativamente como fedatario público capaz de demostrar estos tres requisitos.

No obstante, en Ordenamientos anglosajones, este tipo de registros encajarían más en la figura de notario, debido a que este tipo de fedatarios simplemente dan testimonio de que un determinado documento ha sido firmado Inter partes.

De cualquier manera, lo verdaderamente importante es, que, gracias a esta tecnología es posible la prueba en juicio de estos contratos dada su inalterabilidad y teniendo en cuenta la regla de la sana critica, los jueces, al fin y al cabo, *valoraran de acuerdo a la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados*[31].

Por otro lado, los Smart-contracts probablemente contendrán menos texto que un contrato tradicional. Los términos jurídicos deberán ser traducidos al lenguaje de código, lo cual hace que sea complicado y deja bastante margen para el error. Un ejemplo puede ser el siguiente: los contratos tradicionales suelen contener frases como "aviso razonable" o "en la medida que sea posible". A partir de ahora, los Smart-contracts no permitirán este tipo de condiciones, por lo que se plantean dudas acerca de la redacción de los mismos.

En este sentido, cabe destacar dos hitos importantes. Por un lado, la desaparición del notario como fedatario público para con la contratación bajo documento público, ya que no se necesitaría a partir de entonces, o eso se ha escrito por muchos autores, pero la verdad es que no tiene por qué ser de esta manera. Con el registro de los contratos en el blockchain se permite comprobar solo la integridad y autenticidad del documento, sin embargo, solo el notario o un funcionario público puede dar fecha fehaciente[32], aspecto cuestionable por algunos autores. Por otro lado, la reconversión del abogado tradicional. Esto es, al hablar de estas nuevas tecnologías, se intenta adaptarlas al derecho tradicional, sin embargo, los profesionales de hoy en día son los que deben evolucionar, y en este panorama, deben cambiar de perfil y buscar un acercamiento a la contratación digital e inteligente. Por ejemplo, la figura del abogado no desaparecería ni mucho menos, sino que estaría presente a la hora de redactar las cláusulas de un

[31] von Conta Fuchslocher, Alejandro (2010). «La Sana Crítica». Trabajo de Investigación (Facultad de Derecho, Universidad de los Andes (Santiago, Chile)).

[32] Artículo 1227 del código civil: *La fecha de un documento privado no se contará respecto de terceros sino desde el día en que hubiese sido incorporado o inscrito en un registro público, desde la muerte de cualquiera de los que le firmaron, o desde el día en que se entregase a un funcionario público por razón de su oficio.*

Smart-Contract. Sería necesario por parte del profesional el conocimiento informático para poder codificar ese contrato.

3.4 Demostrar el cumplimiento mediante Blockchain.

Los recientes estudios sobre las RegTech[33] o las tecnologías aplicadas para dar cumplimiento a los requisitos regulatorios, han mostrado que el blockchain puede usarse como una herramienta útil para demostrar ese cumplimiento. El hecho de tener toda la información sobre las transacciones en un registro distribuido en casi tiempo real podría permitir a los reguladores y supervisores monitorear la actividad financiera sin tener que esperar a recibir los informes de las diferentes entidades financieras, y así poder tener, en el futuro, una visión del riesgo en tiempo real y de forma sistemática.

3.4.1. Blockchain como medio para demostrar el cumplimiento ante la prevención contra el blanqueo de capitales o el fraude

Actualmente el sector financiero está sometido a una fuerte regulación en materia de prevención de capitales y contra el fraude[34]. En España, la normativa que regula la materia es la Ley 10/2010 y el reglamento que la desarrolla, aprobado mediante Real Decreto 304/2014 de 5 de mayo[35].

Las principales obligaciones recogidas en esta normativa son las siguientes:

i. Diligencia debida en materia de identificación formal, titularidad real, propósito y seguimiento continuo de las relaciones de negocio. Se trata de la obligación impuesta por la ley de conocer a tu cliente (Know Your Customer KYC)[36]
ii. Obligaciones de información, comunicación y conservación de documentos.
iii. Medidas de control interno, procedimientos, formación, manual de prevención y órganos de control
iv. Fichero de titularidades financieras

[33] Explicado de una manera sencilla, se trata de tecnologías que contribuyen a cumplir con la regulación, o softwares que son creados para facilitar ese cumplimiento.
[34] Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo
[35] Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
[36] Conoce a tu cliente, es una obligación impuesta por la Ley 10/2010 de prevención de blanqueo de capitales y financiación del terrorismo, concretamente en los artículos 3, 4 y 5.

v. Contramedidas financieras internacionales

vi. Régimen sancionador

En este sentido, hoy en día, resulta especialmente caro y se necesita un gran esfuerzo para cumplir con la normativa de blanqueo de capitales y financiación del terrorismo para con las entidades financieras. Asimismo, algunos requerimientos como el "conoce a tu cliente" esto es, la doble identificación de tu cliente, pueden resultar muy lentos y esto puede dar lugar a retrasos en las transacciones, requiriendo en algunos casos entre 30 y 50 días para completarlas a nivel satisfactorio.

Blockchain puede ayudar con el cumplimiento de esta normativa y un ejemplo de la posibilidad de uso de esta tecnología en bases de datos es la red SWIFT[37] que ha creado su "Registro KYC[38]" una plataforma segura y compartida que intercambia datos estandarizados de KYC y que cuenta con más de 1000 millones de relaciones bilaterales en toda la industria. SWIFT es gratuita y ha sido desarrollada con la colaboración de los bancos corresponsales más grandes del mundo para definir un conjunto de datos y documentación en el marco de cumplimiento con KYC. Se trata de una base de datos centralizada, de manera que no se trata, por el momento de una red basada en blockchain. No obstante, el uso de un sistema de distributed ledger (registro distribuido) supondría varias ventajas, como la automatización del proceso y por lo tanto la reducción de tiempo, costes y errores de cumplimiento. Por otro lado, se elimina la duplicación de esfuerzo en los controles de KYC y se podría compartir de manera segura y con todos los bancos en casi tiempo real las actualizaciones sobre la información de los clientes.

Otra de las ventajas sería disponer de una blockchain dedicada a mantener un registro histórico de todos los documentos compartidos y de las actividades de cumplimiento realizadas con cada cliente. Debido a la transparencia en el depósito de la información y su inmutabilidad, este registro serviría para demostrar que la entidad financiera ha

[37] Executive Máster en Dirección de Entidades Financieras (2015) Blockchain. La disrupción en el sector financiero.

[38] The KYC Registry de SWIFT: https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/the-kyc-registry

actuado conforme a la normativa en sus obligaciones de diligencia debida, información, etc.

Un ejemplo de la aplicabilidad del blockchain en materia de cumplimiento KYC, se ha producido en Holanda, donde los bancos en colaboración con *Innopay*[39], han creado un servicio de identidad digital están tratando de crear un servicio común de identidad digital, permitiendo la interoperabilidad entre las entidades. Esto unido al uso de los Smart-contracts, se podría utilizar para automatizar los procesos de cumplimiento en las empresas, ya que una transacción no podría ejecutarse hasta que las dos partes contasen con las adecuadas evidencias de KYC en la blockchain.

Sin embargo, estamos ante una situación similar a la del blockchain como fedatario público, y es que, sería necesario cambiar la ley para considerar a los registros distribuidos o blockchain como fuentes validas de información de clientes. Por otro lado, también sería necesario el desarrollo de la infraestructura basada en blockchain interoperable y compatible con los estándares actuales de la industria.

3.4.2. La auditoría en el blockchain

Cualquier auditoría se caracteriza por la relevancia pública que desempeña al prestar un servicio a la entidad revisada y afectar e interesar no sólo a ésta, sino también a los terceros que mantengan o puedan mantener relaciones con la misma, de manera que puedan conocer la información emitida por la entidad auditada.

Como ya se ha mencionado, una de las características del blockchain y de su tecnología es su inmutabilidad. Por consiguiente, gracias a este elemento, podemos obtener de este tipo de plataformas una prueba irrefutable de la existencia de una transacción, y especialmente, esto resulta útil de cara a mantener un registro de auditoría que garantice la trazabilidad de las transacciones y de la propiedad de los activos. Esta característica es crucial tanto desde el punto de vista del negocio como desde el regulatorio.

[39] Innopay, servicio que utiliza la tecnología blockchain para realizar pagos, identidad digital y E-business.

Llegado a un punto, gracias la utilización de la tecnología blockchain, con su característica de inmutabilidad, se simplificaría el proceso de auditoría, pudiendo llegar incluso a la auditoria en tiempo real, en el que se automatizaría la comprobación. Asimismo, se incrementaría la fiabilidad de la información auditada y se reducirían los costes asociados.

3.4.3. El mito de la inmutabilidad en el Blockchain

Como ya bien se sabe, en blockchain públicas, como bitcoin, la inmutabilidad es algo inherente al registro y es virtualmente, imposible de hackear[40]. Ahora bien, en el caso de blockchain privadas o consorciadas, la inmutabilidad descansa en el "buen comportamiento" de las entidades financieras que forman la red. De esta manera, resulta perfectamente posible y fácil el hecho de que los participantes en una cadena se pongan de acuerdo para romper con esa inmutabilidad si lo deciden juntos. Al fin y al cabo, el blockchain se basa en el consenso[41].

Por tanto, el elemento discutible es la posibilidad de rebobinar una transacción al momento previo al mismo, algo que en el caso de los registros privados es perfectamente posible sin el establecimiento de unas normas o protocolos legítimos de consenso.

En este sentido, nos referimos a la posibilidad de llevar a cabo un rebobinado legal que permita o que pueda ser trazable por las autoridades competentes. Accenture, teniendo como base esta idea, ha desarrollado un método de poder reemplazar la transacción problemática (bien por errónea o bien por exigencias legales) por otra en la cadena o bien poder ser eliminada. Esto es posible utilizando un hash particular, llamado

[40] Para poder hackear una red de blockchain, es necesario realizar el llamado "ataque del 51%", que viene a ser un ataque al 51% de nodos que componen la red de manera simultánea, algo imposible en una red pública.

[41] Ejemplo: Imaginemos un Registro privado utilizado por seis hospitales para agregar datos sobre infecciones. Un programa en un hospital escribe un conjunto de datos grandes y erróneos a la cadena, lo cual es una fuente de inconvenientes para los otros participantes. Unas pocas llamadas telefónicas más tarde, los departamentos de informática de todos los hospitales están de acuerdo en "rebobinar" sus nodos de vuelta una hora, borrar los datos problemáticos, y luego permitir que la cadena continúe como si nada hubiera pasado. Si todos los hospitales están de acuerdo en hacerlo, ¿quién va a detenerlos? De hecho, aparte del personal involucrado, ¿quién sabrá siquiera que sucedió?

Camaleón, que permite, en cualquier caso, que cuando una transacción sea modificada, deje rastro de la misma.

Esto supone la posibilidad de retrotraer los Smart-contracts a un momento inicial o ejercer el derecho al olvido en caso de contener datos personales, no obstante, la mayoría de consorcios en el sector financiero se mostraron reticentes a adoptar este tipo de hash.

Sin embargo, esta opción sería la ideal, siempre y cuando se fijen unas normas y una supervisión de estas acciones, de ahí la necesidad de una regulación y un regulador. Por tanto, se puede constatar que la inmutabilidad en el blockchain está bastante lejos de clasificarse como una pregunta de "si o no". Dependerá de los casos y los usos que se le den a esta tecnología, y también de la normativa que se aplique en estos casos.

Por ejemplo, para aquellos que prefieren las criptomonedas y quieren evitar el dinero de curso real y el sistema bancario tradicional, tiene perfecto sentido en utilizar una blockchain basada en un algoritmo de consenso "proof of work". Si bien, se trata de empresas y otras instituciones que quieren compartir de manera segura sus bases de datos, entonces necesitaran una inmutabilidad basada en el buen comportamiento de la mayoría identificada como validadores (bancos y reguladores), y fundamentada por contratos y la ley.

4. Conclusiones

A modo de conclusión, cabe destacar la importancia que esta tecnología está teniendo en el ámbito del bitcoin, especialmente, de cara a la implementación de criptomonedas. No obstante, a día de hoy, blockchain continúa avanzando, explorando nuevos usos y modelos de negocio.

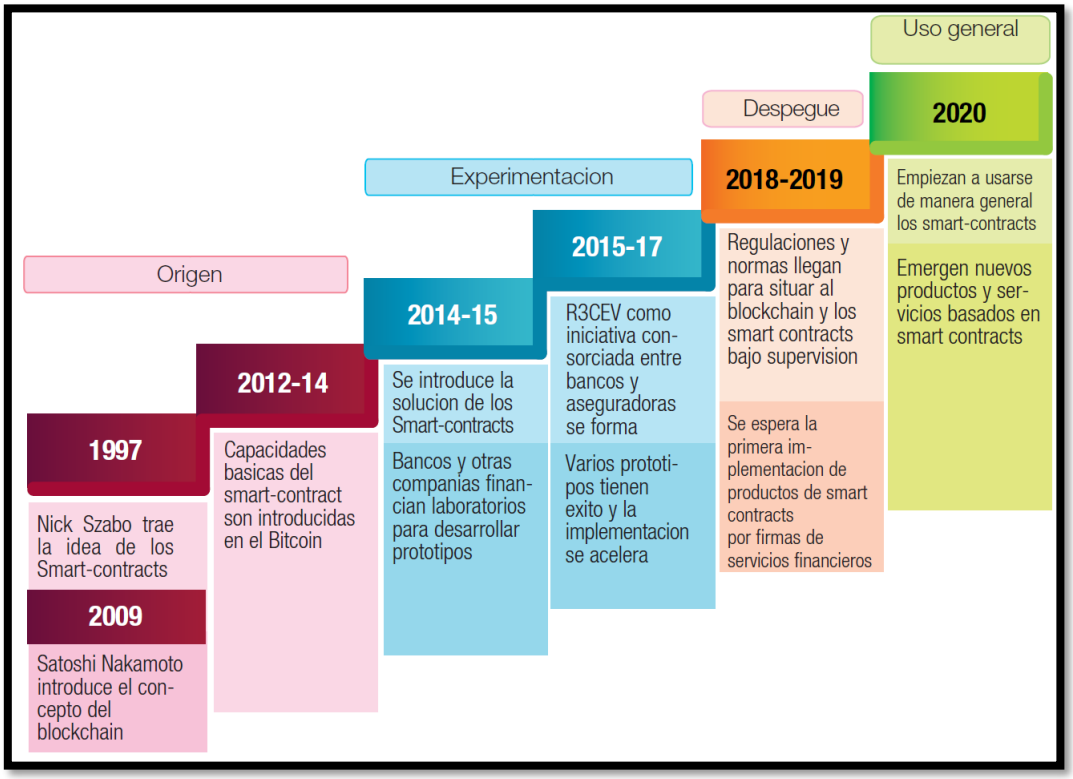
Uno de estos usos, son los Smart-contracts o contratos inteligentes, lo cual hace que la contratación mediante esta tecnología, se convierta en fiable, segura y rápida. En el aspecto jurídico del blockchain, se llegado a una serie de conclusiones diversas sobre sus implicaciones en los diferentes ámbitos del derecho, las cuales tienen su propia valoración, pero siempre con un denominador común, que es la concepción tan liberal

que tienen este tipo de contratos, es por ello, que el bitcoin tenga tan mala repercusión, porque escapan del mundo financiero tradicional.

El hecho de ser una tecnología cuyos prototipos están germinando durante estos últimos años, hace que operen al margen de la normativa actual y precisamente no buscan acercarse a la misma. Se intenta ver al blockchain como una tecnología que aporta muchas ventajas, pero no se advierte de las consecuencias jurídicas que puede tener.

Se ha mencionado en distintas conferencias y publicaciones[42], que el blockchain viene a ser tan disruptivo como lo fue Internet hace ya más de veinte años. Si bien es cierto que puede que sea disruptivo hasta ese punto, es también verdad que podríamos comparar al blockchain de hoy con el Internet de 1993.

Figura 13. Línea del tiempo de la evolución del blockchain e implementación de los Smart-contracts



Fuente: Capgemini Consulting Analysis. Traducción propia

En definitiva, y teniendo en cuenta los diferentes puntos expuestos anteriormente, se puede concluir en varios aspectos jurídicos que pueden resolverse con la normativa

[42] Artículo sobre el blockchain como el nuevo Internet. Extraído de: [url] https://www.entrepreneur.com/article/288715

actual, otros que necesitarían una regulación específica y otros en los que no caben solución:

- En primer lugar, la necesidad de un órgano regulador que supervise este tipo de redes donde operarían las entidades bancarias. Por consiguiente, sería necesario fijar unas normas estandarizadas a nivel regional o mundial, y unas reglas sobre cómo se incorporarían las entidades bancarias (títulos habilitantes o licencias). Es necesario en este tipo de plataformas que no quede a merced del consorcio financiero que ha creado la red y que así, asuman todo el control estableciendo sus propias reglas y estandares que no permitan cumplir con la ley.
- En segundo lugar, es fundamental que, para que los contratos se celebren de manera legal, funcione un sistema fidedigno de identidad digital que permita la posibilidad de identificación de las partes en un contrato, para ello, el nuevo Reglamento eIDAS viene a introducir disposiciones que aplican a esta tecnología. En esta misma línea, cabe destacar la incompatibilidad de la inmutabilidad del blockchain con la privacidad de las personas, la cual puede verse solucionada mediante modificaciones en los algoritmos de consenso, los cuales pueden ser impuestos legalmente a estas plataformas.
- Por otro lado, este tipo de contratación garantiza seguridad jurídica a través de la confianza depositada en el consenso de las Entidades Financieras que forman la plataforma y que, gracias a la tecnología, se trata de registros cuyas transacciones son válidas frente a terceros. La garantía del no repudio de la información por las partes es algo único del blockchain, pero al final, quedara en manos de los jueces que decidirán si tiene o no validez. Aquí entra en juego la seguridad técnica de los registros privados o híbridos, donde se han constatado ataques cibernéticos y ponen de manifiesto que no son tan seguros.
- Finalmente, la ventaja que nos sirve blockchain para poder demostrar el cumplimiento con la normativa existente y futura, como, por ejemplo, la aplicable en materia de blanqueo de capitales. Cuestión que entra en conflicto con la leyenda de la inmutabilidad en el blockchain, de manera que sería posible alterar las transacciones al gusto de los agentes y participantes. Por tanto, es

necesario introducir medidas y normas que garanticen la posibilidad de alterar esos registros, pero dejando un rastro de esa modificación.

Bibliografía

BARROSO, H. “Blockchain. La disrupción en el sector financiero”, Edit. IEB, Madrid, 2016

BRAINE, L., “Smart Contract Templates: Foundations, design landscape and research directions”, Edit. Barclays Bank PLC, agosto 2016.

CANT, B., “Smart Contracts in financial services: Getting from Hype to reality”, Edit. Capgemini Consulting, 2016.

CERMEÑO, J., “Working paper, Blockchain in financial services: Regulatory landscape and future challenges for its commercial application”, BBVA research, num. 16, Diciembre 2016.

EUROPEAN CENTRAL BANK, “In Focus: Distributed Ledger Technology”, European Central Bank, In Focus Núm. 1 2016.

GENDAL, R., “Corda: An Introduction”, Edit. R3CEV, Nueva York, 2014.

GREENSPAN, G., “The blockchain Inmutability Myth”, Coindesk Mayo 2017, http://www.coindesk.com/blockchain-immutability-myth/ [Fecha de la consulta: 10 de mayo de 2017]

HEIKE, M. “IT in Banks: What does it cost?, High IT costs cal for an eye on efficiency”, Edit. Deutsche Bank, 2012

KUAN HON, W., “Distributed Ledger Technology & Cybersecurity Improving information security in the financial sector”, Edit. ENISA, Diciembre 2016.

LUMB, R., “Editing the uneditable Blockchain. Why distributed ledger technology must adapt to an imperfect world”, Edit. Accenture, 2016.

NAKAMOTO, S. “Bitcoin: A peer to peer Electronic Cash System”, 2009

McLEAY, M., “Money creation in the modern economy”, 2014.

PEREZ-SOLÀ, C. y HERRERA-JOANCOMARTÍ, J., “Bitcoins y el problema de los generales bizantinos”, Edit. RECSI, Alicante, 2014.

PINNA, A. y RUTTENBERG, W., “Distributed ledger technologies in securities post-trading”, European Central Bank, Occasional Paper Series, Núm. 172 abril 2016.

PREUKSCHAT, A. “Blockchain: La revolución industrial de Internet”, Edit. Grupo Planeta, Barcelona, 2017

TUESTA, D., “Smart Contracts: ¿lo último en automatización de la confianza?”, Edit. BBVA research, situación economía digital, octubre 2015.

UK Government Chief Scientific Adviser, “Distributed Ledger Technology: Beyond block chain”, Government Office for Science, 2016

WILLIAMS, P. “Bitcoin, Blockchain & Distributed Ledgers: Caught between promise and reality”, Edit. Deloitte, Centre for the Edge, 2016.

YANG, C., “CFO Insights. Getting smart about smart contracts”, Deloitte, CFO insights Junio 2016.

Bibliografía normativa

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Real Decreto de 24 de julio de 1889, texto de la edición del Código Civil mandada publicar en cumplimiento de la Ley de 26 de mayo último

Real Decreto de 22 de agosto de 1885, por el que se publica el Código de Comercio

REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.