icade núm. 101 [Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales]
Monográfico
FinTech: la tecnología en las finanzas. Oportunidades y desafíos
Artículos
3. Cuestiones jurídicas en torno a la cadena de bloques («blockchain») y a los contratos inteligentes («smart contracts») (JAVIER W. IBÁÑEZ JIMÉNEZ)

3 Cuestiones jurídicas en torno a la cadena de bloques («blockchain») y a los contratos inteligentes («smart contracts»)

JAVIER W. IBÁÑEZ JIMÉNEZ

Profesor Propio de Derecho Mercantil. Universidad Pontificia Comillas, jibañez@comillas.edu

Sumario:

RESUMEN: Se tratan algunas cuestiones clave que, desde la óptica legal, y en particular del derecho de la contratación, comienza a plantear en España la introducción y generalización en la práctica de sistemas de contratación electrónica fundados en la tecnología denominada de cadenas de bloques o registros distribuidos, y en el empleo de los llamados contratos inteligentes.

PALABRAS CLAVE: Contratación electrónica # cadena de bloques # contrato inteligente # tecnología de registros

LEGAL QUESTIONS ON BLOCKCHAIN AND SMART CONTRACTS

ABSTRACT: Some incipient and crucial questions posed today in Spain, mainly from a a Spanish contract private-law standpoint, by blockchain and distributed-ledger techonology, are posed hereunder. Namely, those brought by the introduction and market expanding of smart contracts as contract-execution devices.

KEYWORDS : Electronic contracting # blockchain # smart contract # distributed ledger technology (DLT)

Fecha de recepción: 25/05/2017

Fecha de aceptación: 13/06/2017

I. NOTA BREVE PARA UNA INTELECCIÓN DEL FENÓMENO POR EL JURISTA

El inicio de este análisis se centra en un acercamiento a los conceptos de cadenas de bloques (*blockchain*), tecnologías de registros distribuidos (*distributed-ledger technology* , en adelante DLT), y contratos inteligentes (*smart contracts* , en lo sucesivo SC), desde la óptica del derecho patrio. Para la comprensión jurídica de un fenómeno puramente tecnológico por su naturaleza, haremos unas consideraciones preliminares escuetas sobre la significación de estos conceptos para la sociedad y para el comercio (más abajo, 1.1), esbozando una descripción de los pilares tecnológicos de los registros de datos de tipo DLT, y significado jurídico de la relación trabada entre los participantes en un registro que consiste en un sistema distribuido de datos (1.2), para concluir con unas escuetas observaciones jurídico-privadas, hechas en el plano del derecho de la contratación, sobre el llamado contrato inteligente o SC (1.3).

1. LAS LLAMADAS CADENAS DE BLOQUES Y SU SIGNIFICACIÓN PARA EL COMERCIO

La Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (en adelante, LSSI[1)]) incorpora la correspondiente Directiva europea[2)] para dotar de seguridad jurídica a las relaciones *inter privatos* por vía electrónica, y así asegurar la confianza de los operadores. En este contexto, los servicios precitados se prestan a petición de un usuario, sin presencia física y a título oneroso.

El caso de *blockchain* , sin duda se adentra en el ámbito de tales servicios, en la medida en que, por un lado, se contratan bienes y servicios por vía electrónica, y hay además provisión de tales servicios por intermediarios especializados, que son los proveedores de esta tecnología creadores de las redes de comunicación trabadas entre quienes acceden a la información de las llamadas cadenas de bloques. También, naturalmente, en estos supuestos hay transmisión de datos por redes de telecomunicaciones (Internet), y se realizan copias de datos con alojamiento de información en servicios y aplicaciones telemáticas[3)].

Pese a que en el caso de las cadenas de bloques –como seguidamente comprobaremos– inequívocamente se prestan servicios de la sociedad de la información –lo que obliga al prestador a cumplir las exigencias de los artículos 11 y 12 LSSI, entre otras–, lo cierto es que la nota de onerosidad no tiene por qué presentarse en todas las modalidades imaginables de este sistema, pues los proveedores del servicio no necesariamente han de buscar rentabilizar el sistema o red *blockchain* , consistente en una agrupación de nodos o puntos desde los que se opera colectivamente. Al menos, no han de hacerlo necesariamente a través de cobros a los usuarios del servicio de la red. Pudiendo ser el hecho mismo de participar en el sistema un acicate económico suficiente, en la medida en que las empresas que acceden a este servicio aspiran a su vez a prestar otros servicios o a vender o comerciar con bienes utilizando este peculiar sistema de engarce o encadenamiento de datos, unida indisolublemente a una tecnología DLT o de *registro distribuido.*

En definitiva, en estas cadenas de bloque se procesan, almacenan e intercambian datos en línea sin limitación de tiempo, espacio o volumen, y se hace vía internet, lo que implica, si no en sí mismo comerciar (comercio electrónico), sí contratar electrónicamente con prestación de servicios de la sociedad de la información (Botana García, 2001, pp. 5-6; Plaza Penadés, 2003, pp. 413-415; Barranco Saiz, 2006, pp. 4-5), pues, conforme a una noción lata de *e-commerce* , basta para que haya contratación electrónica la concurrencia en la negociación de equipos informáticos, con oferta y aceptación a distancia de las partes, tratamiento y almacenaje digital de datos; en este contexto, la nota de la onerosidad o el ánimo de lucro en el intercambio electrónico puede ser considerado como una característica accesoria, bastando que sea indirecta o no asociada al despacho del servicio de transmisión de datos por la cadena de bloques[4)].

Dicha cadena o *blockchain* consiste, en esencia, en una base de datos compartida en una red de usuarios. En ella se anotan y anudan bloques de datos (por orden temporal de generación) de forma *indeleble* , registrándose de forma *acumulada* y además *inalterable.* Lo que es asegurado por el empleo telemático de algoritmos que encriptan o cifran (criptográfica y doble o asimétricamente, usándose a la par una clave pública o compartida y otra privada no descifrable por otros[5)])los datos. Estos pueden ser intercambiados o circular en bloques para realizar cualesquiera negocios jurídicos, operaciones o relaciones no negociables (otros hechos jurídicos) que tengan lugar entre esos usuarios.

Una notable peculiaridad técnica de importantes consecuencias jurídicas que posee esta base de datos encadenados y encriptados, es que el intercambio de los datos se hace directamente entre los usuarios sin mediadores o intermediarios, pues las transacciones las verifica la propia red de «nodos» (ordenadores de los usuarios adheridos a la red) en todo momento. El gestor del sistema o la comunidad que la crea se limitan a poner a disposición de los usuarios el propio sistema a modo de red de nodos e instruirles para que operen por su cuenta incorporando datos, esto es, realizando operaciones o «transacciones» (que jurídicamente pueden o no ser contratos).

Cada ordenador integrante de la red guarda siempre copia de todos los datos de la cadena de bloques (de datos), que se va engrosando con nuevos eslabones a medida que se va operando en la red (con conformidad *algorítmica* o verificación automática de claves) y todos comparten los datos de las nuevas operaciones practicadas. No cabe discrepancia entre los datos compartidos, pues de diferir versiones de los que se van generando, un *consenso matemático* entre los ordenadores para validar los datos en conflicto primaría la versión más común como aceptable, que será finalmente la compartida en red, sobre la que se seguirá el tracto contractual u operativo. Para alterar con éxito un eslabón con sus datos habría distorsionar los datos encriptados en la mayoría de ordenadores, a un ritmo impracticable[6)]; un solo defraudador carecería en todo caso, en cualquier configuración DLT, para alterar el proceso.

Por otra parte, en la cadena rige un dual principio de univocidad y unicidad operativa, que dota de gran seguridad jurídica al tráfico sobre *blockchain* . Operando en la cadena de bloques no caben dobles transacciones (si fuera una venta de un activo *encriptado* –por ejemplo, criptodivisa– no existe la doble venta), pues en la red las claves públicas, visibles por todos los usuarios en un repositorio, son descifradas desde cada nodo con claves privadas, como en los sistemas de *firmas reconocidas* , con la diferencia de que el repositorio no es central sino compartido; lo que garantiza que los datos (de un pago, de un SC, etc.) vienen del usuario o nodo autorizado para operar con su firma reconocida, a favor de un determinado usuario destinatario de datos, cesionario o beneficiario cuya clave pública emplea el usuario remitente de datos, cedente o iniciador de la operación.

En definitiva, quien opera, contrata o comercia en la cadena (e. g., cedente o transmitente de un activo digital) debe crear un *script* o guión de los datos de la operación, añadidos en un bloque como eslabón de la cadena. Lo hace insertando su clave pública para identificar los *hashes* (funciones criptográficas algorítmicas) de la operación previa, y firmando a la par con su clave privada: el resultado técnico de que un bloque se añade correctamente es la generación un *hash* nuevo, cuyo número algorítmico o *nonce* es testado, generalmente mediante una comprobación o prueba de trabajo que tiene que realizar el nodo aspirante a crear un eslabón (*proof of work,* «minería»), a fin de cerrar y consolidar válidamente dicho eslabón o bloque, que se incorpora a la cadena.

Este *modus operandi* permite transportar información (relativa al contrato) en los propios bloques o paquetes de datos que se engarzan en cada nuevo eslabón; y también transmitir activos virtuales (*tokens* , en argot) por vía digital, como sucede en el caso de las divisas criptográficas que circulan en la red. Por tanto, la cadena de bloques puede servir tanto para ejercer el comercio electrónico por diferentes vías, como asimismo para servir de soporte a la información jurídica anudada a las transacciones, guardada de forma segurísima en la red DLT; lo que constituye una ventaja sin precedentes en la historia del comercio.

2. LA TECNOLOGÍA DE REGISTROS DISTRIBUIDOS: ALGUNAS DE SUS IMPLICACIONES JURÍDICAS

A *blockchain* subyace una tecnología de distribución y acopio de datos, denominada DLT o tecnología *distributed-ledger* . Se ha dicho que la cadena de datos consiste, metafóricamente, en un «libro mayor de contabilidad», cuando en realidad es metáfora más precisa la de un registro compartido o descentralizado por los usuarios de la red donde se hacen las operaciones en cadena. Esa descentralización (en argot, «distribución») evita la presencia de un registrador o validador central con autoridad sobre el resto de participantes o nodos. La propia red verifica y controla concertada y consensuadamente las operaciones, lo que entre otras consecuencias hace superflua la presencia de un anotador o contabilizador de operaciones y activos, y también de un registrador o custodio de los mismos, por un lado, y por otro, hace igualmente innecesaria una organización en niveles o escalones de registro, como sucede por ejemplo en los mercados de capitales con las figuras de los gestores de compensación y liquidación, o con los depositarios centrales de valores. Tampoco se da aquí un depositario central de valores o de operaciones y sus datos anexos como sucede en el caso de los registros de la propiedad o en los registros de contratos actualmente conocidos.

En la medida en que, desde la propia red, sus programas internos de funcionamiento detectan y, en su caso, expulsan cualquier posible copia alterada o manipulada de los datos, el sistema DTL es, como lugar virtual donde se practican anotaciones, segurísimo, lo que genera confianza a los usuarios. En el seno ese registro o espacio de anotación de operaciones algorítmicas (con traducción o descifrado alfanumérico), obviamente, no es precisa, ni tan siquiera posible, la presencia o la mediación de operadores jurídicos como notarios o registradores públicos , pues el sistema custodia muy eficazmente todos los datos, que están reproducidos descentralizada y permanentemente en toda la red, de modo que se da en la DLT una suerte de fe pública automatizada. Lo que no obsta para la necesidad de asegurar legalmente la resiliencia del registro, y, sobre todo, la identidad y capacidad de quienes operan en la red, por fuera de la *blockchain* , antes y después de la inserción de datos.

Por otra parte, el mecanismo de consenso entre los usuarios que es empleado en la DLT para encriptar los mensajes y generar las transacciones o nuevos bloques de datos minimiza la probabilidad de reclamaciones por falsificación, reemplazo, manipulación, sustitución, borrado, o cualquier suerte de manipulación de los datos y de los mensajes, de modo idéntico a como sucede en los sistemas de generación y aplicación criptográfica de firmas avanzadas[7)], donde se produce la vinculación inequívoca entre firmante aparente y real, garantizando el no repudio o rechazo de autoría de la firma, y la integridad e inalterabilidad o imposible modificación del documento enviado, con lo que se salvaguardan tanto los parámetros aceptables de seguridad jurídica en la identidad del firmante como la nota de autenticidad del documento electrónico y sus datos asociados (Martínez Nadal, 2001, pp. 159-161; De la Oliva Santos, 2004, pp. 119-126; Arias Pou, 2006, pp. 387-391)[8)].

Estos efectos son inherentes a la DLT. Cuando un usuario, desde un nodo, añade o incorpora datos a la cadena operando, lo hace en un registro

donde, en lugar de registrador, hay verificación automática por los demás ordenadores de los algoritmos criptográficos introducidos por el operador remitente de datos. Para validar la nueva transacción es necesario el «consenso virtual», esto es, la aquiescencia de los ordenadores a los datos que verifican la procedencia y tracto de la transacción, para validarla y poder añadir un nuevo bloque a la cadena. Como es natural, ese consenso proviene del previo consentimiento común -humano, no virtual- de todos los usuarios a adherirse al mecanismo de generación algorítmica de *hashes* y de uso de claves para encriptar (a *simétricamente* , en argot, para indicar el doble uso combinado de claves públicas y privadas), reconocer y validar los datos introducidos que se van a diseminar por toda la red. La tecnología DLT permite reconocer y sincronizar simultáneamente todas las copias de la base de datos, y ese reconocimiento requiere la aprobación de la mayoría de los ordenadores que forman parte de la red. Y, antes, como se ha dicho, de quienes habilitan el sistema.

Pero indiscutiblemente resulta que, una vez lograda esa aprobación, los datos unidos al nuevo eslabón no pueden ser alterados en modo alguno. Ventaja tecnológica extraordinaria que, además de hacer inatacable por terceros el contenido de los datos, e incluso por los propios usuarios o nodos de la red DLT, viene facilitar significativamente la demostración indubitada frente a terceros de su existencia, reduciendo numerosos y elevados costes de litigación y otros transaccionales asociados[9)].

3. APROXIMACIÓN PRELIMINAR A LA NOCIÓN DE CONTRATO INTELIGENTE DESDE LA PERSPECTIVA DEL DERECHO DE LA CONTRATACIÓN

Adviértase previamente que el llamado contrato inteligente (SC) no es un contrato, sino un mecanismo automático de ejecución de instrucciones informáticas, que puede usarse, como es natural, para ejecutar contratos, precisamente en un marco o entorno DLT, pero que podría servirse de otra tecnología alternativa. Cuestión distinta es que en la DLT se trabaje sobre la base de instrucciones automatizadas que, aun en su versión más simple, son una forma de SC (por ejemplo, pacto de pago de moneda virtual), sin perjuicio de que dicho pacto no esté concebido para las funciones jurídicas generalmente vinculadas al tráfico comercial o financiero. En suma, el SC es un artilugio jurídicamente aprovechable, pero es por definición un grupo de instrucciones o de órdenes informáticas.

Hecha esa aclaración previa, ha de tenerse presente el elemento socializador y en cierto sentido democratizador del comercio que puede inducir en el tráfico jurídico, en lo sucesivo, el uso de SC en las transacciones comerciales, e incluso en el tráfico no mercantil, civil o común. Puesto que, debidamente programadas las instrucciones automáticas del SC, al menos en un entorno B2B o en otro C2C (no así en el B2C donde puede existir un «proferente» o impositor de condiciones), el equilibrio contractual se logra más fácilmente en la medida en que las partes no tienen que aceptar condiciones generales de la contratación, ni siquiera las habitualmente empleadas por los gestores de los servicios disponibles en las plataformas de internet, que entrañan de ordinario la adhesión de los clientes o destinatarios de bienes y servicios a las cláusulas preestablecidas por el prestador de servicios, carente de cualquier capacidad efectiva de discusión o *bargaining* ; en tal sentido, el contrato inteligente, en un entorno DLT nodal, bien podría contribuir al reequilibrio del poder de negociación de las partes, incluso para el comercio B2C, si es que la tecnología SC es capaz de ser conducida por técnicos y juristas, colaborativamente, hacia el telos de garantizar el cumplimiento de las respectivas obligaciones previamente negociadas en condiciones equitativas (al margen de la red)[10)].

A modo de resumen de la técnica subyacente a un SC, y para su comprensión por el jurista interesado, puede entenderse por contrato inteligente o *smart* a un programa informático con instrucciones «autoejecutables» – *self enforceable* – codificadas, donde el código puede, entre otras instrucciones (y de ahí una de sus utilidades principales en el mundo jurídico), contener las relativas al cumplimiento de cláusulas. El diseño de un *contractware* o estructura digital singular del clausulado facilita estas tres funciones distintivas del SC empleado como mecanismo de contratación:

a)Incorporar al negocio de manera ágil y segura, datos nuevos, que pueden formar parte del contenido en sus cláusulas, términos y condiciones, o bien quedar al margen de ellas; en uno y otro caso, a fin de poder reflejar o manifestar, también de forma segura, la voluntad de las partes que se ha de plasmar con la celebración o perfección del contrato. La particularidad sustancial del SC estriba en cómo queda reflejada o documentada esa voluntad, mediante líneas de código descifrables dotadas, como se ha dicho, de máxima seguridad.

b)Conectar la ejecución contractual programada, a través de mecanismos de inteligencia artificial, al desarrollo de una determinada actividad analógica, no virtual, que puede ser física o real, pero que en todo caso puede materializarse siguiendo los pactos del contrato, al margen del programa SC o en una DL (e. g., entrega de bienes en una compraventa automática, contra pago, como sucede en la venta automática).

c)Implementar medidas coercitivas, incluidas las relativas a la ejecución de sanciones, cláusulas penales o liquidación de indemnizaciones, en diversos supuestos previstos en el contrato (en el soporte SC o por fuera de él, de nuevo) para el caso de incumplimiento de las cláusulas, términos y condiciones del contrato; preferiblemente las que tengan lugar al margen del automatismo, que se supone asegurado digitalmente).

Estas funcionalidades se contextualizan en una DLT en un marco de generación confianza en quienes contratan a distancia, aliviando costes de transacción e intermediación. En particular, los que genera interposición de intermediarios como los mediadores profesionales o prestadores de servicio en sitios virtuales, quienes, tanto el ámbito financiero como en otros del tráfico mercantil, operan como monopolistas de confianza global en la red (como eBay), y a través de cuyos sistemas de negociación on-line se intercambian las prestaciones entre particulares.

II. ALGUNAS CONSECUENCIAS DEL EMPLEO DE «BLOCKCHAIN» Y DE «SMART CONTRACTS» PARA EL DERECHO DE LA CONTRATACIÓN Y PARA LA PRUEBA DE LOS CONTRATOS

1. LA EJECUCIÓN AUTOMÁTICA DEL CONTRATO INTELIGENTE EN EL CONTEXTO DEL DERECHO DE LA CONTRATACIÓN PRIVADA

Como hemos señalado, los SC se desenvuelven normalmente en entornos DLT llamados nodales entre particulares o *peer to peer*. Y el contrato inteligente no es en sí fuente productora de obligaciones (1088 y 1091 CC), pues el genuino acuerdo o concordancia de voluntades (1254 y 1258 CC) queda por fuera o al margen del artilugio telemático, que es el soporte, y asimismo el resultado técnico, de emplear un concreto medio informático –programa, software[11)]–.

Tal soporte, en el plano jurídico, se puede articular como mecanismo de documentación contractual, al menos respecto al *modus adimplenti contractus*. De modo que sea singularmente apto para articular, verificar y tutelar, al margen del contenido del acuerdo de voluntades (*cum-tractus* , con-traído o atraído conjunta y recíprocamente) que se sustancia en un pacto o negocio jurídico bilateral documentable en la red DLT, la ejecución de los derechos y obligaciones previstos por las partes como contenido obligacional esencial; para lo que, invariablemente, se ha requerido previo consentimiento o consenso procedente de quienes en él toman parte (1262 CC).

En el contexto DLT es posible programar ejecución automática y digital de órdenes previamente insertadas por los contratantes. Los códigos informáticos que rigen la secuencia programada constituyen y componen cadenas de mandatos condicionados del tipo «si sucede A, haz B»; «si pagas X, entrega Y», etc. Así, normalmente la programación del SC necesita una fuente externa de datos para chequear regular y automáticamente si se cumple o no efectivamente. Tal fuente exterior se suele basa en formatos de texto (PDF, Javascript, JSON,...). Detectada una modificación de datos (nombre del servicio, tipo de documento, fecha del cambio o porcentaje de texto alterado, entre otros), el cambio es almacenado en un formato después legible y verificable por el propio programa (SC en sentido técnico).

La reaceptación de condiciones modificadas es posible, con la consiguiente minoración de costes de cumplimiento, siempre con la transparencia y fiabilidad que otorga la cadena de bloques. Ahora bien, las modificaciones de cláusulas, aun no sustanciales, se han de comunicar al usuario para que tenga opción de desistir o negociar nuevas modificaciones, ya desde la fase precontractual o desde los tratos preliminares. Todo lo cual trae costes, que la preparación de un nuevo SC o de un contrato modificado puede mitigar[12)].

Por lo demás, si se opera en un entorno DLT consensuado o de tipo *permisionado* o con autorización interna otorgada por los nodos-socios, es muy difícil que prospere, como hemos indicado, cualquier acción de eventuales violadores mayoritarios de las propias reglas operativas o protocolos fijados para contratar; otro tanto sucede en redes de acceso libre o *blockchain* "pública", si hay un número elevado de nodos, lo que sucede especialmente en una cadena de bloques pública de gran distribución como la que sustenta el tráfico de las grandes criptomonedas (Bramanathan, 2016).

2. REFERENCIA A LA CUESTIÓN DE LA DOCUMENTACIÓN DEL CONTRATO EN LA CADENA DE BLOQUES

Previamente, merece recordatorio el hecho de que nuestra LSSI impone la equivalencia normativa entre los actos electrónicos y los manuales o autógrafos (art. 23.1), sin perjuicio de que, para contratar válidamente, deban concurrir los requisitos generales (cf. 1261 ss. CC).

El contrato documentado en la cadena de bloques a través de transacciones criptográficas, y el propio contrato inteligente, son electrónicos por naturaleza, y pueden celebrarse como contratos solemnes, en la medida en que se asuma la hipótesis de que la forma de SC, o la adscripción a la cadena de bloques, no empecen el cumplimiento de la función jurídica que desempeña de ordinario la forma contractual en soporte escrito. Que la instrumentación del contenido contractual se haga por mensajes de datos en la red no es motivo sustancial para otorgar al negocio así concluido un rango jurídico inferior, o para discriminar o limitar su eficacia por razones de insuficiencia formal (Illescas Ortiz, 2001, pp. 39-41).

Por otra parte, la contratación en *blockchain* tiene lugar de forma directa (contratación electrónica directa), en el sentido de que no interviene en ningún supuesto mecanismo, modelo o esquema propio del sistema tradicional de formación de los contratos entre presentes, o entre ausentes sin mediación de mecanismos electrónicos. Todas las transacciones que tienen lugar en la cadena de bloques se documentan en el sistema DLT, que es una base de datos interconectada para los nodos autorizados o validados (sistema de *permissioned blockchain*), y, desde luego, con acceso del gestor del sistema y de determinados nodos que puedan venir especialmente cualificados o autorizados para realizar labores de mantenimiento, gestión, supervisión o autorización a terceros para acceder de forma segmentada o parcial a determinados tipos de usuarios, en función de los datos a los que puedan acceder conforme al contrato de constitución de la red. En este sentido debe tenerse presente que no todas las cadenas de bloques son bases de datos con acceso universal a todos los datos por todos los nodos; la tecnología DLT permite escalonar, graduar o segmentar el acceso a la información, seleccionándose los mecanismos de acceso en contratos previos. En caso de selección o discriminación informativa prevista entre nodos estamos ante lo que en argot se denomina redes *semipúblicas o semiprivadas* (algunas de las cuales empiezan a gestarse con éxito en España) y que se contraponen a las cadenas de bloques públicas o de acceso igualitario universal (como las de los mercados de criptodivisas Ethereum o Bitcoin, que son las más populares).

En uno y otro caso, la documentación de las operaciones es interna, automática y registrada en la propia red, sin perjuicio de que otros contratos previos, acuerdos preparatorios o negocios antecedentes hayan podido celebrarse y documentarse antes de operarse en la red; y sin perjuicio asimismo de que el contrato antecedente puede ser un SC igualmente celebrado, negociado y gestado antes de operarse en la cadena de bloques.

Por lo que respecta a los SC, en particular, debe tenerse en cuenta esta posibilidad de su formación previa a su ejecución automática en la red DLT, con lo que su registro DLT sirve como prueba, pudiendo documentarse la operación también de forma previa o preliminar, sin perjuicio del valor de la propia cadena como mecanismo de registro de la transacción y de prueba.

Por último, ha de tenerse presente que la DLT puede servir como soporte documental tanto para documentos públicos como privados, pero *blockchain* en sí mismo, como registro, no es un documento; los datos enlazados en la red podrán constituir, en todo caso, documentos privados en la medida en que quien registra no es funcionario público, por lo que los datos contenidos en la DLT no pueden alcanzar el valor de los documentos públicos (cf. art. 3.7 de la Ley de Firma Electrónica).

3. ALGUNAS CUESTIONES PROCESALES

Es sabido que los contratos electrónicos se rigen por las reglas generales en materia de prueba; el art. 24 LSSI otorga valor probatorio cualificado a los firmados electrónicamente, de conformidad con las disposiciones especiales[13], reconociendo asimismo la validez probatoria del soporte electrónico. Conjugando estas disposiciones con las previsiones de los arts. 299 y 384.1 LEC –este recoge un *numerus apertus* de instrumentos electrónicos[14]–, se colige sin dificultad que los registros DLT pueden aportarse *ad processum* como «instrumentos», y pueden valorarse judicialmente conforme a las reglas de la sana crítica para probar la identidad de las partes de la operación en la cadena de bloques; sirviendo como prueba cualificada, en su caso, para determinar la identidad de los contratantes en un SC, así como la fecha de la operación (cada *hash* involucra en sí una firma con registro temporal o *time stamping* [15]), el contenido de los datos registrados y la autenticidad de las firmas.

El art. 3.8 de la Ley de Firma Electrónica admite como prueba documental en juicio «el soporte en que se hallen los datos firmados electrónicamente», y por tanto, los soportes anudados a la cadena de bloques, en la medida en que se emplea firma electrónica reconocida, sin perjuicio del chequeo de que el gestor de la red o sus entidades certificantes cumplen los requisitos legales para garantizar la prestación eficaz y la *compliance* regulatoria en materia de servicios de certificación, a fin de que el juez pueda asegurarse de que la información generada en la cadena es:

a) Auténtica en su contenido, conforme a los protocolos de consenso para introducirla y recuperarla; garantizándose en particular la identidad de los firmantes.

b) Conservada en su integridad, en el seno de la DLT.

c) Obtenible a fines procesales siguiendo los procesos que permiten garantizar la debida confidencialidad.

Por otra parte, la probabilidad de impugnación de la autenticidad de la firma avanzada *ex* 326.2 en relación con el 3.4 y 3.8 de la Ley de Firma Electrónica es remota, dadas las características de los algoritmos empleados y la estructura de la DLT. Dado el funcionamiento de los mecanismos DLT de criptografía asimétrica, no cabe, por lo demás, alterar el contenido de los datos anudados a la *blockchain* o a los SC empleados en el proceso de transmisión de información en la DLT; sin perjuicio de que la firma electrónica pueda impugnarse *ex* 3.8 LFE por ejemplo, por haber sido utilizada por persona distinta del titular con acceso a la clave privada por razones diversas.

En definitiva, el contenido material jurídico almacenado en la DLT puede ser garantizado judicialmente, respecto, al menos, a la existencia y contenido de sus correspondientes espacios o sitios virtuales con su secuencia de *hashes* distribuidos. Espacios que vienen a ser eslabones de la cadena, que no «archivos» como en los supuestos contemplados en la Ley de Firma Electrónica; lo guardado, que no «archivado» es la serie temporal de funciones criptográficas y series alfanuméricas que identifican al bloque previo registrado para añadir el subsiguiente, quedando todos enlazados[16].

Igualmente debe tenerse en cuenta que, a efectos de comprobación judicial del contenido jurídico material ingresado en la DLT, cada *hash* tiene un sello de tiempo asociado. No cabe alterar los datos asociados a este sello, pues la correlación entre el sellado y su confirmación en la DLT arrojaría un cotejo negativo; pero si los datos se respetan el cotejo será positivo, con lo que el juez podrá siempre comprobar que en la cadena los datos permanecen incólumes, e inmarcesibles, además de ser indelebles, pues no cabe borrar contenidos registrados. La cadena forma una unidad reflejada en cada nodo simultáneamente, lo que asegura la nota de *trazabilidad* , cuyo correlato procesal es la rastreabilidad permanente. De ahí que *blockchain* no necesite generar copias de seguridad.

Por último, debe tenerse presente que el registro *blockchain* es un medio para documentar contenidos muy diversos, que puede servir como medio de prueba semejante a los documentos, en la medida en que los jueces consideren a la cadena (y sus partes) como un instrumento de carácter

documental, por analogía con los documentos electrónicos vinculados a sellos de tiempo. Debe tenerse presente que, conforme al art. 41 del Reglamento (UE) 910/2014 de 23 de julio, sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, el sellado temporal verificado por un prestador de servicios de confianza goza de presunción legal de exactitud respecto a la fecha y hora indicada, y respecto a los datos vinculados; de no existir tal prestador, no rige la presunción, que actualmente sería el caso de las redes DLT. Por lo demás, el sello temporal anudado al *hash*, según ese precepto, será admisible como prueba en juicio aun no siendo «cualificado» por no proceder de un prestador de confianza. Habrá que acreditar en cada caso ante el juez que el *hash* creado en la DLT garantiza la existencia inalterada de los datos en determinada fecha (González Granado, 2016a).

III. «BLOCKCHAIN» Y DERECHO NOTARIAL Y REGISTRAL

Uno de los problemas jurídicos que presenta la tecnología de cadenas de bloques, desde el punto de vista de la seguridad jurídica, es que la seguridad material que proporciona su carácter «distribuido» o compartido simultáneamente en muchos puntos, unido a la que proporciona la tecnología criptográfica de generación segura de funciones hash para crear nuevos datos, parece neutralizar o inutilizar las funciones de mediación propias de notarios como dadores de fe (los datos dan fe de sí mismos y son inalterables) y registradores (no se precisa el control específico de los datos registrados por un tercero, depósito de datos o espacio público con autoridad para evitar la manipulación, porque esta no existe)[17].

Esta primera impresión, sin embargo, debe ser matizada desde el comienzo. *Blockchain* no puede reemplazar las funciones públicas notariales y registrales porque estas han sido conferidas a los fedatarios y registradores por mandato legal, a no ser que se reatribuyan por mandato legal a estos sistemas (Llopis Benlloch, 2017; Ibáñez Jiménez, 2016). Por otra parte, como seguidamente veremos, la tecnología DLT no puede suplir las funciones notariales más genuinamente humanas: la comprobación material y *ad hoc* de la capacidad para contratar de los sujetos introductores de datos. Tampoco, producir los efectos propios de los principios de registración (vinculados a la existencia de un registro público o, en su caso, de una administración pública), independientemente del hecho cierto de la posesión multilateral o colectiva de datos inmutables en la cadena.

1. RELEVANCIA DE «BLOCKCHAIN» PARA LA ACTIVIDAD NOTARIAL [18]

Una red DLT puede ser usada para que la seguridad en la circulación de los documentos notariales sea más segura que por otras vías (por ejemplo, e mail), pues lo que circula sería el *hash* criptográfico. Tal DLT tendría carácter reservado o privado para uso notarial, y podría sustituir o mejorar los actuales servicios de almacenamiento centralizado disponibles en España (actualmente, a través de la Agencia Notarial de Certificación del Consejo General del Notariado, que facilita *public compliance* a los fedatarios públicos), sirviendo un sistema de almacenaje de datos DLT y su recuperación completa (de todo el contenido de actas o escrituras) sin mediación de un certificador.

Este modo de circulación puede dar pie a la oferta por los notarios de nuevos servicios, a la vez que mitiga el coste del depósito notarial de documentos, bastante elevado. Así, el uso de DLT aparta utilidades sustanciales, tanto internas como externas, al funcionamiento de un sistema notarial. En concreto, mitigando costes públicos de transacción, en la medida en que los notarios prestan servicios a la administración pública (como los registradores) en la gestión fiscal (por ejemplo, en el impuesto de transmisiones patrimoniales y otros locales) y catastral, así como en la lucha contra el blanqueo de capitales y en la cooperación con el poder judicial a través del envío de poderes para pleitos.

Por otra parte, como se ha llegado a proponer recientemente desde la propia institución notarial española[19], podrían enviarse datos notariales encriptados (correspondientes a escrituras o actas) por conducto notarial pero a través de la precitada *blockchain* , tanto a los particulares o a las administraciones públicas, aliviando numerosos costes de comunicación y gestión documental. Por ejemplo, los asociados al envío de información previa a la elaboración de actas y escrituras, o de archivos o documentos previamente depositados ante notario (por ejemplo, testamentos, cuadernos particionales, actas de conocimiento,...).

Una vez agregados los documentos a la red, cada hash asegurará la integridad y autenticidad del documento; aunque solo el notario o funcionario autorizado puedan dar fehaciencia de la fecha *ex* 1227, hay que tener presente las normas nacionales y comunitarias precitadas en lo relativo a la consideración como sellos temporales de los hashes producidos y registrados en la DLT.

También son útiles las redes privadas DLT para que los notarios almacenen las comunicaciones electrónicas recibidas y enviadas a terceros por las personas que requieren sus servicios, con los efectos del art. 114.1 de la Ley 24/2001 de 27 de diciembre, si bien hay que tener presente que la cadena de bloques no es un «archivo» sino un registro, sin perjuicio de que el contenido de archivos de texto, audiovisuales o programas informáticos puede perfectamente incorporarse a la red vía SC o eslabones de la cadena, creando nuevos y sucesivos *hashes* .

Así, la identidad digital de la persona, su documentación vital y personal, su historial de contratación, su historial en registros públicos, entre otros, pueden depositarse notarialmente vía DLT privada, sin perjuicio de la posible actualización de datos, que podrá hacerse a través de órdenes programadas en SC.

Por lo demás, se ha dicho que *blockchain* es compatible con una intervención documental y de confrontación física del notario actuar como agente o tercero de confianza, reemplazando las pruebas de trabajo propias de la minería DLT en la medida en que goza de la condición legal de fedatario público.

Finalmente, debe retenerse que inmutabilidad de los datos contenidos en una red DLT (y en los SC por extensión), y la publicidad automática en los registros distribuidos de la comunidad de usuarios, son características que no apuntan precisamente a que *blockchain* vaya a reemplazar al servicio notarial. El error tal vez más común relativo a esta cuestión, proveniente sobre todo de entornos no jurídicos, consiste en identificar el medio técnico para prestar un servicio, con el prestador de servicio en sí, ya que *blockchain* , ni directa ni indirectamente puede realizar control de legalidad o asesoramiento... obviamente, en el caso del servicio notarial de tipo latino, donde el fedatario realiza operaciones de control de legalidad muy completas y complejas. Otro error asaz extendido, incluso entre los juristas, es el desconocimiento de la esencia de la función notarial; pues la labor del notario no es solo ni principalmente la del cotejo físico o material de documentos, o la comprobación de la presencia de las partes y la correspondencia entre los hechos percibidos y los hechos constatados (aunque también), sino más bien la de un auténtico control de legalidad, de forma y fondo, de los documentos cuya elevación a público se solicita, y una creación de seguridad jurídica extraordinaria o reforzada *ope legis* derivada, en el caso de los contratos, de la comprobación de la posibilidad de consentir libremente y de la existencia de consentimiento en cada acto intervenido (1261 ss. CC).

2. PRINCIPIOS DE REGISTRACIÓN Y CADENA DE BLOQUES

Obviamente, *blockchain* no es un registro público. La cuestión que planteamos aquí es si puede cumplir funciones equivalentes. La respuesta, inicialmente, ha de ser necesariamente ambigua; positiva, porque el consenso público podría otorgar a la DLT un valor registral sustitutivo de facto; y negativa, porque en tanto el Estado y la Ley no otorguen a la DLT el valor de instrumento técnico para soportar un registro público, no se desencadenarán en la correspondiente *blockchain* los efectos que despliega la aplicación de los principios registrales en el contexto del derecho registral (inmobiliario, mobiliario, administrativo, etc.), como la fe pública registral, la publicidad formal o material, o la calificación y legitimación registral. Estos últimos, además, no se puede olvidar que están íntimamente conectados y son indisociables de la naturaleza de la intervención humana directa, tanto por el enjuiciamiento genuinamente humano que supone el proceso de calificación (juicio técnico-jurídico documental y de conexión compleja de informaciones, *ex* 20 y 21 C Com, 6 y ss. RRM, entre otros preceptos), como la mediación humana directa que entraña la aplicación de estos procesos, irreemplazable en principio (como lo es también la mediación *humano oculo* en el juicio notarial de conocimiento o

de capacidad de los contratantes).

Como recientemente se ha recordado (Jiménez París, 2016, pp. 1-24, esp. 15 ss.), los registros dan seguridad al tráfico (mobiliario o inmobiliario) generando y protegiendo a terceros adquirentes con una apariencia jurídica de titularidad del crédito hipotecario, o de los activos registrados, frente a otros titulares, si se adquiere de buena fe (cf. 32 a 40 LH, 1473.2 CC), en detrimento de la protección individual del dueño, potencialmente desposeído *a non domino*. Con arreglo al derecho civil, la venta de cosa ajena, aun válida, no cede la propiedad (*nemo dat quod non habet*), pero en el derecho hipotecario el dueño despojado se sacrifica en favor del adquirente de buena fe, mediante un juego de presunciones legales irrebatibles (principios de fe pública registral, publicidad formal y material).

Obviamente, la DLT no es un registro en el sentido de que no juegan estos principios de registración. Por otro lado, la red no es una institución jurídica administrativa (no lo pretende), ni se confecciona al objeto de inscribir la titularidad de derechos reales (propiedad) sobre fincas, como tampoco para inscribir o anotar las vicisitudes de las personas jurídicas o instituciones afines (como es el caso de los registros mercantiles).

Así las cosas, y en una primera aproximación, puede negarse que, jurídicamente, la red sea un registro: ni es una institución jurídica para crear fe pública y tutelar a terceros, ni es oficina pública, y ni tan siquiera es un grupo ordenado de libros integrantes de un archivo, debido a las características que le son inherentes y que se han señalado.

Eso no significa que, aun siendo inaplicables a la red los principios de registración, no sirvan los «registros *blockchain* » para anotar, custodiar y disponer, incluso con carácter de prueba documental o análoga aprovechable en juicio (con valor de documento privado), de todas las informaciones relativas a contratos, operaciones que se susciten o ejecuten en la red, e incluso el contenido de la documentación antecedente o precedente a estas operaciones en red. Documentación que puede anudarse a *blockchain* s registrales internas, y circular eventualmente en un tráfico virtual que podrá sustanciarse o no en SC, y que, por lo demás, puede consistir en la generación masiva de réplicas virtuales de otros documentos públicos y privados relativos a estos negocios antecedentes. Pudiendo, así, servir una *blockchain* registral para reforzar, singularmente en caso de discrepancia inter-registral o entre distintos documentos (por ejemplo, en casos como el descrito de adquisiciones *a non domino,* si la documentación relevante o referida consta en la DLT), la argumentación jurídica de quien invoca la DLT como soporte probatorio.

IV. CONCLUSIONES

Los retos jurídicos que plantea el uso de contratos inteligentes, en el marco de las tecnologías de registro distribuido, son actualmente inabarcables. Se requiere una investigación por sectores del ordenamiento capaz de dar respuesta al posible acoplamiento a las normas existentes de las respuestas a los retos que plantean en la práctica del tráfico los SC y las DLT tanto públicas como privadas. En muchas ocasiones, el derecho vigente no puede acoger los supuestos fácticos presentados en la aplicación de estas tecnologías, por lo que es preciso un nuevo abordaje, así doctrinal como normativo, de la diversidad de cuestiones presentadas. En las páginas anteriores se han presentado algunos ejemplos (por ejemplo, inexistencia de ficheros en *blockchain* , ausencia de intermediarios, democracia participativa inherente al registro DLT que diluye la responsabilidad…), que ponen de relieve la envergadura y profundidad de las disfunciones entre el derecho vigente y la composición y factura de las soluciones jurídicas requeridas en el marco del tejido tecnológico analizado.

V. BIBLIOGRAFÍA

Arias Pou, M.ª (2006). *Manual práctico de comercio electrónico.* Las Rozas:La Ley, Wolters Kluwer.

Barranco Saiz, J. (2006). Sociedad de la Información. *Telos: Cuadernos de comunicación e innovación* , 69, 4-5. http://telos.fundaciontelefonica.com/telos/editorial.asp@rev=69.htm, acceso 2.04/2017.

Blanco Pérez, M. A., López-Román, E., Montalván Calderón, E., Suárez Otero, E., Farran Castellà, P., & Espinoza Valencia, F.F. (2017). Contratos inteligentes: los smart contract, post, en Abogacía Española, Consejo General, 6.03.2017. Obtenido de http://www.abogacia.es/2017/03/06/contratos-inteligentes-los-smart-contract/, acceso 6.05.2017.

Bramanathan, R. (2016). Blockchains, Smart Contracts and the Law…u nravelling the legal issues surrounding The DAO, 24 de junio. Obtenido de http://blog.coinbase.com/blockchains-smart-contracts-and-the-law-709c5b4a9895#.khhs8mehv, acceso 13.04.2017.

Botana García, G. A. (2001). Noción de comercio electrónico. En Botana García, G.A. (coord.), *Comercio electrónico y protección de los consumidores* (pp. 5-64). Madrid: La Ley.

De La Oliva Santos, A. (2004). Consideraciones procesales sobre documentos electrónicos y firma avanzada, 2.º Congreso Nacional de Registradores de España, Santiago de Compostela, *Estudios Legislativos,* 119-12.

García Más, F. J. (2004). *Comercio y firma electrónica,* 2.ª ed., Valladolid.

González Granado, J. (2016a). Eficacia probatoria de la blockchain. Criptografía y artículo 1.227 del Código Civil. «Blog» de Javier González Granado, 25 de abril. Obtenido de http://tallerdederechos.com/eficacia-probatoria-de-la-blockchain-criptografia-y-articulo-1227-del-codigo-civil/, acceso 2.05.2017.

– (2016b). ¿Enviará Blockchain de vacaciones a los notarios? «Blog» de Javier González Granado, 4 de abril. Obtenido de http://www.notariabierta.es/enviara-blockchain-vacaciones-los-notarios/, acceso 2.05.2017.

González Rosales, F. (2017). *Blockchain ¿tecnología útil para los notarios?* Blog de Francisco Rosales de Salamanca, 17.04.2017. Obtenido de http://www.notariofranciscorosales.com/uso-blockchain-los-notarios/, acceso 5.05.2017.

Hosser, T. (2016). Blockchain basics, comercial impacts and governance challenges. *Governance Directions* , *68* (10), 608-612. Obtenido de http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=c1d6f0e7-6453-4328-9592-d6a0721c47cd@sessionmgr4010&vid=3&hid=4102, acceso 01.05.2017.

Iansiti, M., y Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review* , *95* (1,) 118-127. Obtenido de http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?sid=236e6b71-a4b9-46b9-b559-a8b99b5c0f5d%4sessionmgr102&vid=3&hid=122, acceso 3.05.2017.

Ibáñez Jiménez, J. (2016). *Blockchain, ¿El nuevo notario?,* documento Everis NTT Data, octubre,http://repositorio.comillas.edu/xmlui/bitstream/handle/11531/14564/Blockchain_el_nuevo_notario.pdf?sequence=1, acceso 3.05.2017.

Illescas Ortiz, R. (2001). *Derecho de la contratación electrónica* . Madrid: Civitas.

Jiménez París, T.A. (2016). La publicidad de los derechos reales y el Registro de la Propiedad en España. Obtenido de http://eprints.ucm.es/35416/1/La%20publicidad%20de%20los%20derechos%20reales%20y%20el%20Registro%20de%20la%20Propiedad%20en%20Es acceso 6.05.2017.

Levine, M. (2016) *Blockchain Company's Smart Contracts Were Dumb*, 17 de junio. Obtenido de http://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb,, acceso 22.03.2017.

Llopis Benlloch, J. C. (2017). Blockchain y profesión notarial. *El notario del siglo XXI: Revista del Colegio Notarial de Madrid* , 71. Obtenido de, en http://www.elnotario.es/index.php/hemeroteca/revista-70/7106-blockchain-y-profesion-notarial, acceso 1.04.2017.

Martínez Nadal, A. (2001). Firma electrónica. En *Comercio electrónico y protección de los consumidores* (pp. 159-202). Madrid:La Ley.

Marvin, R. (2017). Blockchain: The invisible tech that's changing the world. *PC Magazine* , 91-113. Obtenido de http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=0e099e27-8c5b-4549-9e79-8cdc91a3eabe%40sessionmgr4007&vid=6&hid=4102, acceso 21.04.2017.

Morell Ramos, J. (2016). Smart contracts: teoría, práctica y cuestiones legales, Obtenido de http://terminosycondiciones.es2016/09/21/como-crear-smart-contract-mediante-terminos-condiciones/, acceso 22.1.2017.

Ormazábal Sánchez, G. (2005). El valor probatorio de la firma electrónica. En Peguera Poch, M. (coord.), *Derecho y nuevas tecnologías* (pp. 205-229). Barcelona: UOC.

Plaza Penadés, J., (2003). Contratación electrónica y pago electrónico (en el Derecho nacional e internacional). En Orduña Moreno, F. J. (dir.), *Contratación y Comercio Electrónico* (pp. 413-415). Valencia: Tirant lo Blanch.

Pertíñez Vilchez, F. (2013). Los contratos de adhesión y la contratación electrónica. En Moralejo Imbernón, N., y Quicios Molina, S. (coords.), *Tratado de Contratos* (pp. 1791-2004), Tomo II, 2.ª ed. Valencia: Tirant lo Blanch.

Smolenski, M. (2016). *Getting started with Ethereum* , 6 de junio. Obtenido de, http://medium.com/@mikesmolenski/getting-started-with-ethereum-4a3841276b6e#.l4k018ybs, acceso 11.04.2017.

FOOTNOTES

1

34/2002, de 11 de julio, BOE núm. 166, de 12 de julio de 2002.

2

2000/31/CE, de 8 de junio, DO L 178 de 17.7.2000, p. 1.

3

Cf. E. de M. LSSI.

4

Conforme, con carácter general para la contratación electrónica (Pertíñez Vilchez, 2013, pp. 1911-1915).

5

Tan sencillo como clarificador, Marvin (2017).

6

Al menos, en las experiencias conocidas DLT, como bitcoin o ethereum v. Smolenski (2016).

7

Que, recuérdese, se caracterizan por su irrefutabilidad, integridad y autenticación; por basarse en certificados reconocidos expedidos por prestador de servicios de certificación (lo podrían ser los gestores de la DLT), y por producirse en dispositivos seguros de creación de firma (lo son los algoritmos de encriptación de datos productores de los resúmenes o hashes que circulan en *Blockchain* mediante encriptación y desencriptación asimétrica).

8

No faltan quienes afirman la posibilidad de uso de la firma avanzada o reconocida por persona distinta del titular, de modo que no es igual la certeza de que la firma corresponde a un titular determinado, lo que sí garantiza el sistema, a la certeza de que la firma la use ese titular (García Más, 2004, pp. 56-60).

9

Vide Hosser (2016, pp. 608-612); Iansiti y Lakhani (2017, pp. 118-120, 124 y 127).

10

Una aproximación más difusa en tal sentido puede verse en Blanco Pérez, López-Román, Montalván Calderón, Suárez Otero, Farran Castellà, Espinoza Valencia (2017).

[11]

Sobre estas cuestiones, Morell Ramos (2016).

[12]

Como señala Levine (2016), el mayor riesgo de los contratos SC es la imprevisión del programador, aprovechable por defraudadores que operen según el programa «lícitamente» como sucedió en el caso Lybian Investment Authority vs Goldman Sachs (bien resumido en *Blockchain Company's Smart Contracts Were Dumb*, 17 de junio, http://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb, acceso 22.03.2017).

[13]

Ley 59/2003, de Firma Electrónica, BOE núm. 304, de 20 de diciembre de 2003 (RCL 2003, 2975).

[14]

Conforme, Ormazábal Sánchez (2005, pp. 46-49).

[15]

La DLT, más que almacenar archivos que contienen documentos, los registra fijándolos con un sellado temporal que prueba su existencia y contenido en un día y hora; v. Llopis Benlloch (2017).

[16]

Con descripción semejante de la cuestión, González Granado (2016a).

[17]

Para una primera aproximación al tema, González Granado (2016b).

[18]

González Rosales (2017).

[19]

De forma seminal en los foros del Observatorio Fintech Icade Everis, en particular en *Blockchain* y la función notarial, taller de notarios, U. P. Comillas, Madrid, 16 de noviembre de 2016