Título del Trabajo Final

Estudio de los aspectos legales, retos y limitaciones en la implementación de tecnologías DLT y *smart contracts* en la sindicación de préstamos corporativos.

Andrés Torrenti-Visiedo
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Nombre Consultor
Josep Cañabate Pérez

Fecha Entrega
01/2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	Estudio de los aspectos legales, retos y limitaciones en la implementación de tecnologías DLT y *smart contracts* en la sindicación de préstamos corporativos.
Nombre del autor:	Andrés Torrenti-Visiedo
Nombre del consultor:	Josep Cañabate Pérez
Fecha de entrega (mm/aaaa):	01/2020
Área del Trabajo Final:	
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*

Resumen del Trabajo (máximo 250 palabras):

La irrupción de la tecnología *blockchain*/DLT y el advenimiento de los denominados s*mart contracts*, o contratos inteligentes, promete revolucionar múltiples aspectos de nuestra vida cotidiana. Esta tecnología tiene el potencial de alterar de manera fundamental y definitiva la forma en la que empresas, personas, gobiernos y administraciones públicas interactúan entre sí. El impacto de las nuevas infraestructuras, servicios y plataformas basados en la tecnología *blockchain* es latentemente disruptivo. En este trabajo estudiamos la irrupción de la tecnología *blockchain*/DLT y los s*mart contracts* en la industria de servicios financieros, y en particular en el sector bancario, con especial atención a las aplicaciones dirigidas a la gestión de la sindicación de préstamos corporativos, la distribución de dichos préstamos en los mercados secundarios, y los servicios de agencia asociados. En la actualidad, se plantean diferentes alternativas técnicas y múltiples interrogantes sobre los aspectos legales asociados a la implementación de dicha tecnología, y se cuestiona la capacidad e idoneidad del marco legal europeo e internacional actual para adaptarse a los cambios que la industria reclama. El siguiente trabajo intenta ofrecer luz al respecto, y presenta de manera crítica la situación actual del desarrollo de la tecnología en el ámbito propuesto, estudiando las limitaciones que en el marco regulatorio y legal actual podrían afectar al desarrollo de esta, con especial énfasis en el ámbito europeo.

Abstract (in English, 250 words or less):

The irruption of the blockchain, and DLT technologies in general, and the advent of smart contracts promises to revolutionise multiple aspects of our daily lives. This technology has the potential to fundamentally and definitively alter the way in which companies, individuals, governments and public administrations interact with each other. The impact of new infrastructures, services and platforms based on blockchain technology is latently disruptive. In this paper, we study the emergence of blockchain / DLT technologies and

smart contracts in the financial services industry, and the banking sector in particular, with special attention to applications in the syndication of corporate loans, secondary market distribution, and loan agency services. Currently, different technical alternatives are considered, and multiple questions raised about the legal aspects associated with the implementation of such technology, as well as the capacity and suitability of the current European and international legal framework to adapt to the changes demanded by the industry. The following work tries to shed some light in this respect, and presents in a critical way the development of the technology in the proposed field, studying the limitations that in the current regulatory and legal framework could affect its development, with special emphasis on a European scope and framework.

Palabras clave (entre 4 y 8):

Blockchain, *smart contracts*, GDPR, R3 CORDA.

Índice

Lista de figuras

1. Introducción

La irrupción de la tecnología *blockchain*/DLT y el advenimiento de los denominados s*mart contracts*, o contratos inteligentes, promete revolucionar múltiples aspectos de nuestra vida cotidiana. Esta tecnología tiene el potencial de alterar de manera fundamental y definitiva la forma en la que empresas, personas, gobiernos y administraciones públicas interactúan entre sí. El impacto de las nuevas infraestructuras, servicios y plataformas basados en la tecnología *blockchain* es latentemente disruptivo. En este trabajo estudiamos la irrupción de la tecnología *blockchain*/DLT y los s*mart contracts* en la industria de servicios financieros, y en particular en el sector bancario, con especial atención a las aplicaciones dirigidas a la gestión de la sindicación de préstamos corporativos, la distribución de dichos préstamos en los mercados secundarios, y los servicios de agencia asociados. En la actualidad, se plantean diferentes alternativas técnicas y múltiples interrogantes sobre los aspectos legales asociados a la implementación de dicha tecnología, y se cuestiona la capacidad e idoneidad del marco legal europeo e internacional actual para adaptarse a los cambios que la industria reclama. El siguiente trabajo intenta ofrecer luz al respecto, y presenta de manera crítica la situación actual del desarrollo de la tecnología en el ámbito propuesto, estudiando las limitaciones que en el marco regulatorio y legal actual podrían afectar al desarrollo de esta, con especial énfasis en el ámbito europeo.

2. DLTs, blockchains y *smart contracts*

2.1 Introducción

Las consideraciones de eficiencia y de coste están siempre detrás de las discusiones alrededor de la implantación de nuevas tecnologías, sin ser excepción las basadas en *blockchain* o DLT[1] y el uso de los "*smart contracts"* o contratos inteligentes. En el caso de los *smart contracts*, por ejemplo, tales eficiencias surgen fundamentalmente del hecho de la utilización de software como soporte y medio para realizar ciertas tareas relacionadas con las obligaciones establecidas por un "contrato tradicional", a través de procesos automatizados y algoritmos que se ejecutan sobre plataformas *blockchain* o DLT, que permiten la ejecución de procesos de una forma descentralizada y segura, y que han de servir para agilizar procedimientos administrativos, o para validar, ejecutar y/o hacer cumplir acuerdos y transacciones. Si bien la automatización en sí misma no es un concepto nuevo (desde la automatización en la industria, hasta la banca en línea, la automatización está y ha estado presente en todos los aspectos de nuestra vida cotidiana desde hace décadas), los contratos, tanto en el ámbito civil como mercantil, son aún en la actualidad

[1] Distributed Ledger Technologies (DLT)

contratos “no automatizados”, donde la tecnología no tiene un papel relevante, que requieren casi en exclusividad de la interacción y el aporte humano para definir, redactar, negociar, concluir, evaluar, dirimir y ejecutar cualquiera de sus actuaciones (con un coste extraordinario en tiempo, recursos económicos y humanos). En este sentido, la automatización de algunos, o todos, de estos procesos pueden traerán considerables beneficios para la administración pública, la empresa y la ciudadanía en general. En este capítulo nos centraremos en presentar las bases conceptuales de la tecnología y la infraestructura que harán posible dicho cambio.

2.2 Distributed Ledger Technologies

Desde un punto de vista técnico, “*Distributed Ledger Technologies*” o DLT por sus siglas en inglés, son simplemente aquellas tecnologías e infraestructuras que permiten la gestión de una base de datos de forma descentralizada por varios participantes o usuarios. Para la gestión distribuida de una base de datos en un sistema DLT, no se cuenta pues con la existencia de una autoridad superior única que ejerza las funciones de árbitro y verificador de los registros almacenados. Los registros (datos, transacciones encuentran guardados, duplicados, en diferentes bases de datos distribuidas dentro de la red, aumentando la transparencia, y dificultando cualquier tipo de fraude o manipulación. Los participantes en una red DLT tendrán una copia idéntica de la base datos compartida, que se actualiza de acuerdo con una metodología de consenso para la verificación de registros (en lugar de confiar en una autoridad central o intermediario para mantener y actualizar los registros).

DLT y *blockchains* comparten un origen conceptual: son fundamentalmente libros de registro de registros digitalizados y descentralizados. A menudo, los términos se confunden, pero se diferencian por un conjunto no compartido de características específicas. Podríamos decir que DLT es un término genérico[2] que abarca a todas las diferentes tecnologías que utilizan, de un modo u otro, una gestión distribuida en la red. *Blockchain* es, en esencia, un tipo de libro de registro distribuido que organiza los datos en bloques, que se encadenan en un modo de solo adición y que son, además, inmutables.

2.2.1 Cadena de bloques: Blockchains

En el sentido más general, una “cadena de bloques” o *blockchain* es una lista de registros o transacciones, llamados bloques, firmados criptográficamente, que se desea mantener y actualizar en el tiempo. Cada vez que se agrega un bloque a la cadena, se vincula al bloque inmediatamente precedente, lo que imprime un orden temporal a los registros que viene determinado por el momento de inclusión en el *blockchain*. Las cadenas de bloques incluyen implícitamente, además,

[2] En el contexto actual sobre el uso de smart contracts, la tecnología DLT (en todas sus formas y variantes, como veremos) es generalmente entendida como la infraestructura básica de soporte y el principal medio de automatización.

dos elementos adicionales: primero, un conjunto de reglas de validación, que definen las condiciones para que los bloques, y los registros que los componen, se incluyan en la cadena de forma ordenada y segura; y segundo, un algoritmo o protocolo para hacer cumplir las reglas de validación en las que todas las partes que registran los datos en la cadena confían.

En un principio, se crearon *blockchains* para transacciones específicas que tenían reglas de validación preestablecidas (por ejemplo, para la transferencia de valor digital en forma de "criptomonedas", como Bitcoin). Sin embargo, otras plataformas posteriores generalizaron el concepto, permitiendo la definición de transacciones arbitrarias y reglas de validación programables, escritas en un lenguaje de programación que permite que se puedan implementar dichas reglas con la garantía de se aplicarán consistentemente a través del protocolo particular que rige la plataforma. Estas nuevas plataformas permitieron la irrupción de los contratos inteligentes, o *smart contracts* , donde se pueden integrar y automatizar varios tipos de cláusulas contractuales (como por ejemplo, en el ámbito de los contratos de financiación, las referentes a los paquetes de garantías, fianzas, condiciones para el pago de intereses, amortizaciones, gastos de transmisión y transaccionales, impuestos, delimitación de los derechos de propiedad, etc.) que rigen las transacciones de activos que pueden ser controlados digitalmente a través del hardware y del software con los que trabajamos. Las transacciones y las reglas de validación que se definen de esta manera se conocen comúnmente como contratos inteligentes, o *smart contracts*, y los sistemas para implementarlas y ejecutarlas se conocen como plataformas de *smart contracts,* como por ejemplo *Hyperledger Fabric*[3] *o Ethereum*[4].

El ejemplo más ilustrativo de una cadena de bloques es un registro de transacciones donde los miembros de una comunidad registran la transferencia de activos entre ellos. Por ejemplo, pensemos en Bitcoin, o cualquier otra criptomoneda. En este caso particular, la regla principal de validez es que un miembro de la comunidad que quiera transferir Bitcoins a otro miembro posea al menos la misma cantidad de monedas que intenta transferir. En lo que respecta a la aplicación de la validación, la solución más sencilla es confiar en un único registro contable, una autoridad central de control, o en términos de un sistema monetario tradicional, un banco.

Una comunidad puede programar una aplicación para transferir monedas y desplegarla en el servidor de uno de los miembros, que se convertiría en el encargado de la aplicación, es decir, en el responsable último de que el programa se ejecute correctamente según lo previsto. Ahora bien,

[3] https://www.hyperledger.org/projects/fabric Hyperledger Fabric es una *blockchain* mantenida por "The Linux Foundation" y diseñada como una base para desarrollar aplicaciones o soluciones con una arquitectura modular. Hyperledger Fabric aprovecha la tecnología de bloques para alojar contratos inteligentes o *smart contracts* llamados "*chaincode*" ("código de cadena") que comprenden la lógica de las aplicaciones del sistema.

[4] https://www.ethereum.org/beginners/ Como otras *blockchains*, Ethereum tiene una criptomoneda nativa llamada Ether (ETH). ETH tiene muchas de las mismas características de Bitcoin. A diferencia de otros *blockchains*, Ethereum puede hacer mucho más. Ethereum es programable, lo que significa que los desarrolladores pueden usarlo para crear nuevos tipos de aplicaciones. Estas aplicaciones descentralizadas (o "dapps") obtienen los beneficios de la criptomoneda y la tecnología de cadena de bloques. Una vez que se "cargan" a Ethereum, siempre se ejecutarán según lo programado.

encomendar a una entidad central única (custodio) dicho poder tiene una serie de riesgos potenciales como, por ejemplo:

- *La introducción de un único punto de vulnerabilidad*. Es decir, si el custodio deja de funcionar correctamente, o simplemente se pierde la conexión, nadie puede hacer ninguna transacción.
- *La existencia de un monopolio de facto en el servicio de administración de la red*. Los custodios normalmente cobran por sus servicios. Las entidades que son responsables de la administración y el buen funcionamiento de la red están en una posición de poder para aumentar sus tarifas al amenazar con bloquear usuarios o relajar el nivel de servicio.
- *El control del algoritmo de red* ("Big Brother"). ¿Cómo estar seguro de que el custodio no manipula los registros o la aplicación en beneficio propio o de un reducido grupo de miembros de la comunidad? ¿Y si se alteran las reglas de validación?
- *La ingobernabilidad de la red*. La imposibilidad de llegar a un acuerdo sobre quién debe gestionar la red.

Todas estas cuestiones motivaron el desarrollo de protocolos de validación de registros descentralizados con garantías sobre la inmutabilidad de los datos almacenados, y con el ideal de proporcionar a los miembros de la comunidad con un mecanismo para compartir la tarea de validación entre ellos. Dichos protocolos de validación, que son la base de las tecnologías y plataformas *blockchain*, se clasifican en dos categorías, según el conocimiento de las identidades de las partes (participantes o usuarios) que realizan y participan de las transacciones: cadenas de bloques con y sin permiso; esto es: "*permissioned blockchains"* vs. "*permissionless blockchains*".

2.2.1.1 *Permissioned blockchains* vs. *permissionless blockchains*

En las cadenas de bloques "permitidas" (con permiso) existe un mecanismo externo que permite la identificación de las partes que desean agregar registros en la cadena de bloques (identificación de los miembros de la comunidad) y/o participar como validadores de transacciones (asumiendo -descentralizando- así las tareas que un custodio, o administrador de red único realizaría). Los protocolos que se pueden aplicar a las *permissioned blockchains* se han estudiado durante décadas en el campo de sistemas distribuidos, donde se les conoce como protocolos "bizantinos tolerantes a fallos" ("*Byzantine Fault-Tolerant protocols*" o BFT[5]), aunque han sido objeto de una atención renovada más recientemente [KIAYIAS, A., RUSSELL A. (2018)] por parte de investigadoresy profesionales como consecuencia de su utilización en diversas plataformas *blockchain*. La plataforma más conocida en este ámbito es el *Hyperledger Fabric*[6], que permite la creación de

[5] [25] LAMPORT, L. SHOSTAK R. PEASE M. *The Bizantine Generals Problem* https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf; [24] KIAYIAS,A.,RUSSELL A. (2018) *Ouroboros-BFT: A Simple Bizantine Fault Tolerant Consensous Protocol*

[6] https://www.hyperledger.org/

cadenas de bloques permitidas con servicios de identificación personalizados y una selección de protocolos BFT.

En las cadenas de bloques sin permiso, o "*permissionless blockchains"*, cualquiera puede agregar registros o contribuir a la validación de las transacciones simplemente "identificándose" con un seudónimo. Las cadenas de bloques sin permiso se enfrentan al desafío de lidiar con un participante malicioso que se valga de múltiples seudónimos diferentes para influir en el protocolo de validación a su favor (una técnica conocida como "*Sybil attacks*"). Casi todas las criptomonedas (Bitcoin, Litecoin, etc.) pertenecen a esta categoría. La plataforma de *smart contracts* más popular, *Ethereum*, también pertenece a esta categoría. Actualmente, el protocolo sin permiso más probado para minimizar el riesgo de un *Sybil attack* es el llamado "*Proof-of-work*"[7] [NAKAMOTO S. (2008)]. En todos los protocolos BFT, un proceso clave es la selección del validador o validadores de transacciones. En las cadenas de bloques permitidas ("*permissioned blockchains"*) esto se puede hacer; por ejemplo, simplemente al azar, aleatoriamente, o siguiendo una secuencia o protocolo predefinido. Sin embargo, en una cadena de bloques sin permiso ("*permissionless"*), este mecanismo no funciona, como vimos, debido al riesgo de los *Sybil attacks*. La idea clave del protocolo *Proof-of-work* a es la introducción de un novedoso "sistema de lotería" para asignar la siguiente ronda de validación: esto es, entregarlo al primer validador que resuelva un puzle criptográfico de alta complejidad diseñado específicamente para ser resuelto sólo por medios de fuerza bruta [TSCHORSH F., SCHEURERMANN B. (2016)], por lo que la probabilidad de ser resuelto es una función de la potencia de cálculo disponible (lo que hace que un *Sybil attack* sea poco práctico, ya que un atacante necesitaría tener más poder de cálculo que la combinación de todos los participantes honestos). La incapacidad para identificar a los participantes en una plataforma *permissionless* (como, por ejemplo, *Bitcoin* o *Ethereum*) tiene implicaciones inmediatas en la privacidad y la protección de datos (como se estudiará posteriormente) con respecto a las plataformas *permissioned*. En este sentido, si bien es cierto que dicha incapacidad para identificar a los participantes es buena para la conservación de la privacidad del usuario, ya que un individuo puede participar en una plataforma *permisionless* sin revelar su identidad, no lo es tanto en cuanto a que se acepta a individuos u organizaciones desconocidos/as para el proceso de datos y la validación de los registros en el sistema, con la responsabilidad de procesar transacciones ajenas.

[7] También conocido por los investigadores de sistemas distribuidos como "*consenso Nakamoto*", en referencia a la descripción de Bitcoin por Satoshi Nakamoto en [24] NAKAMOTO S. (2008). También ver [26] VUKOLIC M. (2015).

2.3 Smart contracts

¿Qué son los *smart contracts*? Desafortunadamente, no tenemos una respuesta sencilla para esta pregunta, y aún dentro de las comunidades de profesionales legales y de las tecnologías de la información y la comunicación no hay una noción universalmente reconocida de lo que es un *smart contract* o "contrato inteligente". El término *smart contract* se usa de forma razonablemente laxa para definir un amplio rango de características basadas en dos conceptos fundamentales: (i) la existencia de un contrato; y (ii) la propiedad de ser "inteligente". Necesitamos considerar lo que ambos términos significan e implican, así como las diferentes concepciones de un "contrato inteligente" para poder evaluar cómo determinados aspectos de un contrato legal (tradicional) pueden funcionar, replicarse y automatizarse en el contexto de los *smart contracts* y las plataformas basadas en tecnologías DLT.

2.3.1 Elementos de un smart contract

De forma general, un contrato tradicional, expresado en lenguaje natural, sin ningún aspecto elemento automatizable, no se calificaría como contrato inteligente. Por otra parte, y desde una perspectiva el legal, el mero código sin ningún tipo de acuerdo entre las partes que hacen uso de dicho software no puede constituir un contrato el sentido legal, sin importar cuán de efectivo o cuán de inteligente es el código que ejecuta determinados pasos preprogramados. El término "inteligente" en este contexto se refiere realmente a la característica de ser automatizable, es decir, a la habilidad de un software de realizar determinadas tareas (o replicar determinadas cláusulas, por ejemplo) a través de procesos automatizados. El término "contrato" denota un acuerdo constituido por una serie derechos y obligaciones que son legalmente exigibles y ejecutables. Ambas condiciones son los elementos básicos de un *smart contract*.

2.3.2 Contratos inteligentes vs. contratos legales

Algunos autores[8] [CLACK C., BAKSHI V., BRAINE L. (2016)] consideran dos formas básicas de determinar los contratos inteligentes o *smart contracts*: en particular distinguiremos el concepto de "*smart contract* code" del concepto "smart legal contract". En adelante, cuando nos refiramos, de forma genérica, a s*mart contracts* estaremos hablando en realidad de *smart legal contracts* y no de *smart contract* code. *Smart contract* code, o código de *smart contracts*, se refiere a un código o programa basado en lógica condicional (lógica "*if/then*") que evalúa si una o más condiciones preestablecidas se cumplen y, en tal caso, ejecuta unas tareas específicas, que podrían tener una relevancia contractual o legal, pero no necesariamente. El software tomaría los pasos necesarios

[8] [27] CLACK C., BAKSHI V., BRAINE L. "*Smart contract Templates: foundations, design landscape and research directions*" http://www.resnovae.org.uk/fccsuclacuk/images/article/sct2016.pdf (Junio 2016)

para, por ejemplo, asegurar el cumplimiento de determinadas obligaciones (emitir las instrucciones de repago de un préstamo), garantizar la ejecución de determinados derechos (envío de notificaciones de reposesión de un activo arrendado) o ejecutar la transferencia de activos (transferencia de la propiedad), entre otros. Pero, en cualquier caso, no es necesario que estas tareas automatizadas tengan relevancia contractual alguna, y de hecho el *smart contract code* no necesita estar asociado a ningún contrato legal en absoluto. Los *smart legal contracts* por el contrario, se refieren a contratos legales que han sido total o parcialmente representados y ejecutados por un código o software o, en otras palabras, que las obligaciones contractuales de una de las partes del contrato se ejecutan a través de las acciones automatizadas de dicho software. Teniendo en cuenta los conceptos básicos de *smart contracts* y enfatizando los aspectos de automatización y ejecutabilidad, CLACK C., BAKSHI V., BRAINE L (2016)[9] han intentado definir los contratos inteligentes de una forma quizá un poco más específica: "*A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution*"

2.3.3 Automatización: smart contracts en entornos DLT

Un *smart contract*[10] no sólo requiere un acuerdo entre las partes, se caracteriza además por ser automatizable total o parcialmente. Para la automatización de acciones se requiere el uso de ordenadores, o hardware sobre el que ejecutar un código. El proceso y ejecución automatizada de contratos, o más concretamente, la ejecución de determinadas tareas asociadas a contratos puede darse perfectamente en el seno de una plataforma DLT[11]. Las plataformas DLT tienen ciertas características que las hacen atractivas para el desarrollo de aplicaciones basadas en *smart contracts*:

- Las plataformas DLT mantienen los datos registrados de forma distribuida dentro de una red de computadoras, de forma que cada uno de los participantes (o nodos) retienen una copia idéntica del registro de datos.
- Mantiener un juego del registro de datos o cambiar los registros en una base de datos compartida requiere el consentimiento de los nuevos participantes de acuerdo con el método de consenso utilizado en la plataforma.

[9] [27] CLACK C., BAKSHI V., BRAINE L. "Smart contract Templates: foundations, design landscape and research directions" http://www.resnovae.org.uk/fccsuclacuk/images/article/sct2016.pdf (Junio 2016)

[10] Los contratos "inteligentes" no son, por otra parte, necesariamente inteligentes; de hecho, en la gran mayoría de los casos no lo son. Un contrato debería considerarse "inteligente" cuando el software es capaz de realizar tareas más complejas (por ejemplo, haciendo uso de algún tipo de inteligencia artificial) que la mera automatización y ejecución de determinadas condiciones preestablecidas relativamente simples.

[11] Aunque *smart contracts*, DLT o *blockchains* son términos que se confunden a menudo, son diferentes.

- Una vez validada y aprobada por los nodos, la información se registra o se actualiza en cada uno de ellos de forma paralela, de forma que la información es idéntica en cada uno de los nodos en cualquier momento.
- La red de ordenadores sobre la que se implementa la plataforma DLT puede ser pública o privada, y tanto el acceso a la red como la capacidad de los participantes de visualizar y/o acceder a datos específicos puede estar restringida.
- En ciertos casos, las plataformas DLT pueden tener uno o más "operadores" con derechos de administración[12] (por ejemplo, para hacer cambios al código que rige la red DLT). En este modelo, los usuarios tienen que estar autorizados (*permissioned blockchain*) por el operador, pudiendo incluso crear sus propias redes DLT ejecutando sus propias aplicaciones. Incluso en un modelo DLT "tradicional" (*permissionless blockchain*), donde no hay un operador de plataforma, hay a menudo un grupo central de desarrolladores que tienen un papel muy parecido en la práctica (en virtud de su conocimiento técnico y su habilidad para influenciar la opinión de los participantes, e incluso construir consenso entre los usuarios).
- La información almacenada en la plataforma DLT pueden ser de tipo estático (nombres, números de cuentas) o dinámico (registro de propiedad, saldo cuentas corrientes, o ejecutables/programables (*smart contracts*).
- Las plataformas DLT puede ser conectadas a sistemas externos y/o fuentes de datos externas confiables (denominados "oráculos") que pueden ser necesarias para la ejecución de los *smart contracts* (por ejemplo, para disponer de los valores actualizados del Euribor/Libor para determinar el tipo de interés aplicable en un préstamo corporativo).
- Usar la plataforma DLT como la base sobre la cual concluir o ejecutar contratos inteligentes tiene la ventaja de que solo hay una versión software del s*mart contract* embebida en la plataforma. Por lo tanto, las fricciones que pudieran resultar entre las partes contratantes por el uso de diferentes versiones del mismo software se pueden evitar, garantizando la ejecución automatizada de las acciones asociadas a *smart contracts*, que no pueden ser alteradas ni interferidas (las partes entran en transacciones o contratos individuales, cuyos términos se almacenan en la cadena de bloques; una vez que cada transacción o la ejecución de un contrato se confirma -de acuerdo al modelo de consenso aplicable en cada caso/DLT- ésta se encadena a los bloques anteriores en la cadena)

[12] Tener un operador/administrador puede resultar contraintuitivo dada la naturaleza de la tecnología DLT y el concepto subyacente original de sustituir a una autoridad central o cualquier tipo de intermediarios por la confianza en la gestión descentralizada de la propia plataforma, pero sin embargo hay plataformas DLT que se han desarrollado y continúan siendo administradas por un operador central, y que son particularmente relevantes en determinadas aplicaciones y en el uso de *smart contracts* (como por ejemplo, R3 Corda https://www.r3.com/platform/)

2.3.4 Idoneidad y límites para la automatización

En teoría algunas cláusulas contractuales pueden ser susceptibles de codificadas y automatizadas, pero no todas. Claramente los contratos inteligentes se prestan para automatizar acuerdos con condiciones claras y transacciones repetitivas. En cualquier caso, la automatización dependerá del tipo de software que se utilice. Si el software es solo capaz de verificar condiciones sencillas y ejecutar acciones específicas, muchas menos cláusulas serán automatizables que si el software es más sofisticado y puede evaluar e interpretar datos externos, hechos, requerimientos legales o incluso hacer uso de inteligencia artificial y, en última instancia, tomar decisiones por él mismo. En cualquier caso, el software tendría que estar conectado a través de un "oráculo" [GENDAL BROWN, R. (2018)] a fuentes de datos externas para verificar si las condiciones que desatan determinadas acciones se cumplen. A continuación, exponemos algunos ejemplos y consideraciones del espectro de cláusulas automatizables:

- Cláusulas con lógica condicional muy simples (tipo "*if/then*"). Son condiciones fácilmente codificables y automatizables; por ejemplo, una cláusula condicional sencilla que estipulara la obligación de pagar una determinada cantidad, el repago mensual de un préstamo, o la entrega de un determinado activo sobre un pago realizado.
- Aquellas cláusulas condicionales que requieran una evaluación subjetiva, como por ejemplo "para la satisfacción de las partes" puede estar sujeta cierta incertidumbre y necesitar de la intervención humana. En definitiva, la automatización dependerá de cómo interpretable sea una cláusula; dependerá de factores tales como si el clausulado es ambiguo, o si se requiere un juicio razonado para la interpretación.
- Cláusulas que no tienen condiciones o instrucciones de ejecución, sino que meramente estipulan la ley aplicable o la jurisdicción. Estas cláusulas pueden ser codificadas, pero han de distinguirse de las cláusulas automatizables que hemos discutido hasta ahora. Presentan una función conceptual particular pero no implican ninguna acción.
- Cláusulas que requieren de una decisión activa; por ejemplo, ejercer un derecho u otra acción (como la entrega de un activo en concepto de pago en especie o efectivo). Dependerá de si, y hasta qué punto, se concede la autoridad al software.
- Permitir cambios o enmiendas, y extensiones o periodos de gracia (interrumpir la ejecución del *smart contract* cuando se considere oportuno) es difícil de conseguir en plataformas DLT|.
- La automatización es también muy difícil de conseguir en lo que respecta a aquellas cláusulas "no escritas"; por ejemplo, estipuladas en el Código Civil. El software debería estar al corriente de todas las disposiciones legales que afecten a la ejecución del contrato en toda su dimensión.

2.3.5 Ejecución de smart contracts

Como se ha dicho anteriormente, un *smart contract* ha de ser ejecutable alguna forma. Las dos posibilidades generalmente consideradas son: por medio de una ejecución utilizando los poderes y las herramientas que proporciona la ley de una jurisdicción particular (lo que vendría a ser una ejecución legal), o por la denominada "ejecución a prueba de manipulaciones de código" (o "ejecución práctica"). Esta distinción va al corazón de la diferencia entre un *smart legal contract* y un *smart contract code*, sin implicaciones necesariamente legales. Un *smart legal contract* legal debe capaz de ser ejecutable legalmente en un juzgado; en otras palabras, un juzgado reconocería que el acuerdo entre las partes es legalmente vinculante y que, como tal, puede ser ejecutado través de unos determinados medios. En cualquier caso, es importante remarcar que un juzgado no tendría jurisdicción para ejercer dichos poderes donde no hay un acuerdo legalmente vinculante entre las partes. En el caso en el que un contrato inteligente sea solamente un *smart contract code*, que no constituyan acuerdo legalmente vinculante, las partes podrían utilizar la "ejecución practica" o "ejecución a prueba de manipulaciones", y delegar en la tecnología el control de la ejecución de las acciones pertinentes de forma automática. Esta forma de ejecución práctica puede ser posible donde todas las acciones asociadas a la ejecución se pueden llevar a cabo desde el lado de la tecnología (por ejemplo, la transferencia automática de la propiedad de títulos desmaterializados, simplemente modificando los registros correspondientes de un libro de registro donde se almacena la información de la propiedad/titularidad de dichos activos). Sin embargo, la situación es mucho más difícil en los casos en los que el software o la tecnología tienen que interactuar con el mundo real, como por ejemplo en cuando se requiere la entrega de un activo físico. En este sentido se están haciendo muchos esfuerzos en pro de la *tokenización* de activos reales (como activos inmobiliarios o acciones), donde la transferencia de un *token*[13] supone la transferencia de la titularidad del activo real subyacente.

2.3.6 Modelos de smart contracts

En primer lugar, existe una distinción básica entre el "Modelo Integrado" y el "Modelo No Integrado", dependiendo de cómo está escrito el *smart contract*. Cuando el contrato propiamente dicho, en parte o en su totalidad, está escrito en un lenguaje de programación cualquiera lo denominaríamos Modelo Integrado ("*Integrated Model*")[14]. El mismo software se utilizaría para automatizar las cláusulas contractuales y tomar un papel fundamental en la conclusión y la

[13] Un token es un activo digital que está implementado dentro de una plataforma DLT/ *blockchain*

[14] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

ejecución de parte o todo el contrato. En este modelo el código sería sin duda una parte integral y vinculante del contrato; es decir, qué algunos o todos los derechos y obligaciones de las partes estarían escritos en lenguaje de programación y no en lenguaje natural. En segundo lugar, tendremos una situación en la que un contrato inteligente podría estar redactado exclusivamente en lenguaje natural, pero qué incluyera un acuerdo entre las partes para utilizar un software específico para la ejecución o conclusión del contrato (por ejemplo, la utilización de un software para la gestión de las compensaciones asociadas a un incumplimiento de contrato). Este es el denominado Modelo No Integrado ("*Non-Integrated Model*"). Bajo el Modelo No Integrado, el software o código no forma parte del contracto en sí.

Existe otra clasificación de los modelos de contratos inteligentes que atiende a cómo se concluyen y se ejecutan los contratos. En este sentido, podemos diferenciar dos tipos principales (no exclusivos) de modelos[15]:

(i) cuando el contrato puede ser a concluido directamente por él mismo y de una forma autónoma por un software con o sin acuerdo de las partes ("*Conclusive Model*" o "Modelo Concluyente"). En otras palabras, en el "Modelo Concluyente" el software puede formar o crear obligaciones legalmente vinculantes entre las partes; por ejemplo, un ordenador (nodo) ejecutando por sí mismo código en nombre de una de las partes del contrato, puede enviar una oferta de venta de acciones sobre otro ordenador (nodo) que ejecuta código en nombre de la otra parte, que de forma autónoma puede aceptar ofertas de compra y venta de acciones; y

(ii) Adicionalmente, el contrato podría también ejecutarse por un software "automatizado" ("*Performance Model*" o "Modelo de Prestaciones"). En el "Modelo de Prestaciones", y para seguir con el ejemplo anterior, una vez concluido el acuerdo entre las partes, los ordenadores podrían enviar instrucciones a cualquier otra parte para hacer efectiva la compraventa. Si dos ordenadores fueran nodos operando en una red DLT que contiene un registro definitivo de propiedad de un activo, el código que se está ejecutando en las dos máquinas puede ser capaz de realizar una transferencia efectiva del activo simplemente haciendo la pertinente modificación del registro en el libro de registros. Aún cuando esto puede ser más fácil de conseguir en un contexto en el que el "activo" relevante es nativo a un entorno DLT (como las criptomonedas o tokens) se están haciendo ingentes esfuerzos para la *tokenización* de otros activos "reales", como divisas, acciones, bonos o activos inmobiliarios. A su vez, el Modelo de Prestaciones y el Modelo

[15] [13] "*Smart Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

Concluyente pueden cada uno de ellos combinarse con el Modelo de Prestaciones y el Modelo Concluyente. Cada modelo tiene sus particulares problemas y retos legales y tecnológicos. Si los *smart contract* están, o pueden estar, desarrollados en lenguaje natural con solo ciertos aspectos automatizados (como, por ejemplo, la emisión de pagos), o si se pueden también implementar enteramente como contratos enteramente autoejecutables, dependerá del estatus y el desarrollo del marco legal y tecnológico futuro.

3. *Smart contracts:* retos del marco Legal

3.1 Introducción

En el análisis de los *smart contracts* cubriremos dos áreas fundamentales: en primer lugar, la existencia, y los elementos fundamentales, de lo que son contratos legalmente vinculantes y, en segundo lugar, los retos existentes para asegurar la validez y la naturaleza vinculante de los contratos inteligentes, incluyendo: (i) la capacidad legal; (ii) los requerimientos de autoridad; (iii) la identificación y verificación de la entidad; (iv) sobre términos generales y condiciones, y otras leyes; y (v) la forma y los requerimientos necesarios para el registro público. También abarcaremos el estudio de las deficiencias y los errores que se cometen en *smart contracts*, incluyendo: (i) la identificación y asunción de responsabilidades; (ii) la modificación de los contratos inteligentes; (iii) la jurisdicción, la ley aplicable; (iv) la resolución de disputas; (v) confidencialidad y la protección de datos; y (vi) lavado de capitales ("*anti-money laundry*" o "AML"), financiación del contraterrorismo ("*counter-terrorism financing*" o "CTF") y anti corrupción ("*Know Your Customer*" o "KYC").

3.2. Contratos válidos y legalmente vinculantes

3.2.1 Elementos fundamentales

Cada sistema legal tiene su propias a reglas aplicables para la definición de los que es un contrato válido vinculante y, aunque existen unas pautas comunes generales, es importante estudiar cada caso. En el caso alemán, por ejemplo, siendo una jurisdicción de derecho civil ("*civil law jurisdiction")* un contrato se forma por un acuerdo de las partes en base a unos "términos esenciales" [16] . Los términos esenciales deben ser determinados o ser suficientemente determinables (por ejemplo, en la compra de un coche los términos esenciales son la identificación del vendedor y del comprador, la obligación del vendedor de transferir el activo o los derechos

[16] [12] "*Smart contracts: is the law ready?*" (2018) */ White paper prepared by Smart Contracts Alliance*

de propiedad del coche específico, y las obligaciones del comprador de corresponder con el pago del precio acordado y aceptar la transferencia). Continuando con la ley alemana, el acuerdo se forma con una "declaración unilateral y congruente de intención". Una declaración de intención es la expresión de una voluntad para alcanzar un resultado legal específico (por ejemplo, establecer, modificar o terminar una relación legal). Las declaraciones que establecen un contrato son generalmente la oferta por una de las partes y la aceptación de dicha oferta por la otra. Ambas partes pueden hacer sus declaraciones y por lo tanto formalizar el acuerdo con una firma o acordando un contrato que estipula las obligaciones relevantes. Bajo determinadas condiciones, las partes pueden también "declarar" su intención implícitamente por el hecho de realizar ciertas acciones, o por no actuar, o permanecer "en silencio". La existencia y el contenido de cada declaración (oferta/aceptación) debe ser evaluada desde la perspectiva de su respectivo receptor. Las partes pueden por supuesto dar por finalizado un contrato en persona, representados por terceros (un representante legal), o designar terceras partes para entregar o recibir sus declaraciones (un "mensajero"). Si un contrato inteligente está basado en un acuerdo "tradicional", al que las partes acceden de forma convencional (en persona, papel, o por medios electrónicos; es decir que no estamos en la situación de un Modelo Concluyente de contrato inteligente), los requerimientos para la conclusión de contratos válidos serían enjuiciados simplemente como los de cualquier otro contrato no inteligente[17]. En el Modelo No Integrado específicamente, el contrato se redacta en lenguaje natural igual que se haría en un contrato no inteligente. Las partes pueden ponerse de acuerdo, entre otras cosas, en la utilización de un determinado software o tecnología. El contrato se evidenciará por las declaraciones en lenguaje natural pertinentes realizadas a tal efecto por cada parte. Las reglas aplicables en el sistema legal correspondiente determinarán hasta qué punto el acuerdo y su contenido deben determinarse únicamente a partir de la redacción del contrato, o si se tiene que tomar en consideración un contexto más amplio. En el Modelo Integrado, por el contrario, el contrato se redacta en un lenguaje de programación, por lo tanto, debe ser posible determinar o evidenciar el acuerdo sobre los términos esenciales del lenguaje de programación del contrato o una combinación de partes de lenguaje natural y de programación[18]. Como primer paso para determinar si un contrato inteligente alcanza los requerimientos de un contrato legalmente válido, vinculante y ejecutable bajo la ley aplicable, se debería dilucidar si la ley es lo suficientemente amplia como para abarcar los lenguajes de programación como un tipo de lenguaje en el que se pueda redactar un contrato "tradicional" legalmente vinculante. Si la ley no permite la elección libre del idioma en el contrato, o si la definición del "idioma del contrato" no es lo suficientemente amplia para incluir

[17] [12] "*Smart contracts: is the law ready?*" (2018) */ White paper prepared by Smart Contracts Alliance*

[18] [29] Herian, Robert (2018). "*Legal Recognition of Blockchain Registries and Smart Contracts*". EU Blockchain Forum.

un lenguaje de programación, entonces las leyes tendrían que ser enmendadas para permitir de forma expresa a las partes entrar en un contrato escrito enteramente en un lenguaje de programación. El argumento de que un lenguaje de programación puede no ser considerado como un lenguaje fácilmente leíble o entendible, y por lo tanto no apto para todos los tipos de contratos, puede ser rebatido por el hecho de que las partes pueden en cualquier caso entrar en contratos legalmente vinculantes y ejecutables que no están escritos necesariamente en su lengua nativa. Se debería considerar también, a modo general, si existen algunos tipos de contrato dónde no es aceptable la utilización de un lenguaje de programación en ningún caso, como por ejemplo, en contratos con consumidores que no son capaces de leer o entender un lenguaje de programación; o si, por el contrario, puede haber excepciones (a un consumidor se le proporciona con una traducción al lenguaje natural de un contrato redactado en un lenguaje de programación de la misma forma que se proporciona una traducción si el contrato no está escrito en su lengua nativa.

3.2.2 Capacidad de representación

En general las partes de un contrato deben de tener la capacidad legal para entrar dicho contrato; en caso contrario el contrato no será válido ni vinculante, ni legalmente ejecutable. En el Modelo Concluyente, las partes pueden utilizar aplicaciones software para terminar o ejecutar de una forma automática contratos nuevos, o para emitir una oferta o aceptarla, o para generar cualquier tipo de avisos legales o realizar determinadas acciones de acuerdo con el contrato[19] (por ejemplo, el software podría automáticamente pedir un préstamo y cerrar un acuerdo de financiación si hay un banco que aprueba la solicitud). Por lo tanto, surge la pregunta de si el software en sí mismo (el nodo que ejecuta ese aplicativo) podría ser visto como una parte del contrato bajo el Modelo Concluyente o si estaría actuando como el representante, o el agente de una de las partes y, si ese fuera el caso, si tendría la capacidad legal para hacerlo. En la actualidad la respuesta para ambas preguntas es probable que sea no, aunque hay determinados temas legales qué deberían de estudiarse a la hora de conceder a una aplicación software la capacidad legal de llegar a ser una parte del contrato original. Se debería determinar si bajo las leyes existentes, el software que ejecuta automáticamente un acuerdo (si se dan determinadas condiciones) está obligado a actuar meramente como un "mensajero" de las partes o sí podría ser considerado como una parte del contrato (o como un representante, o agente). Nos deberíamos plantear si la capacidad del software para entrar en un contrato debería estar limitada de alguna forma, por ejemplo, requiriendo el consentimiento de la persona que nomina a la "persona electrónica" (aplicación que se ejecuta en el nodo correspondiente), o de todas las personas que utilizan el software.

[19] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

Deberíamos considerar si la creación de una personalidad legal implicaría que la responsabilidad legal (y financiera) recaería sobre el software cómo una persona legal no natural. Si fuera así, deberíamos considerar además si el software necesita poseer sus propios activos (probablemente mantener un cierto nivel mínimo de activos) para hacer frente a sus responsabilidades financieras, en el caso que fuera necesario, con respecto a su contrapartida. Se deberían además desarrollar reglas sobre el software como "persona legal" para cuando tuviera la capacidad y la autoridad de entrar en contratos de forma totalmente independiente, aunque el marco legal existente para compañías ya da una solución a muchos de estos problemas. En resumen, si las leyes existentes no proporcionan una respuesta clara, se debería plantear la modificación del marco legal para facilitar el uso de los contratos inteligentes bajo el Modelo Concluyente, como por ejemplo para reconocer las acciones de las partes en la programación de software para la ejecución automática un contrato, cuándo y dónde las condiciones relevantes se cumplan[20]. Finalmente, también deberíamos de identificar si hay algunas situaciones en las que la ley requiere notificaciones (u otras comunicaciones en relación a contratos) emitidas por una persona legal o natural. Si este es el caso, deberíamos considerar si sería, en tal caso, apropiado enmendar el marco legal existente para permitir tales notificaciones o comunicaciones para que sean entregadas vía software en el contexto de un *smart contract.*

3.2.3 Requerimientos de autoridad

En muchas circunstancias las partes de un contrato desearán determinar si su contrapartida tiene la necesaria autoridad y/o si ha obtenido la aprobación pertinente para entrar en un contrato y/o realizar determinadas acciones. Esto no es único a los *smart contracts* y es común para las partes de un contrato llevar a cabo este tipo de *due diligence* antes de entrar en cualquier tipo de acuerdo. En cualquier caso, en el contexto los contratos inteligentes, las partes pueden intentar llevar a cabo dicha *due diligence* de una forma automatizada o electrónica. En este sentido, deberíamos verificar si bajo el marco legal europeo se permite hacer uso de los registros electrónicos (por ejemplo, a través de un registro central de compañías o agencias de referencias de crédito). En caso negativo, necesitaríamos considerar si los cambios se deben de hacer sobre el marco legal existente para permitir verificaciones automatizadas electrónicas de los niveles de aprobación y de autoridad. Es también necesario considerar sí la infraestructura necesaria existe en la práctica para permitir verificaciones electrónicas de autoridad y de niveles de aprobación (por ejemplo, si existen registros públicos (oráculos) de directores o de resoluciones de consejos de dirección qué pueden ser accedidos y leídos por una aplicación DLT a través de los interfaces pertinentes. Si no

[20] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

es así, deberíamos pensar si existe la necesidad para crear o es puntualizar la creación de dichos registros. Adicionalmente, deberíamos considerar si algunos de los ajustes a las reglas existentes o los principios legales existentes en relación con autoridad ostensible puede ser apropiado en el contexto de los *smart contracts*. En algunos casos, la existencia y el uso de registros electrónicos puede hacerlo más difícil para una persona falsear y aparentar qué se tiene la autoridad adecuada para entrar en un contrato en nombre de una compañía u otra entidad Por otra parte es mucho más probable que los contratos inteligentes se cierren de forma remota por lo tanto otros riesgos como el hacking o fue el robo de identidad digital pueden ser incluso mayores problemas.

3.2.4 Identificación y verificación

Un un reto práctico que surge cuando utilizamos plataformas DLT es cómo identificar la contrapartida si el libro de registros distribuidos habilitas transacciones anónimas o pseudo anónimas. Este puede ser el caso de las transacciones que se registran en referencia a una dirección IP o una dirección de monedero ("*wallet*"). Dependiendo de la jurisdicción y del tipo de contrato inteligente, las partes serán requeridas a identificarse y verificar la identidad y la firma de las contrapartes, sus representantes y otras personas o entidades relevantes (por ejemplo, para satisfacer los requerimientos lavado de capitales ("*anti-money laundry*" o "AML"), financiación del contraterrorismo ("*counter-terrorism financing*" o "CTF") y anti corrupción ("*Know Your Customer*" o "KYC"). Las consecuencias de la disconformidad con los requerimientos de identificación y verificación (*non-compliance*) dependerán del sistema legal relevante. En general, no cumplir con los requerimientos y controles establecidos implica saltarse el marco legal y regulatorio, con los correspondientes riesgos de sanción. Un fallo a la hora de identificar verificar la identidad firma de las personas relevantes podría también cuestionar la capacidad y la autoría de las mismas y, bajo determinados sistemas legales, podría impactar la validez legal y la naturaleza vinculante del contrato en sí mismo[21]. Si los contratos inteligentes se cierran en modo convencional (en persona o en papel) la identificación es la verificación de las contrapartidas y se llevará a cabo como en cualquier contrato tradicional. En cualquier caso, incluso ante una situación semejante, algunas acciones automatizadas que siguen a el cierre del contrato pueden requerir identificación y verificación de identidad, como por ejemplo pagos o ciertas instrucciones. La identificación y verificación de la identidad puede ser más difícil bajo el Modelo Concluyente donde existe un cierre automatizado de contratos. Hasta qué punto la identificación y la verificación de las identidades es posible dependerá en gran medida de las características del software, la infraestructura y las fuentes de datos disponibles. Habiendo dicho esto, se pueden

[21] Por otra parte, pudiera darse que un sistema legal determine que la no identificación de la contrapartida no afecta la existencia de un contrato válido y vinculante, al menos hasta el punto de que las contrapartidas estén suficientemente determinadas (o sean) determinables en virtud de las características la plataforma DLT elegida.

proporcionar procedimientos *ad hoc* de acuerdo con las contrapartidas o los términos de la plataforma DLT. En general, los medios de verificación de identidad electrónica bajo el marco legal aplicable pueden proporcionar una solución a estas consideraciones. Dentro de la Unión Europea la regulación EU No. 910/2014 (eIDAS regulation[22]) contiene dicho marco legal. Además de tratar con otras cuestiones más generales relacionadas a la identificación electrónica de personas, prevé que las "firmas electrónicas cualificadas" se consideren equivalentes a las a las firmas manuscritas. Se tendrá que desarrollar otra aproximación plausible para ligar la identidad digital de una persona o de una entidad legal con su identidad real; por ejemplo, los participantes en plataformas DTL firman las transacciones con una clave privada única. Una posibilidad es que estas claves se reconozcan como firma electrónica. Al menos validaría que una persona con acceso a la clave privada relevante firmara una transacción de esta forma, pero más allá de esto, sí a cada firmante autorizado se le asignara una única clave privada, las contrapartidas podrían utilizar dichas claves como un proxy de las firmas de firmantes autorizados. De esta forma, las listas de especímenes de firmas manuscritas serán eliminadas y la firma será verificada de una forma automatizada.

Algo más de análisis se requerirá para ver si el uso de la criptografía y las claves criptográficas utilizadas para firmar transacciones en plataformas DLT cumplirían con los requerimientos para ser una "firma electrónica cualificada" bajo la regulación eIDAS. Como primer paso, los legisladores deberían determinar qué tipo de pruebas (si las hubiera) aceptarían los tribunales según la legislación legal existente marco en apoyo de una reclamación donde el contrato inteligente ha sido debidamente firmado por la persona indicada por el contrato con su clave privada. En particular, se debe considerar si la evidencia de identificación por medios electrónicos (como las claves criptográficas mencionadas) es admisible. De lo contrario, es posible que las leyes existentes deban modificarse para permitir expresamente que dicha evidencia sea considerada por los tribunales[23]. Además, los legisladores deberían determinar el peso que el tribunal debe dar a tales pruebas y considerar cómo la evidencia puede ser presentada en la práctica. Por ejemplo, se debería tener en cuenta si las claves criptográficas o los certificados digitales deben ser tratados como el equivalente al uso de una firma manuscrita y en qué circunstancias tal evidencia podría ser cuestionada o anulada. Algunas consideraciones prácticas incluyen discernir si los registros impresos de tales claves criptográficas o certificados digitales podrían ser producidos o si pudiera ser preferible (o incluso necesario en algunos casos) examinar dichos registros electrónicos directamente, o confiar en testimonio de las partes, o de un testigo

[22] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[23] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

que haya examinado dichos registros. Al determinar si y cómo debe aceptarse dicha evidencia y el peso que debe tener, los legisladores deben considerar si existe un marco para determinar quién puede actuar como una autoridad de certificación. Una clave criptográfica o el certificado digital puede tener más peso probatorio si es proporcionado o emitido por un proveedor certificado o autoridad cuyas credenciales se puede comprobar Si no existe tal marco, los legisladores deberán crear reglas que rijan la calificación y la garantía técnica que dichos organismos deben aportar. En principio parece que sea mucho más factible en las redes "*permissioned blockchain*," con una entidad o estructura cerrada central de control de acceso y validación de registros y transacciones.

3.2.5 Términos generales y condiciones

La mayoría de las jurisdicciones tienen leyes específicas relacionadas con el uso de "términos generales y condiciones" y/o "términos estándar" aplicables. Los "términos generales y condiciones" son, por ejemplo, de aplicación habitual tanto en el ámbito del consumo y la protección de los consumidores ("B2C"[24]) como en el entorno de las relaciones entre empresas ("B2B"[25]), aunque en éste ultimo de forma mucho menos estricta. En el contexto de los *smart contracts* es necesario considerar, en primer lugar, si (o cuando) un contrato inteligente puede ser entendido como "términos generales y condiciones" ("T&Cs") y, en segundo lugar, de no ser así, cómo dicho contrato inteligente se ajusta a los términos generales cuando éstos son de aplicación. En muchas jurisdicciones, el hecho de que los términos del *smart contract* hayan sido preestablecidos y sean aplicables a un número considerable de contratos es condición suficiente para que éste sea entendido como parte de los "términos generales y condiciones". En este contexto, es importante distinguir entre la estandarización de los términos contractuales y la estandarización del software que puede utilizarse para la implementación de los *smart contracts*; necesariamente, el uso de un software o código standard no implica *per se* que podamos entender dicho *smart contract* como "términos generales y condiciones". En principio, los *smart contracts* tendrán menos probabilidades de ser considerados como T&Cs si se negocian suficientemente entre las partes, o si no han sido proporcionados por unas de las partes. Por ejemplo, cuando usamos una plataforma DLT pública, aunque los términos de dicha plataforma se pueden considerar como que se han proporcionado a los usuarios por los operadores de la plataforma o los desarrolladores (programadores), que son los responsables del diseño del código, un juez podría analizar la cuestión en profundidad, en base a los principios legales existentes en un determinado marco jurídico, y llegar a una conclusión diferente. En segundo lugar, es importante ver si existen determinadas características de los contratos inteligentes que hacen que éstos tengan más dificultades para cumplir las condiciones y los requerimientos aplicables en los términos

[24] Business-to-Consumer

[25] Business-to-Business

generales, o si es necesario un tratamiento especial para los *smart contracts*. En general, las leyes relativas a los T&Cs pueden tomar la forma de términos de obligado cumplimiento o de requerimientos específicos, lo que implica que no se permiten desviaciones fuera de dichos términos. Aquellas cláusulas de un *smart contract* que violan los requerimientos legales obligatorios pueden ser inválidas, creando lapsos y lagunas en el contrato. Además, algunas condiciones generales pueden prohibir el uso de términos potencialmente onerosos o inesperados que requieren la atención de un consumidor o que requieren que el usuario sujeto a tales condiciones acceda a ella de forma que es entendible, lo que plantea problemas de tipo práctico, especialmente en contratos inteligentes en el Modelo Integrado, donde todo está escrito en lenguaje de programación. En este sentido, los legisladores deberían pues, en primer lugar, considerar si (y, de ser así, cuándo) los contratos inteligentes pueden clasificarse como "términos y condiciones generales" según los principios del marco existente, y, en segundo lugar, si dicho marco dificulta el uso de contratos inteligentes en la práctica; por ejemplo, porque los T&Cs han de ser entregados y/o presentados en un medio particular, o porque los T&Cs escritos en un lenguaje de programación pueden ser considerados como "no apropiados", "inciertos", "inadecuados" o "inteligibles" y por lo tanto inválidos, al no cumplir con el requisito de que el contrato sea "justo, claro y no engañoso". Si existen tales requisitos, los legisladores deberían considerar si las leyes han de ser enmendadas para facilitar el uso de contratos inteligentes que se consideren (en su totalidad o en parte) como "términos y condiciones" generales. Esto podría tomar la forma de enmiendas al marco legal actual para proporcionar una mayor flexibilidad en las normas aplicables a todos los tipos de términos y condiciones generales (es decir, para contratos inteligentes y no inteligentes)[26]. Alternativamente, podría hacerse desarrollando condiciones específicas para el uso de contratos inteligentes (por ejemplo, en el ámbito del consumo y la protección a los consumidores, garantizando la existencia de una traducción de los T&Cs al lenguaje natural, si éstos han sido escritos en un lenguaje de programación). Los legisladores también deben considerar si las leyes existentes que rigen el uso de los términos y condiciones generales podrían tener el efecto de invalidar parcialmente el término de un contrato inteligente (por ejemplo, si algunos de sus términos se consideran injusto) y si la ley existente buscaría "llenar" la brecha resultante. Si este es el caso, los legisladores deben considerar si esto es viable en un contrato inteligente.

[26] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

3.2.6 Requerimientos de forma y registro público

En lo que respecta a las plataformas DLT, los legisladores deben determinar si las disposiciones relevantes bajo las leyes existentes son lo suficiente amplias para permitir implícitamente que los registros se realicen y almacenen utilizando DLT. Si las disposiciones pertinentes no son lo suficientemente amplias para reconocer tales registros basados en DLT, se debe considerar si las modificaciones a las leyes existentes son necesarias para hacer esto. En algunos casos, esto puede no ser necesario, si la ley existente no prohíbe expresamente el uso de tales registros o de otra manera cuestionar su validez. Sin embargo, en algunos casos, los legisladores pueden necesitar enmendar las leyes relevantes para expresamente reconocer que un registro digital registrado electrónicamente utilizando DLT debe considerarse un registro válido, siempre que cumpla con ciertos requisitos. Los legisladores deberán estipular los requisitos y el propósito por el cual dicho registro será válido. También se puede requerir que la legislación reconozca o permita específicamente el uso de DLT para un propósito específico. A modo de ejemplo, Francia ha introducido reformas legislativas que proponen el reconocimiento de un registro DLT y sus registros para la representación, transmisión y compromiso de valores no cotizados a discreción de la empresa emisora correspondiente. De nuevo, en otros casos, puede que no sea necesario para proporcionar específicamente dicho reconocimiento en la medida en que la legislación pertinente que establece el registro o su estado de derecho ya es suficientemente neutro desde el punto de vista tecnológico. Los legisladores tendrán que hacer una evaluación al respecto. En este contexto, los legisladores también tendrían que considerar temas relevantes relacionados con los registros basados en DLT, como el nivel de seguridad que debería exigirse, el grado de acceso y confianza del público que se permitiría si el registro estuviera disponible solo en dicha forma, así como la compatibilidad con los requisitos de protección de datos. Como un paso adicional, se podría considerar introducir requisitos relacionados con la participación de terceros (como notarios, autoridades públicas o tribunales) en el proceso de contratación inteligente, teniendo en cuenta que estos terceros pueden desempeñar roles particulares en una transacción, como informar o advertir a las partes sobre ciertas implicaciones de la transacción. En este caso, los legisladores también deben tratar de garantizar que dichos requisitos sean lo suficientemente flexibles para permitir el uso de la tecnología donde corresponda; por ejemplo, al permitir que un tercero valide un contrato inteligente mediante la aplicación de un certificado digital (en lugar de firmar o aplicar físicamente un sello o sello, como se puede hacer para un contrato tradicional). Incumbirá a los legisladores hacer una elección de política acerca de si y en qué medida se deben hacer cambios para los requisitos existentes relacionados con la forma y/o la participación de terceros. Cuando el propósito principal de un requisito de formulario es para proporcionar una función de evidencia y / o transparencia, los legisladores podrían considerar que en el uso de un DLT de acceso público, el registro (o la grabación de transacciones en una plataforma DLT pública) se considera que

cumple esta función. En este caso, pueden decida enmendar la legislación existente para prescindir del requisito o considere que se cumple mediante el uso del libro mayor. Por otro lado, en circunstancias donde un requisito de formulario está (principalmente) allí para proporcionar algún tipo de aviso o advertencia función, los legisladores pueden ser más reacios a relajar tales funciones dada su importancia para garantizar que las partes sean debidamente protegidos (o, al menos, sin riesgo excesivo sin conocimiento o comprensión). En particular, las transacciones de bienes raíces pueden requerir que los acuerdos sean registrados por un notario y los derechos registrados; mientras que los legisladores pueden tener más confianza en el establecimiento de un registro de la propiedad inmobiliaria basado en DLT (siempre que el registro cumpla la transparencia y la evidencia funcionan adecuadamente y pueden mantener la confianza del público), es menos probable que se sientan cómodos eliminando el requisito de registro notarial en la medida en que esto también sirve para advertir a las partes contratantes y darles consejos.

3.2.7 Deficiencias y errores en contratos inteligentes

Es probable que los sistemas legales y los tribunales existentes tengan leyes, normas, principios y herramientas para tratar adecuadamente la asignación de responsabilidad financiera ("*financial liability*") derivada de deficiencias o errores contractuales. Sin embargo, puede ser más difícil para los legisladores evaluar si la aplicación de esas leyes, normas, principios y herramientas a los *smart contracts* resulta en un efecto deseado con respecto a la asignación de la responsabilidad financiera subyacente. Los legisladores deberían considerar adoptar un enfoque común en la ingeniería de software y "probar" la legislación en el contexto de diferentes errores y deficiencias para determinar los resultados probables de la asignación de responsabilidad en virtud de un *smart contract* en el marco existente. En la medida en que se identifiquen fallos o resultados indeseables, la ley podría modificarse en consecuencia[27]. A modo de ejemplo, si el marco legal existente no especifica cómo las pérdidas económicas relacionadas con un defecto en software de código abierto deben asignarse, los legisladores pueden decidir que es apropiado considerar que las pérdidas se circunscriban a un entorno societario ("B2B"), pero no extensible para contratos a consumidores ("B2C"), ya que los consumidores generalmente pueden tener menos capacidad para soportar tales pérdidas. En este caso, los legisladores pueden decidir introducir leyes específicas que establezcan cómo se debe asignar la responsabilidad en esta situación. Alternativamente, los legisladores deben estar preparados para reaccionar ante resultados indeseables a medida que surgen casos en los tribunales como lo harían normalmente. En cualquier caso, los legisladores pueden decidir que las particularidades de los contratos

[27] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

inteligentes significan que las partes contractuales deben específicamente asignación de responsabilidad de dirección (generalmente o en ciertos casos solamente). Alternativamente, pueden decidir facultar a ciertas autoridades tales como reguladores de los servicios financieros para establecer reglas sobre la asignación de responsabilidad para contratos inteligentes, en la medida de lo posible y apropiado. Los legisladores deben considerar si deben ir más lejos y establecer cómo debe asignarse la responsabilidad en ciertas circunstancias. Por ejemplo, en el caso de contratos inteligentes con consumidores ("B2C"), los legisladores podrían establecer que el consumidor no es considerado responsable en caso de cualquier error en el código, el desempeño incorrecto del software, etc., y que esta asignación de responsabilidad anularía cualquier término en conflicto en el propio contrato.

3.2.8 Errores de interpretación

Los legisladores deberían, como primer paso, determinar si las leyes existentes establecen una "doctrina del error" e identificar consecuentemente el impacto que esto puede tener en los contratos inteligentes. Se debería considerar si las deficiencias en la comprensión del software por las partes afectan a la validez de un contrato inteligente. Al considerar esto, se debe tener en cuenta si existen circunstancias por las que esta situación puede estar más justificada: por ejemplo, en el caso en el que la contraparte es un consumidor, los legisladores pueden considerar apropiado permitir al consumidor un margen para subsanar un error o exigir al proveedor de servicios que demuestre que el consumidor no se equivocó. Los legisladores deberían considerar igualmente si diferentes estándares o requisitos deberían aplicarse en circunstancias diferentes: por ejemplo, un menor nivel de comprensión del software puede ser aceptable (no afectaría la validez del contrato) en virtud del Modelo No Integrado, en comparación con el Modelo Integrado.; o si sería apropiado imponer un deber de "buena fe" en los proveedores de servicios de codificación inteligente por contrato, para asegurar de manera razonable que se realizan los mejores esfuerzos para hacer un código consistente con las intenciones escritas y el espíritu del acuerdo entre las partes contratantes (que, por ejemplo, pueden establecerse en un lenguaje natural contrato bajo el modelo no integrado).

3.2.9 Errores de omisión

Como primer paso, los legisladores deben considerar si las leyes existentes contienen las disposiciones necesarias que permiten, en principio, remediar los errores y despejar las lagunas existentes entorno a los *smart contracts*. Si este es el caso, bastará con analizar si el enfoque actual es realmente viable para los contratos inteligentes, por ejemplo, cuando una cláusula de un contrato inteligente viola la protección legal, u otros requisitos y, por lo tanto, se considera un

contrato nulo. En caso contrario, por lo tanto, se tendrán que considerar enfoques alternativos o se desarrollar los remedios y disposiciones legales específicas para dar cobertura a aquellas particularidades propias de los contratos inteligentes que no están presentes o totalmente cubiertas en el marco legal existente.

3.2.10 Errores de software

Los legisladores deben evaluar cómo se asignaría la responsabilidad en virtud de la legislación actual cuando hay un error en el software de un *smart contract*, particularmente en el Modelo Integrado. En particular, los legisladores deberían considerar cómo las leyes existentes cubren un error de software y los principios legales que podrían aplicarse a una situación en la que el error surge bien sea en una plataforma o servicio de código abierto, o en software desarrollado y proporcionado por un tercero. Si el marco legal actual no es claro, los legisladores deberían considerar enmendar las leyes existentes o introducir nuevas leyes para abordar estos temas. Por ejemplo, se puede plantear el desarrollo de "plantillas" para *smart contracts*, que podrían incluir un campo para que las partes indiquen, en el caso que nos ocupa, cómo se acordó que la responsabilidad se asignara en el caso de detectarse un error de codificación[28]. También se puede considerar si sería apropiado proporcionar una advertencia, o mensaje, en el caso de que las partes no acuerden expresamente la asignación de responsabilidad por un error de codificación.

Los legisladores también deben considerar si las leyes existentes prevén los eventos de fuerza mayor ("*force majeure*") que podrían excusar a una o más partes de un contrato de sus obligaciones. Si existe tal marco, se debe evaluar si la descripción de esos eventos de fuerza mayor incluiría, por ejemplo, ataques cibernéticos, indisponibilidad de fuentes de datos o acceso a internet, corrupción de datos, etc. Que son seguramente más pertinentes en el contexto de contratos inteligentes.

3.2.11 Transacciones nulas

Como primer paso, los legisladores deben identificar si las leyes existentes requieren que, en algunas circunstancias (por ejemplo, cuando la transacción es ilegal o imposible, o una de las partes no tienen la capacidad legal necesaria), las partes deben ser puestas en la posición en la que habrían estado si el contrato o la transacción no se hubiera producido (en el caso de una "transacción nula"). Si ese es el caso, en vista de la inmutabilidad de los registros de una plataforma DLT, los legisladores pueden necesitar considerar remedios alternativos que logren

[28] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

los mismos o similares resultados para las partes (por ejemplo, compensación o reversión de la transacción). Sin embargo, en algunas circunstancias, puede que no haya una alternativa adecuada o viable a un *smart contract* nulo; los legisladores deben determinar qué impacto pueden tener las alteraciones de los registros y su impacto en terceros (por ejemplo, cuando se compra un activo después de una supuesta adquisición bajo un contrato inteligente que se declara ulteriormente nulo).

3.2.12 Integridad del libro de registros

Aunque se acepta generalmente que los registros en una plataforma basada en tecnologías DLT son inmutables, puede que no sea siempre el caso[29]: podríamos pensar en un protocolo que permitiera la flexibilidad de modificar registros por mayoría o consenso, o cualquier otro tipo de mecanismo. De hecho, ha habido ya casos en los que se ha producido una alteración de los registros de la plataforma como consecuencia de una violación de la seguridad en el sistema[30].

Aunque alterar los registros y modificar las bases de datos, o eliminar determinadas transacciones del registro, en base a un protocolo de mayorías y supuestos tiene detractores, permanece como una posibilidad. Puede ser necesario incluso por razones legales o regulatorias. Por ejemplo, en el caso de información personal o confidencial.

El *smart contract* podría además proporcionar la posibilidad de enmendarse o actualizarse (particularmente interesante en el ámbito financiero en refinanciaciones y/o restructuraciones) por las partes, bien por autoridad o poder unilateral, o multilateral, autorizándose los cambios a través de firmas electrónicas o claves privadas. Podrían considerarse otros casos, por ejemplo, en el contexto de un contrato de crédito inteligente, si el acreditante acepta la reducción del tipo de interés aplicable, pero el *smart contract* se mantiene inalterado, no se modifica, y el acreditado continúa efectuando el pago de intereses en base al tipo inicialmente acordado, el acreditante puede repagar al acreditado la diferencia correspondiente. Esto podría incluso realizarse a través de un nuevo *smart contract* en "sentido" inverso. Es importante remarcar que, aunque el resultado

---

[29] [10] QUIN, K., GERVAIS, A (2019) "*An overview of blockchain scalability, interoperability and sustainability*"; and
[28] TSCHORSH F., SCHEURERMANN B. (2016) *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies*

[30] https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft

El 17 de junio de 2016, un código de *smart contract* que se ejecuta en Ethereum DLT fue "hackeado" o, más precisamente, ciertas vulnerabilidades en la forma en que se había codificado el contrato inteligente habían sido explotadas. Como resultado, hubo llamadas de los usuarios de Ethereum para cambiar el registro DLT para revertir efectivamente las transacciones que hicieron uso de este truco. Sin embargo, hubo s partidarios y objetores de este enfoque propuesto; estos últimos consideraban que cambiar el registro DLT no era un "remedio" a un defecto de software; el software se había ejecutado correctamente, y exactamente como estaba codificado, y simplemente dio lugar a resultados que algunos no habían previsto y que no eran deseables. Podría decirse que esta "inversión" de la transacción socavaría la inmutabilidad y la naturaleza (en principio, a prueba de falsificaciones) de los registros DLT, que se considera uno de los beneficios clave de la tecnologia DLT. La divergencia en las opiniones entre la comunidad de usuarios llevó a un grupo de ellos a realizar cambios en su versión del software y a revertir las transacciones "deshonestas". Otros los usuarios no lo hicieron, lo que dio como resultado una "bifurcación" o "desdoblamiento" del registro original, en el que dos versiones de dicho registro coexisten. Estas versiones del registro son la horquilla ("fork") Ethereum (para revertir las transacciones falsas) y la horquilla "clásica" Ethereum (aceptar las transacciones falsas como válidas).

financiero es el mismo, las implicaciones factuales y legales son importantes. Por ejemplo, el acreditado toma ahora una posición de riesgo financiero de contrapartida con respecto al acreditante. Además, podría haber implicaciones de tipo fiscal o de tipo legal en el caso de un proceso contencioso entre las partes o una insolvencia.

3.2.13 Ley aplicable y jurisdicción

Las cuestiones que conciernen a la ley aplicable y la jurisdicción no son exclusivas de los *smart contracts* en absoluto, y conciernen a toda situación en la que hay un elemento interjurisdiccional en el contrato. Un ejemplo podría ser el de un contrato inteligente gobernado por ley francesa, donde los servicios que tienen que ser ofrecidos en España, o si el contrato implica la transferencia de propiedad o garantías en España, donde las leyes españolas en materia de comercio internacional, o fiscales aplicarían. En el caso de *smart contracts* sobre una plataforma DLT, la situación se complica ya que la red dispone de nodos en múltiples jurisdicciones lo que puede originar potencialmente cuestiones difíciles de resolver sobre ley aplicable y jurisdicción. Si las leyes aplicables son las leyes de la jurisdicción donde el activo se encuentra físicamente, puede ser un problema de difícil solución, en particular para activos intangibles cuya localización se determine por el registro de propiedad que, en el contexto de un registro distribuido (DLT), puede ser efectivamente cualquier jurisdicción en el mundo. Para las cuestiones relativas a la determinación de la propiedad de los activos y los derechos de propiedad en plataformas DLT podemos encontrarnos con situaciones donde puede no estar claro el criterio a aplicar. La Convención de la Haya de 5 de Julio de 2006[31] ("*Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary*") no parece aplicar en el entorno DLT ya que los activos en garantía no estarían custodiados por ningún intermediario (no hay un registro centralizado ni un gestor del registro designado). En este sentido, las partes pueden buscar una solución DLT intermedia o "híbrida"; un compromiso en el diseño de la tecnología que garantice la existencia de un operador central; una especie de custodio, que garantice la aplicabilidad de las estipulaciones contenidas en la Convención en este caso, y que registraría la propiedad de los activos. Esto implicaría que las partes tendrían un recurso contra el custodio, en relación con los activos en cuestión, mas que un derecho de propiedad directo. La figura del intermediario (u "oráculo") puede verse en soluciones DLT "híbridas", como Corda R3, dirigidas a la industria financiera, como veremos más tarde.

[31] https://assets.hcch.net/docs/3afb8418-7eb7-4a0c-af85-c4f35995bb8a.pdf

3.2.14 Resolución de disputas

La resolución de disputas en el ámbito de los *smart contracts* presenta todo tipo de interrogantes, desde la validez y efectividad de ciertas pruebas digitales en un juzgado, hasta la necesidad de contar con traducciones a lenguaje natural de partes de un contrato inteligente escrito en un lenguaje de programación, o la urgencia de contar con peritos y expertos cualificados que puedan entender y evaluar dicho código. Podríamos pensar en un sistema de arbitraje en paralelo, permitido por el sistema legal correspondiente, que se encargara de la resolución de disputas relacionadas con *smart contracts,* por ejemplo, a través de una cláusula de arbitraje necesario en caso de disputa[32]. La resolución de la disputa por arbitraje implicaría que la decisión del árbitro sería implementada en la plataforma DLT por medio de un intermediario, como los descritos anteriormente, con capacidad para enmendar y actualizar registros. Ese árbitro podría ser automatizado, total o parcialmente, y podría tener control sobre fondos o activos que permitiera resolver la disputa de forma automática sin la intervención de terceros. En cualquier caso, y dependiendo de la evolución y la complejidad de los *smart contracts* parece bastante lógico pensar que los legisladores podrían plantearse la creación de juzgados especializados en la resolución de disputas de contratos inteligentes, de la misma forma que en diferentes jurisdicciones europeas hay ya juzgados especializados en áreas como la construcción, el comercio exterior o las negligencias médicas, con apoyo de expertos y técnicos en la materia.

3.2.15 Confidencialidad

Las diferentes partes que participan en un *smart contract* pueden desear que la existencia del contrato sea confidencial, y que los términos y condiciones del mismo se mantengan privados. Esto se puede conseguir con la inclusión de cláusulas de confidencialidad siempre y cuando el software no se ejecute en un entorno público, por ejemplo, un servidor privado o una plataforma DLT privada. En el caso de la utilización de plataformas DLT públicas, la información puede estar potencialmente al alcance de los diferentes participantes/usuarios de la plataforma, o del operador de ésta, aunque sometido a los términos y condiciones de uso. Mantener la confidencialidad requeriría la restricción de los accesos a la información o, por lo menos, intentar garantizar el anonimato de la información relevante mediante técnicas de encriptación, por ejemplo. En cualquier caso, siempre existirá un cierto nivel de tensión e incertidumbre al utilizar plataformas abiertas, dada la incertidumbre y las potenciales vulnerabilidades a las que se los

[32] [13] "Smart *Contracts: legal framework and proposed guidelines for lawmakers* (2018)" whitepaper by European Bank for Reconstruction and development (EBRD) and Clifford Chance

usuarios se exponen[33]. Además, debemos tener en cuentan las tensiones que aparecen también cuando se quiere garantizar el borrado de información o la gestión y tratamiento de datos personales en una plataforma descentralizada, global y pública.

3.2.15.1 Confidencialidad y GPDR

El Reglamento de protección de datos general de la UE ("*Global Data Protection Regulation*" o "GDPR" por sus siglas en inglés), que comenzó a aplicarse en mayo de 2018, ha producido cambios significativos a las normas de privacidad de datos de la UE y ha provocado una reflexión significativa sobre su impacto en los sistemas basados en tecnologías DLT. Las reglas GDPR[34] se aplican en el contexto de almacenamiento y procesamiento de datos personales, es decir, información relacionada con una persona física identificada o identificable, como un nombre o detalles de una transacción en la que se han comprometido. Los efectos de las reglas GDPR (Reglamento General de Protección de Datos o "RGPD" por sus siglas en español, acrónimo que utilizaremos a partir de ahora) en sistemas basados en DLT y *smart contracts* son demasiado numerosos para discutirlos en detalle (aunque volveremos a ellos en la próxima sección), pero algunos de los temas clave incluyen los siguientes:

- En relación con los datos personales almacenados en un registro compartido en relación con un *smart contract* (por ejemplo, el nombre y la dirección de una persona), existe una dicotomía planteada por el derecho de una persona a ser olvidada en virtud del artículo 17 del RGPD, por una parte, y, por otra, la inmutabilidad de la información que se le presupone a los sistemas distribuidos. Si bien dichos datos personales pueden ser "sellados" criptográficamente, el Grupo de Trabajo del Artículo 29, el organismo asesor de la UE considera que dichos datos personales sellados criptográficamente solo son seudónimos y no son completamente anónimos. En consecuencia, en la opinión de dicho Grupo de Trabajo, incluso este tipo de datos personales con seudónimo permanecería asimismo sujeto a la RGPD. Por otra parte, es importante tener en cuenta que, en cualquier caso, ningún sistema es infalible; se han identificado debilidades que afectan tanto a la seguridad de los datos como a la integridad de los registros y a la eficacia de la utilización de seudónimos en plataformas basadas en tecnologías DLT públicas [28][35].
  Una respuesta práctica puede ser por lo tanto no almacenar los detalles de identificación que hacen que los datos sean "personales" en registro compartido; en su lugar, dichos

[33] [10] QUIN, K., GERVAIS, A (2019) "*An overview of blockchain scalability, interoperability and sustainability*"; and
[28] TSCHORSH F., SCHEURERMANN B. (2016) *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies*

[34] Global Data Protection Regulation (GDPR) https://gdpr-info.eu/

[35] TSCHORSH F., SCHEURERMANN B. (2016) *Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies* Humboldt University of Berlin

datos deben almacenarse en un registro externo, accesible a las llamadas que a él pueda hacerse desde las referencias en un *smart contract* (asumiendo que el código del *smart contract* tiene autoridad y es técnicamente capaz de acceder a la información). Sin embargo, si bien esto puede sonar como una solución simple, tiene desventajas en términos de manteniendo múltiples bases de datos, la vulnerabilidad de la base de datos fuera del sistema a la manipulación, etc.

- Los sistemas basados en DLT a menudo tienen una amplia distribución geográfica. Esto significa que los participantes en el sistema, sus computadoras y las personas cuyos datos se están procesando en relación con un contrato inteligente podrían ubicarse en cualquier parte del mundo. Por lo tanto, es muy probable que los datos personales procesados en relación con un contrato inteligente estén sujetos a las regulaciones de varios jurisdicciones; en este sentido, los participantes deberán preocuparse no sólo por el impacto en RGPD, incluidas las posibles restricciones a la transferencia internacional de datos, pero posiblemente también por las regulaciones de privacidad de datos en todas o muchas de las jurisdicciones en las que los participantes en el sistema, sus computadoras, y las personas cuyos datos están siendo procesados están localizados.
- Para cumplir con el GDPR, es crucial que se identifiquen el "controlador" y el "procesador" en cada sistema basado en tecnologías DLT. En general, el "controlador" es la persona que determina los propósitos y los medios de procesar datos personales, mientras que el "procesador" sólo procesa los datos personales en nombre del “controlador”. Identificar a estas personas y sus respectivos roles puede ser difícil, especialmente dada la naturaleza descentralizada de los sistemas basados en DLT/Blockchain y la capacidad de los participantes de la red para entrar en *smart contract* directamente entre sí, de forma individual (es decir, sin la necesidad de una contrapartida común en todas las transacciones), compartir recursos de igual a igual y agregar o actualizar información en el registro compartido sin necesidad de la autorización de un administrador central. En general, cualquier participante que incorpore datos personales en lpos bloques del registro compartido puede considerarse como un "controlador", bajo el GDPR, de los datos que ha proporcionado o al que tiene acceso a través del sistema, a menos que sea un mero proveedor de servicios tecnológicos que respalde el sistema, en cuyo caso es probable que se caracterice como un “procesador”.
- Incluso cuando los datos personales no se almacenan en registro compartido en relación con un *smart contract* el uso de la misma clave pública para “firmar” varios contratos en nombre de una contrapartida individual puede hacer que esa contrapartida se vuelva identificable, ya que la clave pública es generalmente visible para todos los participantes del sistema. Por lo tanto, las claves públicas pueden convertirse en datos personales sujetos a la GDPR.

Los desafíos planteados por el GDPR para los datos personales y los sistemas DLT son múltiples y pueden requerir que los legisladores identifiquen soluciones prácticas para facilitar el desarrollo de las aplicaciones basadas en *smart contracts*. Este es particularmente el caso de las jurisdicciones de la UE (donde el GDPR tiene un efecto legal directo), pero el amplio alcance extraterritorial del GDPR y la distribución geográfica de los sistemas DLT significa que su impacto probablemente sea mucho más amplio.

3.2.16 AML, CTF, KYC

En la mayoría de las jurisdicciones, determinadas entidades y personas (especialmente en el ámbito financiero, pero no sólo) tienen que cumplir con los requerimientos establecidos por los reguladores en materia de AML, CTF and KYC a nivel nacional, supranacional e internacional. Aunque los requisitos son relativamente similares en diferentes jurisdicciones, los detalles y las consecuencias de su incumplimiento pueden variar substancialmente entre jurisdicciones. Si el *smart contract* sigue un modelo No-Concluyente, utilizando la terminología introducida anteriormente, es decir, que la entrada de las partes en el contrato no está automatizada, probablemente se seguirá un proceso de AML/KYC similar a la de cualquier otro contracto. Sin embargo, en algunos casos, la evolución de una transacción en el tiempo, el mismo cumplimiento del contrato, o su ejecución pueden llevar a la necesidad de realizar nuevos procesos de AML/KYC, por ejemplo, en la transferencia de créditos de una entidad bancaria a otra en el ámbito de un préstamo sindicado, o la absorción de una acreditada por parte de otra compañía o el otorgamiento de garantías adicionales por terceros. En todos estos casos, el software tendría que ser capaz de identificar estos supuestos y ejecutar las acciones relevantes cuando se hayan satisfecho los requerimientos correspondientes de AML/KYC. Para ello, en un modelo de contrato inteligente automatizado (Concluyente), el software tendría que ser capaz de gestionar el cumplimiento de estas condiciones y tener acceso de forma automatizada a la información correspondiente en el formato adecuado, lo cual no es baladí. Además, mantener la confidencialidad alrededor de los procesos de AML/KYC cuando se utilizan plataformas DLT públicas puede, como vimos, suponer un reto importante en determinadas aplicaciones. La disponibilidad de la información de AML/KYC de forma centralizada y confidencial ayudaría enormemente, pero si, por ejemplo, todos o la mayoría de los participantes de una industria decidieran compartir esta información (muy probablemente en un entorno privado). En cualquier caso, no hay una solución única ya que cada participante puede tener diferentes políticas de privacidad y/o obligaciones de confidencialidad.[36]

[36] SWIFT ha desarrollado un registro KYC para la industria financiera: SWIFT KYC Registry

4. Plataformas DLT y Smart Contracts en la Industria Financiera: Sindicación de Préstamos

4.1 ¿Qué es la financiación sindicada de préstamos corporativos?

De forma general, y sin ánimo de ser exhaustivos en la descripción, podemos decir que la financiación sindicada de préstamos corporativos consiste en el otorgamiento de financiaciones corporativas con carácter sindicado; es decir, financiaciones concertadas por un grupo de acreedores (las entidades acreditantes) a uno o varios deudores (las entidades acreditadas). El proceso empieza cuando se manifiesta una necesidad de financiación por parte de la sociedad deudora, que iniciará los primeros contactos con sus "bancos de referencia" (es decir, aquellos con los que habitualmente trabaja y de los que es cliente) para explorar la posibilidad de contratar una determinada financiación (volumen, estructura, términos y condiciones, etc.). A partir de ahí, si el volumen de la financiación es elevado, o el perfil de riesgo y las condiciones de mercado así lo aconsejan, las entidades financieras participantes pueden optar por sindicar el préstamo y asegurarlo (es decir, garantizar la financiación independientemente del éxito de la sindicación bancaria) o no. Los términos y condiciones negociados con los bancos que participan en la estructuración y aseguramiento de la operación quedarán plasmados en un documento de términos y condiciones (*"term sheet"*) y estos términos y la regulación de la financiación se desarrollarán en un contrato de crédito (finalidad, condiciones para el otorgamiento, régimen de amortizaciones, supuestos bajo los cuales el acreedor puede vencer la financiación, etc.). En paralelo, es común que determinadas filiales presten garantía solidaria y a primer requerimiento y/o garantías reales con la finalidad de garantizar la financiación. La sindicación del préstamo es liderada por los bancos aseguradores ("*underwriters*") y organizadores ("*lead arrangers*") que son los responsables de la estructuración de la financiación y la distribución del crédito. Estos bancos son los que se encargan de evaluar la "profundidad" del mercado y el interés de las diferentes entidades bancarias por la financiación. Distribuyen la información y gestionan la distribución (venta) de las participaciones en el préstamo sindicado, estableciendo diferentes segmentos o niveles de participación, dependiendo del interés, el apetito de riesgo y el balance de cada banco participante (distribución del crédito en participaciones de mayor o menor cuantía). La sindicación, y la gestión de la financiación una vez cerrada ésta, core a cargo de un agente administrativo (agente de la financiación, administrativo y de pagos, y agente de garantías), que bien puede ser una entidad independiente o, tradicionalmente, una de las entidades bancarias que garantizan la financiación. El Agente administrativo se encarga, además, de la gestión administrativa de las transferencias (venta y liquidación) de participaciones entre entidades

bancarias y/o fondos de inversión en el mercado secundario, una vez se cierra la sindicación primaria.

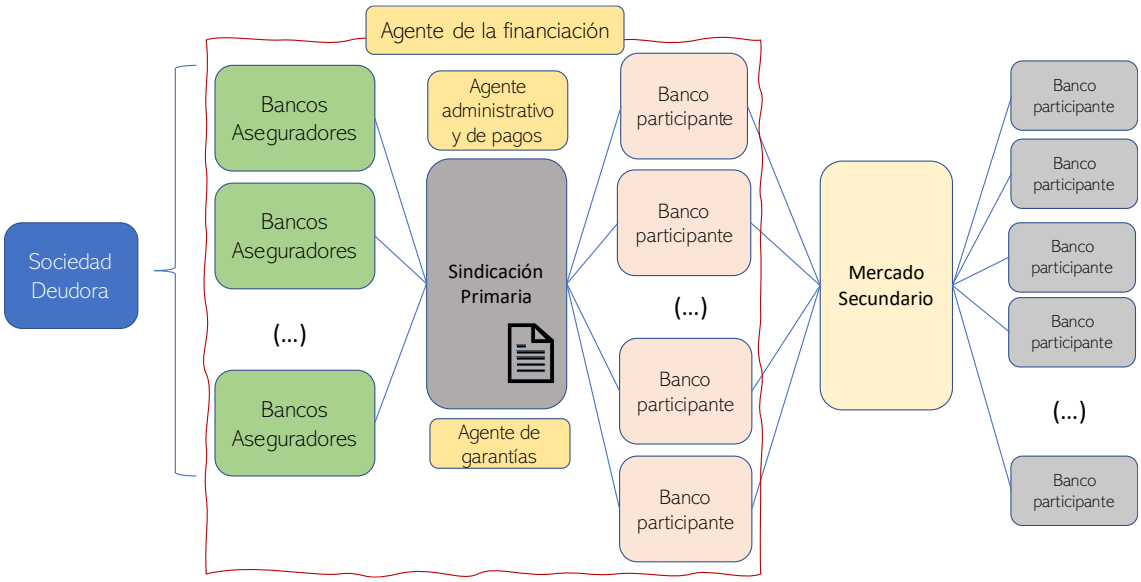

Figura 1.

Sindicación de Prestamos Corporativos

4.2 Impacto de las plataformas DLT y los *smart contracts* en la sindicación de préstamos

La irrupción de la tecnología *Blockchain*/DLT y el advenimiento de los s*mart contracts* promete revolucionar la industria de servicios financieros, y en particular el sector bancario. De entre los servicios financieros asociados a la banca corporativa, el mercado de préstamos sindicados es un área donde se prevé un elevado grado de evolución a medio y corto plazo a causa de la irrupción de nuevos servicios y plataformas basados en tecnologías DLT, la automatización de un mayor número de tareas administrativas y la adopción de los *smart contracts*. Con un mercado descentralizado, un sistema contable distribuido podría servir, por ejemplo, como registro de activos y plataforma de distribución y liquidación para los mercados primario y secundario.

El mercado de préstamos sindicados adolece de tres problemas fundamentales, que las nuevas tecnologías prometen resolver, o, al menos, mitigar[37]:

a) El proceso de sindicación de préstamos en sí mismo, y el precio al que se venden las participaciones, es relativamente cerrado y opaco;

[37] [29] "*Impact of distributed ledger technology on syndicated loans*" Whitepaper Genpact

b) La liquidación de la compraventa de participaciones lleva tiempo, supone una carga administrativa importante para todas las partes implicadas y bloquea cantidades importantes de capital; y
c) Los costes transaccionales y de gestión asociados son elevados.

La forma en la que los nuevos servicios y plataformas DLT prometen resolver estos problemas gira alrededor de los siguientes puntos clave[38]:

1) Almacenamiento de datos distribuido; reducción drástica (¿eliminación?) del riesgo de manipulación, pérdida o disparidad en la información asociada a cada transacción y que se comparte entre los participantes de una determinada financiación (bancos e instituciones financieras, agentes administrativos, agentes de garantías, sociedades acreditadas, asesores legales y financieros, etc.);
2) Autenticación y firma digital; para la autorización, aprobación, ratificación, consentimiento de acciones (o personas) relativas a la transacción de forma segura y eficiente por parte de las entidades participantes (por ejemplo, consentimiento a una prórroga o carencia en el pago de intereses, repago de principal, aprobación de una enmienda al contrato de financiación, liberación de garantías, etc.);
3) Trazabilidad de la cadena de registros y de todas las operaciones y acciones realizadas por los participantes de una determinada transacción;
4) Validación de la información; transparencia y consenso en la información proporcionada y distribuida, en los cálculos realizados (por ejemplo, determinación del EURIBOR aplicable para el siguiente periodo de interés, o cálculo de los intereses devengados y distribuidos a cada entidad participante por parte del agente administrativo y de pagos);
5) Inmutabilidad; seguridad de la información, imposibilidad de falsear los registros compartidos (y validados) y la información distribuida; y
6) Automatización (especialmente en el caso de la implantación de soluciones que se apoyen en la introducción de *smart contracts* sobre infraestructuras DLT); eficiencia administrativa, aumento de la productividad, reducción de costes en la gestión y administración de sindicaciones primarias y la distribución de participaciones en el mercado secundario (especialmente relevante en el mercado de financiaciones apalancadas -en referencia a LBOs/CLOs[39]). Reducción de los costes transaccionales en general, incluidos la distribución de pagos (intereses, amortizaciones), la liquidación en la compraventa de participaciones entre entidades participantes (transferencias de crédito).

[38] [30] PETROV D (2019) "*The Impact of blockchain and distributed ledger technology on financial services* "; and
[29] "*Impact of distributed ledger technology on syndicated loans*" Whitepaper Genpact
[39] Leveraged Buy-Outs (LBOs) / Collateralised Loan Obligations (CLOs)

En este sentido, tenemos:

- Impacto en el mercado primario

  En la actualidad la distribución y venta de participaciones en el mercado primario es un proceso poco automatizado, con un alto grado de participación e interacción humana. Las transacciones de discuten de forma bilateral entre los *desks* de las entidades participantes (entre la entidad que vende o distribuye una participación y la entidad o entidades o que están interesadas -y han sido invitadas- a participar en la financiación). Es un proceso a veces largo y, como comentábamos anteriormente, relativamente cerrado y opaco, donde se comparte la información exclusivamente necesaria para la evaluación del crédito sujeta a la firma de acuerdos de confidencialidad. La introducción de plataformas basadas en tecnologías DLT tienen el potencial de transformar este proceso, para convertirlo en una subasta abierta, con todas las garantías de confidencialidad, seguridad, trazabilidad e inmutabilidad discutidas anteriormente, en la que los participantes tengan acceso a la información necesaria en tiempo real (incluyendo el estado de la sindicación), liberando recursos, aumentando la productividad de los equipos de sindicación para la negociación y la distribución de participaciones, y acelerando el proceso de las financiación -y seguramente reduciendo los precios para la sociedad que busca la financiación.

- Impacto en el mercado secundario

  El impacto en el mercado secundario será, muy probablemente, doble. En primer lugar, un efecto parecido al observado para el mercado primario, es decir, facilitar la distribución de las participaciones, incrementar la eficiencia y productividad de los equipos de distribución, y mejorar la gestión de las carteras de crédito y, por tanto, la gestión del capital regulatorio. En segundo lugar, reducir los tiempos de liquidación de las participaciones una vez efectuadas las operaciones de compraventa (operaciones de "*trading*"). Este problema no es baladí. El tiempo que transcurre entre la confirmación de una confirmación de compraventa y la liquidación de las posiciones puede ser de días, incluso semanas. En una operación de "trading" de participaciones a "par" (compraventa por el 100% del valor nominal) el tiempo de liquidación de las posiciones puede acercarse a las dos semanas. En operaciones a descuento ("*distressed*"), incluso más. Reducir los tiempos de liquidación de posiciones es importante porque: (i) libera capital para la entidad que vende; (ii) los departamentos de *trading* pueden realizar nuevas transacciones de compra o cobertura de riesgo más rápidamente; y (iii) se reducen y limitan los desajustes temporales entre activos y pasivos en libros.

Las razones por las que el tiempo de liquidación es tan elevado es, en parte, debido a la carga administrativa asociada al cierre de las transacciones de compraventa, pero no solo, por ejemplo:

1) La operación de transferencia del crédito debe ser aprobada por el deudor/es;
2) El agente administrativo (agente de la financiación) debe, a su vez, confirmar la validez de la operación (ya que el contrato de financiación impone determinadas restricciones a las transferencias del crédito);
3) El agente debe verificar la titularidad y cuantía de la exposición de la entidad vendedora;
4) El agente debe realizar a su vez las verificaciones asociadas a los procesos de AML/KYC impuestos por el regulador;
5) Los incentivos que el comprador pueda tener para forzar la liquidación en una determinada fecha por determinado tipo de incentivos;
6) El agente puede no estar operativo u operar por debajo de su capacidad normal (por razones técnicas u otras). La gran mayoría de las operaciones de compraventa se concentran en unos pocos días al final de cada trimestre;
7) La gestión administrativa de las transacciones de *trading*, y en general la gestión administrativa de la sindicación de préstamos corporativos, es un proceso relativamente poco automatizado y manual (entrada de datos, verificación de *trades*, procesos AML/KYC, gestión de *waivers*, firma de documentos, etc.)

- Impacto en la gestión administrativa de la transacción (durante la vida de la misma, desde el cierre de la financiación hasta su extinción o refinanciación)

  El impacto en la gestión cotidiana de las transacciones sindicadas puede ser considerable. En particular, y principalmente desde el punto de vista del agente administrativo, la irrupción de nuevos servicios y plataformas DLT y la adopción de los *smart contracts* puede suponer un cambio determinante en la industria. Las tareas administrativas y muchas de las acciones asociadas al cumplimiento de las obligaciones contractuales que realiza el agente administrativo podrían ser automatizadas con la irrupción de los *smart contracts* (en modelo "Integrado" o "No-Integrado") para, por ejemplo: (i) determinar de periodos de interés; (ii) fijar los tipos de referencia (LIBOR/EURIBOR, etc.) para el cálculo de intereses; (iii) calcular los intereses devengados; (iv) distribuir y gestionar pagos; (v) verificar el cumplimiento de ratios financieros; (vi) distribuir y dar acceso a la información en tiempo real; (vii) verificar y/o autorizar *trades*; (viii) liquidar operaciones de compra-venta; etc.

4.3 Retos y restricciones a la implementación de soluciones basadas en tecnologías DLT y *smart contracts* en la Sindicación de Préstamos

Como hemos visto anteriormente, la necesidad de contar en la industria financiera, en particular en el caso que nos ocupa, la sindicación de préstamos corporativos, con una infraestructura que reemplace el ecosistema existente de sistemas difícilmente interoperables (caros, tecnológicamente obsoletos, y de difícil mantenimiento) por otro, más automatizado, flexible, interoperable, confiable y seguro es crucial para garantizar la continuidad y la rentabilidad de determinadas líneas de negocio. A medio y corto plazo, entendemos que el futuro estará dominado por plataformas que garanticen que los acuerdos de financiación, como cualquier otro contrato mercantil, se registrarán, gestionarán y ejecutarán automáticamente, al menos en gran parte, si no en su totalidad; y donde las partes podrán formalizar de una forma más transparente, segura y eficaz, cualquier tipo de transacción comercial y financiera. Pensamos que los mercados financieros evolucionarán hacia un modelo más abierto, donde las entidades colaborarán más estrechamente, compartiendo información con menores fricciones, garantizando la seguridad, fiabilidad y consistencia de las transacciones, y reduciendo los costes transaccionales asociados y los tiempos de gestión, administración y liquidación de estas. Sin embargo, el camino hacia este punto no está exento de dificultades, retos y restricciones, no sólo técnicas sino, y quizá principalmente regulatorias, legales, y otras de naturaleza más estratégica y comercial.

4.3.1 RGPD

Desafortunadamente, a pesar de que el advenimiento de las nuevas plataformas basadas en tecnologías Blockchain/DLT auguraba un empoderamiento individual de los usuarios de dichas plataformas, reduciendo la influencia de organismos de control centralizados, diferentes voces se han alzado para poner de manifiesto el conflicto que existe entre el modo en el que algunas de estas plataformas (y los protocolos subyacentes) trabajan y algunos de los artículos de la RGPD. Algunos autores han advertido especialmente de las consecuencias potencialmente negativas que las restricciones impuestas por la regulación europea pueden tener en el desarrollo de estas nuevas tecnologías en el continente, mientras que otros, por el contrario, entienden que una regulación como la europea es especialmente necesaria y pertinente en este momento para la regulación de los nuevos servicios que se nos ofrecen.

En la normativa RGPD europea, tal y como ya vimos anteriormente, la protección de los datos está en el espíritu de la norma, entendida como un equilibrio estable entre la privacidad y el intercambio libre de información. Las leyes de protección de datos conceden al individuo los

derechos sobre el use de su información personal por terceros, pero también conceden a los "controladores" (aquellos que velan por el cumplimiento del buen uso de las normas) de la información la capacidad de procesar dicha información de determinadas formas, de forma que, a pesar de ello, se respeten los principios fundamentales que se establecen en la norma. RGPD establece los seis principios básicos de la protección de datos[40]: (i) el proceso de los datos debe ser acorde a ley, justo y transparente; (ii) la información debe ser recogida y almacenada por razones específicas y no procesada para usos incompatibles; (iii) la información almacenada y administrada debe ser en todo momento la adecuada y nunca excesiva o innecesaria; (iv) la información recogida debe ser siempre correcta y estar al día; (v) la información no deberá ser almacenada por más tiempo del estrictamente necesario; y (vi) el tratamiento y el almacenamiento de la información deben de hacerse de modo seguro.

RGPD define los roles de controladores de la información ("*data controllers*" o "DC") y procesadores ("*processors*") para asignar las responsabilidades correspondientes. En plataformas Blockchain/DLT privadas ("*permissioned*") existen dos casos posibles: (a) cuando todos los participantes participan en la validación de los registros, siendo en este caso todos ellos considerados como controladores de la información conjuntos o "*joint data controllers*" ("JDC"); y (b) aquellas plataformas que cuentan con validadores especifíficos, en cuyo caso éstos entrarían en la categoría de controladores ("*controlers*"). El hecho de que en las plataformas privadas ("*permissioned*") las identidades de los participantes sean conocidas simplifica las cosas ya que se podrían aceptar las condiciones necesarias previas a la participación (firmar un contrato, aceptación de términos y condiciones) en la forma de forma que existe un acuerdo tácito, previo y vinculante para el cumplimiento de la regla general. Lamentablemente para el caso de las redes públicas ("*permissionless*") la situación no está clara. No sólo el hecho de que todos los participantes de una plataforma publica (¡!) pudieran ser considerados como JDCs, sino también la naturaleza pseudo-anónima de los mismos y la posibilidad (si no certeza) de la transferencia y/o el control de la información por entidades o participantes que pueden encontrarse en jurisdicciones más allá del ámbito europeo. Muchos interrogantes continúan abiertos. Por ejemplo, en relación con la utilización de técnicas criptográficas ("hashes") y claves públicas como datos personales, ¿es un "hash" de información personal información anonimizada?; para plataformas Blockchain/DLT esto significa que se tendrá que poner especial atención sobre dónde y cómo se utiliza la información que puede establecer la conexión entre una clave pública con su propietario, al igual que cuando se almacenan datos encriptados. En cuanto a los principios aplicables sobre el proceso de datos personales, cabe destacar, por ejemplo, que los protocolos actuales subyacentes en plataformas Blockchain/DLT se basan en el mantenimiento de copias enteras del registro general en cada uno de los nodos de validación del mismo, y que este principio

[40] Global Data Protection Regulation (GDPR) https://gdpr-info.eu/

puede estar en conflicto con algunos de los principios de protección de datos tal y como se estipulan en el artículo 5 de la RGPD:

(i) Proceso de los datos acorde a ley, justo y transparente – en un ecosistema descentralizado es imposible garantizar un tratamiento de datos acorde a ley, y la trazabilidad de la responsabilidad asociada a un tratamiento inadecuado de la información es materialmente imposible ya que no se pueden establecer identidades vinculantes.

(ii) Información recogida y almacenada por razones específicas y no procesada para usos incompatibles – similarmente al principio anterior, en plataformas públicas "*permissionless*" es imposible establecer un uso indebido de la información y de establecer las responsabilidades correspondientes.

(iii) Información almacenada y administrada en todo momento la adecuada y nunca excesiva o innecesaria – en este caso, el principio es independiente del uso de unas plataformas u otras ("*permissioned*" o "*permissionless*"). Los consorcios de la industria que en la actualidad lideran el desarrollo de plataformas privadas deberán también sumir su responsabilidad y evaluar si la información que se recoge y almacena para validar los registros y operaciones son los estrictamente necesarios y si dichas reglas de validación son las adecuadas.

(iv) Información recogida/almacenada debe ser correcta y estar al día y (v) no deberá ser almacenada por más tiempo del estrictamente necesario – estos dos principios están relacionados con dos derechos recogidos en la RGPD: el derecho al olvido ("*right to erasure*") y el derecho a la modificación/enmienda ("*right to amend*"). Las plataformas Blockchain/DLT mantienen, por diseño, una copia de todos los registros/transacciones como estrategia de seguridad, garantizando la inmutabilidad e integridad de la información de forma descentralizada. Esto hace que, en la mayoría de las plataformas, sea muy difícil, si no prácticamente imposible, cambiar o enmendar un registro, aún por razones totalmente legítimas. Aunque estas características sean deseables en la muchos casos y aplicaciones, no garantizan los derechos que, a tal efecto, la RGPD establece. En la actualidad hay diferentes alternativas (protocolos, plataformas) que pueden

(v) Tratamiento y el almacenamiento de la información deben de hacerse de modo seguro – tanto en el uso de plataformas abiertas o cerradas ("*permissionless*" o "*permissioned*", respectivamente) el concepto de comunicación segura o tratamiento de la información de modo seguro es más un objetivo que una certeza. La utilización de sofisticados protocolos de autenticación o las técnicas criptográficas más avanzadas van asociadas en algunos casos a un impacto en el rendimiento de las plataformas. La seguridad total no existe y el advenimiento de la computación cuántica pone de manifiesto la necesidad futura de un cambio de paradigma en este sentido.

4.3.1.1 Posibles maneras de garantizar el cumplimiento de la RGPD

Consideraremos dos escenarios de referencia, que son a nuestro juicio los más relevantes[41]

a) Aplicaciones sobre plataformas "*permissionless*" (públicas/abiertas) como "*backend*": en este caso, existe una interacción con una aplicación (o entorno de aplicación) que utiliza una red "*permisionless*" como "*backend*", como por ejemplo "*Ethereum Smart Contracts*". Desde un punto de vista de los roles en las plataformas, los nodos usuarios de la aplicación intermediaria se identifican con los DCs ("*data controllers*"), ya que son éstos los que recogen la información y la almacenan, la validan y procesan. Como tales, son estos nodos los responsables de garantizar el cumplimiento de la RGPD. Actualmente, la única forma de hacerlo sería la de contar con un servidor externo de referencia, identificado y controlado, que realice las funciones de apoyo y control necesarias, y al que los usuarios de la plataforma pudieran referirse para el cumplimiento de la norma. Esta solución plantea cuestiones y dudas sobre el modelo de la descentralización de las plataformas abiertas/públicas y las modificaciones a realizar sobre los protocolos subyacentes.
b) Aplicaciones sobre plataformas "*permissioned*" (cerradas/privadas): en este caso, por ejemplo, un consorcio ofrece la infraestructura base y una serie de servicios a los usuarios finales, verificando, almacenando, validando y procesando las transacciones que se dan en la plataforma garantizando que se cumplen los principios establecidos en la RGPD, garantizando la trazabilidad de las acciones, la seguridad y la privacidad, y estableciendo claramente roles y responsabilidades. En este entorno, todos los miembros del consorcio están claramente identificados y pueden declararse como JDCs ("*joint data controllers*").

4.3.2 Restricciones estratégicas, comerciales o inspiradas en restricciones regulatorias

Muchas son las restricciones que pueden imponerse a la implementación de una solución, de una infraestructura común, o de un estándar *de facto*, si no cuenta con la flexibilidad suficiente para garantizar el cumplimiento del marco regulatorio actual (y futuro), vencer las reticencias naturales de un sector tradicionalmente continuista, contrario al cambio y la innovación, y asegurar una mayor rentabilidad y eficiencia en el negocio. Desde este punto de vista, entendemos que hay una seria de principios básicos que han de respetarse:

1. La infraestructura ha de ser inclusiva, única (o interoperable con otras que funcionen sobre la base de los mismos principios, protocolos y/o estructuras), permitiendo un

[41] IBAÑEZ, LD., O'HARA, K., SIMPERL, E. (2018) "*On blockchains and the General Data protection Regulation"*

reconocimiento de las partes (usuarios) y garantizando la posibilidad de interactuar y realizar transacciones de forma directa;

2. Se ha de asegurar el conocimiento de las identidades de los participantes (las plataformas "*permissionless*", como vimos, no garantizan este requisito). Éste es un requerimiento fundamental tanto para las entidades financieras participantes como para el regulador financiero o las autoridades europeas en materia de protección de datos;
3. Se ha de asegurar la privacidad de los participantes. Esto es, las únicas partes (usuarios) que deben tener acceso a la información de una determinada transacción, realizada o ejecutada sobre la plataforma, son las entidades (usuarios) que participan en dicha transacción, y aquellos que garantizan la validez de la transacción (agentes administrativos, reguladores, administradores de la plataforma, etc.). Igualmente, al punto anterior, no se puede garantizar la privacidad de las transacciones al 100% en plataformas públicas/abiertas;
4. Lógica compartida. Es decir, tal y como avanzábamos anteriormente, que los protocolos utilizados sean inteligibles, o que la codificación de los contratos inteligentes o la lógica que rige la plataforma sea común a todos los participantes;
5. Compatible con el marco regulatorio actual. Es decir, que se cumpla con las exigencias de los reguladores financieros en materia de control y conformidad de las transacciones realizadas (por ejemplo, exigencias de capital, cumplimiento de los procesos de KYC/AML, obligaciones de información satisfechas, etc.) y con el marco europeo de protección de datos, RGPD.
6. Solidez. La industria financiera es especialmente sensible a los errores por lo que la plataforma ha de ser resiliente y sólida, capaz de proporcionar un entorno estable y confiable a las entidades usuarias. Los registros y la información recogida en la plataforma, gestionada y almacenada por los usuarios y gestores ha de ser 100% fiable.
7. Inmutable pero enmendable. Los registros han de ser inmutables, ofreciendo trazabilidad y seguridad a las transacciones, pero ha de garantizarse la flexibilidad necesaria para corregir y/o enmendar transacciones, o términos y condiciones en contratos inteligentes (u otros).
8. La plataforma debe ser actualizable, estable, segura y capaz de gestionar un alto número de transacciones en tiempo real sin errores.

4.3.3 Corda: una solución de consenso para la industria en la sindicación de préstamos

Corda es una plataforma DLT para el proceso, la transmisión, la gestión y el almacenamiento de información compartida[42] como, por ejemplo, la realización de cualquier transacción financiera, o la ejecución de contratos de financiación u otro. Ha sido ideada en base a las necesidades de las instituciones financieras sujetas a regulación. Aunque la solución es una plataforma DLT inspirada en las tecnologías Blockchain, se ha adaptado a la realidad de una industria regulada y sometida a escrutinio y control constante. Corda permite la redacción (codificación) de contratos inteligentes que se ejecutan en la plataforma, y cuenta con una red de "notarios", nodos que garantizan de forma independiente la univocidad de las transacciones y su registro para evitar conflictos. Para asegurar la consistencia de los datos y las transacciones, Corda se basa en "hashes" criptográficos para identificar a usuarios y transacciones. No toda la información es visible a todos los usuarios. Sólo aquellos usuarios que forman parte una transacción, junto con los nodos de control y administración, son capaces de acceder a la información relevante a dicha transacción. El consenso se establece entorno a dos conceptos habituales de las plataformas Blockchain/DLT: (i) la validez de la transacción; y (ii) la unicidad de la transacción. La validez y la unicidad de la transacción (validación del cumplimiento de las condiciones establecidas en el contrato, por ejemplo, y la unicidad de la transacción) es verificada por los participantes en la transacción y por la red de "notarios". La plataforma permite extender la participación a agentes externos ("oráculos") que proporcionen servicios (de información, de control, u otros) pertinentes o necesarios para el normal desarrollo de las operaciones permitidas (por ejemplo, un operador externo o agente, parte en la transacción como proveedor de un índice o tipo de interés necesario, fijado en base a las estipulaciones del contrato por un agente externo, imparcial. Dicho "input" proporcionado por un agente externo, es crucial parala ejecución, desarrollo y control del correcto funcionamiento de la transacción y los protocolos que la regulan. La idea subyacente, además, es que la interoperabilidad de la red sea tal que un día tanto el regulador financiero como juzgados especializados, si fuera el caso, puedan interceder y conectarse para un mayor control y seguridad en el flujo de la información.

El modelo Corda difiere considerablemente del modelo inspirado inicialmente por Bitcoin[43]. Desafortunadamente, el modelo Bitcoin no puede ser aplicado con éxito en un entorno de negocios debido a las limitaciones de rendimiento, escalabilidad y los problemas de seguridad y

[42] [7] GENDAL BROWN, R. *et al* (2016) *"Corda: An Introduction"*

[43] [8] GENDAL BROWN, R. (2018) *"The Corda Platform"*

privacidad que presenta, sin entrar en la incapacidad de adecuarse a un entorno regulado o de garantizar el cumplimiento de la norma RGPD de protección de datos europea. Igualmente, en este sentido, la adaptación de arquitecturas públicas (como por ejemplo Ethereum) a un entorno profesional, y en particular a determinados servicios financieros, está siendo difícil. Parece que existe una preferencia en la industria por una infraestructura más cerrada. Precisamente en esa dirección encontramos las plataformas *Enterprise Ethereum* como *Quorum*, u otras como *Hyperledger Fabric*. Quizá una de las dudas que ofrecen estas soluciones es que su implementación se entiende como la creación de redes independientes, aisladas, específicas de cada caso, lo que presenta potencialmente un inconveniente porque los activos transferidos y las transacciones realizadas en estas redes pueden no ser fácilmente reutilizables o validables en otras. El problema de la interoperabilidad no es baladí. La necesidad de encontrar un consenso entre todas las entidades financieras (la interoperabilidad no es una opción es una necesidad) está manera forzando la colaboración entre ellas y parece que Corda (Corda R3, donde participan, entre otros BNP Paribas, BNY Mellon, HSBC, ING, Natwest, etc., es una prueba de ello) puede convertirse en la solución *de facto* apoyada por la industria.

5. Conclusiones

La irrupción de la tecnología *blockchain*/DLT y el advenimiento de los denominados *smart contracts*, o contratos inteligentes, promete revolucionar y alterar de manera fundamental y definitiva la forma en la que empresas, personas, gobiernos y administraciones públicas interactúan entre sí. En este trabajo hemos estudiado la irrupción de dicha tecnología en la industria de servicios financieros, con especial atención a las aplicaciones dirigidas a la gestión de la sindicación de préstamos corporativos, la distribución de dichos préstamos en los mercados secundarios, y los servicios de agencia asociados. Hemos constatado que, aunque en la actualidad el marco legal existente permite, en términos generales, el uso de los *smart contracts*, especialmente en entornos como la sindicación de préstamos corporativos, no se puede garantizar con total seguridad que los resultados de su aplicación en dicho entorno sean deseables o predecibles. Hemos puesto de manifiesto, además, las lagunas legales que existen entorno a la posibilidad (o imposibilidad) de ejecutar determinados tipos de *smart contracts*, de enmendarlos, o de garantizar su validez o inteligibilidad; la dificultad para determinar la jurisdicción y la ley aplicable en entornos abiertos y/o de plataformas públicas, y/o la imposibilidad de garantizar el cumplimiento de la norma europea de protección de datos (RGPD). Hemos observado todos estos casos en detalles y hemos discutido su alcance, proponiendo en cada situación diferentes sugerencias al estudio y consideración legal de los mismos. Finalmente, hemos puesto de manifiesto las dificultades prácticas y los retos que afronta la industria financiera a la hora de introducir el uso de *smart contracts* sobre plataformas DLT, y cómo las decisiones que se toman

en la industria están completamente supeditadas a las restricciones que, no sólo desde un punto de vista legal, sino también regulatorio y estratégico se imponen a las entidades reguladas (por ejemplo, la obligación de identificar a las entidades participantes en una transacción que se ejecute, liquide o gestione a través de una determinada plataforma DLT, el control sobre los flujos de capital o crédito, o las exigencias debidas en términos de privacidad y seguridad de la información, entre otras) y que limitan y dificultan la elección y el desarrollo de soluciones técnicas apropiadas. En este sentido hemos observado como observado las plataformas DLT cerradas ("permisionned") son las que, en principio, garantizan soluciones más acordes con las necesidades de la industria y cuentan con mayor aceptación ya que permiten, en principio, solucionar muchos de los problemas asociados al uso de Smart Contracts en entornos abiertos:

a) en primer lugar, estas plataformas facilitan que los participantes puedan establecer y acordar los protocolos legales necesarios, y la correspondencia unívoca entre acciones y consecuencias, para blindar la resolución de conflictos a priori, incluyendo el andamiaje legal necesario que soporte y regule el uso de la plataforma, y asumiendo y/o aceptando un determinado marco legal; y
b) en segundo lugar, introducen, además, la posibilidad de contar con la participación de agentes externos ("oráculos") para el control y el apoyo al servicio de la transacción (en su rol de agentes administrativos), limitando el intercambio y validación de registros al interior de un sindicato de financiación, o resolviendo el nombramiento y establecimiento de nodos de control ("notarios"). Es decir, las plataformas cerradas ofrecen un sistema de control, relativamente descentralizado, restringido a un número determinado de nodos de control bien identificados y debidamente cualificados, que se adecúa relativamente bien a las necesidades de la industria (esto es, la regulación financiera y de protección de datos europea), permitiendo, si fuera necesario, el acceso a un agente externo para la verificación y el control de las transacciones y los flujos de capital (particularmente interesante para el regulador financiero, por ejemplo).

De entre todas las plataformas cerradas, hemos visto que las aplicaciones basadas en Corda (consorcio CordaR3) cuentan, por el momento, con mayor aceptación en la industria, siendo uno de los estándares más reconocidos. En este sentido, las entidades financieras están colaborando decididamente, obligadas a entenderse, para lograr establecer un estándar *de facto* que permita avanzar en la introducción de la tecnología cumpliendo con el marco regulatorio y legal y garantizando la interoperabilidad y los niveles de servicio adecuados. CordaR3 es una iniciativa muy interesante pero las limitaciones y las lagunas legales descritas entorno a la introducción y el uso de smart contracts no se resuelven del todo. Queda mucho camino por recorrer en la aplicación práctica de la tecnología DLT en el ámbito de la sindicación y distribución de

préstamos. La gran incógnita será entender cómo de rápido será capaz de adaptarse el marco regulatorio y legal actual para no ralentizar la introducción y la aceptación de estas nuevas soluciones tecnológicas a medio plazo, que tantos beneficios pueden proporcionar.

5. Bibliografía

[1]. LOESCH, Stefan (2018)

A guide to financial regulation for fintech entrepreneurs
London, UK: John Wiley & Sons

[2]. ANTONOPOULOS, Andreas M. (2015)

Mastering Bitcoin. Unlocking digital cryptocurrencies
Sebastopol, CA, US: O'Reilly

[3]. NARAYANAN, A., BONNEAU, J., *et al.* (2016)

Bitcoin and cryptocurrency technologies
Princeton, NJ, US: Princeton University Press

[4]. TAPSCOTT, D., TAPSCOTT, A. (2016)

Blockchain revolution
London, UK: Portfolio Penguin

[5]. *Blockchains and Laws. Are they compatible?* [April 2019]

A whitepaper championed by Baker McKenzie in collaboration with R3
https://www.bakermckenzie.com/en/-/media/files/expertise/fig/br_fig_blockchainsandlaws_jul17.pdf [May 2019]

[6]. RASKIN, M. (2017)

The law and legality of smart contracts [April 2019]
The Georgetown Law Technology Review (Vol 1:2, pag. 305-341. Georgetown, WA, US
https://www.ilsa.org/ILW/2018/CLE/Panel%20%2311%20-%20THE%20LAW%20AND%20LEGALITY%20OF%20SMART%20CONTRACTS%201%20Georgetown%20Law%20Technology%20Rev.._.pdf [June 2019]

[7]. GENDAL BROWN, R. *et al* (2016)

Corda: An Introduction
https://docs.corda.net/_static/corda-introductory-whitepaper.pdf [April 2019]

[8]. GENDAL BROWN, R. (2018)

The Corda Platform
https://www.corda.net/content/corda-platform-whitepaper.pdf [April 2019]

[9]. HERIAN, R. (2018)

Legal recognition of blockchain registries and smart contracts
The Open University Law School
http://oro.open.ac.uk/59481/9/Legal%20Recognition%20of%20Blockchain%20Registries%20and%20Smart%20Contracts%20%28Final%20Draft%20Report%20%2B%20Appendix%29.pdf
[April 2019] Discussion document for the workshop "Blockchains and smart contracts legal and regulatory framework" Paris, France, 12th December 2018

[10]. QUIN, K., GERVAIS, A (2019)

Hoschschulle Luzern / Imperial College London / Liquidity Network
EU Blockchain Forum
An overview of blockchain scalability, interoperability and sustainability
https://www.eublockchainforum.eu/sites/default/files/research-paper/an_overview_of_blockchain_scalability_interoperability_and_sustainability.pdf?width=1024&height=800&iframe=true [April 2019]

[11]. IBAÑEZ, LD., O'HARA, K., SIMPERL, E. (2018)

On blockchains and the General Data protection Regulation
University of Southampton
Licensed under a Creative Commons "Attribution-Share Alike 4.0 International" license
https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf [April 2019]

[12]. *Smart contracts: is the law ready?* (2018)

White paper prepared by Smart Contracts Alliance
https://www.dlapiper.com/~/media/files/people/tank-margo/smart-contracts-is-the-law-ready-web.pdf?la=en&hash=003897A104F6A74DD9FC1C2E0FE2A4F16ADE500F
(an initiative of Chamber of Digital Commerce Digital, Georgetown, WA, US)
https://digitalchamber.org/about/ [May 2019]

[13]. *Smart Contracts: legal framework and proposed guidelines for lawmakers* (2018)

Whitepaper by European Bank for Reconstruction and Development (EBRD) and Clifford Chance, available at https://www.ebrd.com/documents/legal-reform/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf [April 2018]

[14]. *Smart contracts for the digital age* (2018)

Clifford Chance
file:///C:/Users/Andre/Downloads/Thought_Leadership_Smart_Contacts_LR_6037304.pdf
[April 2019]

[15]. Global Debt Registry taps blockchain for loan registry

https://www.finextra.com/pressarticle/74488/global-debt-registry-taps-blockchain-forloan-registry [April 2019]

[16]. *Blockchain in financial services*

https://www.pwc.com/us/en/industries/financial-services/research-institute/topissues/blockchain.html [April 2019]

[17]. *Blockchain and Its Coming Impact on Financial Services*

http://jwm.iijournals.com/content/21/1/124 [April 2019]

[18]. *Applications of blockchain to financial services: three banking use cases*

https://finsia.com/insights/news/news-article/2018/05/10/applications-of-blockchain-tofinancial-services-three-banking-use-cases [April 2019]

[19]. *How is the UK approaching financial blockchain regulation?* (ComputerworldUK - article)

https://www.computerworlduk.com/security/how-is-uk-approaching-financial-blockchainregulation-3680781/ [April 2019]

[20]. *Blockchain in financial services: birth of the hybrid FinTech lawyer*

https://www.taylorwessing.com/download/article-blockchain-in-financial-services.html [April 2019]

[21]. *Around the world in Blockchain Regulations*

https://medium.com/edchain/around-the-world-in-blockchain-regulations-e077d9a2a535 [April 2019]

[22]. *Blockchain in the financial services sector: what's on the regulator's agenda?*

http://www.osborneclarke.com/insights/blockchain-in-the-financial-services-sector-whatson-the-regulators-agenda/ [April 2019]

en relación a: *FCA - Distributed Ledger Technology: Feedback Statement on Discussion Paper 17/03* [April 2019]
https://www.fca.org.uk/publication/feedback/fs17-04.pdf

[23]. KIAYIAS,A.,RUSSELL A. (2018)

Ouroboros-BFT: A Simple Bizantine Fault Tolerant Consensous protocol
https://eprint.iacr.org/2018/1049.pdf [May 2019]

[24]. NAKAMOTO S. (2008)

Bitcoin: A Peer-To-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf [May 2019]

[25]. LAMPORT, L. SHOSTAK R. PEASE M. (1982)

The Bizantine Generals Problem

ACM Transactions on Programming Languages & Systems,

Vol. 4, No. 3, July 1982, Pages 382-401

https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf [June 2019]

[26]. VUKOLIC M. (2015)

The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication

https://allquantor.at/blockchainbib/pdf/vukolic2015quest.pdf [June 2019]

[27]. CLACK C., BAKSHI V., BRAINE L. (2016)
Smart contract Templates: foundations, design landscape and research directions
http://www.resnovae.org.uk/fccsuclacuk/images/article/sct2016.pdf [Junio 2016]

[28]. TSCHORSH F., SCHEURERMANN B. (2016)
Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies
Humboldt University of Berlin
https://eprint.iacr.org/2015/464.pdf [December 2019]

[29]. *Impact of distributed ledger technology on syndicated loans,* Whitepaper Genpact, available at https://www.genpact.com/downloadable-content/insight/impact-of-distributed-ledger-technology-on-syndicated-loans.pdf [December 2019]

[30]. PETROV D (2019) *The Impact of blockchain and distributed ledger technology on financial services*, University of Economics - Varna, Bulgaria.
https://stumejournals.com/journals/i4/2019/2/88.full.pdf [December 2019]