Contratos automatizados, Cadenas de Bloques y Registros de la Propiedad

Automated Contracts, Blockchain and Real Estate Registries

por

FERNANDO P. MÉNDEZ GONZÁLEZ
Registrador de la propiedad, mercantil y de bienes muebles y Profesor Asociado de la Universidad de Barcelona

LUIS A. GALLEGO FERNÁNDEZ
Registrador de la propiedad, mercantil y de bienes muebles e Ingeniero de Telecomunicaciones.

RESUMEN: La tecnología de la cadena de bloques no es una nueva tecnología sino la utilización de algunas tecnologías criptográficas existentes, combinadas de acuerdo con la teoría de juegos, a fin de alinear los diferentes intereses en juego sin intervención de una autoridad central, pero sin conseguirlo. En caso de conflicto, la regla del consenso genera indefensión.

No es, por ello, una tecnología autosuficiente. Los contratos automatizados solo son autoejecutables en supuestos simples, pero, en la medida en que avanza la complejidad, requieren el constante recurso a terceros.

Los contratos y las titularidades inmobiliarias son complejos, a diferencia de los derechos simples de crédito.

Los Registros son el instrumento de intervención del Estado en el sistema transaccional inmobiliario para evitar conflictos, dotando de seguridad y agilidad a las transacciones inmobiliarias.

La cadena de bloques puede ser un instrumento auxiliar útil al servicio de la fortaleza institucional del Registro de la Propiedad.

ABSTRACT: The blockchain technology is not a new technology, but the use of existing cryptographic technologies, combined with the games theory, in order to line up different interests in place without intervention of any central authority, but it does not get it.

In case of a conflict, the consensus rule generates defenselessness. This is why blockchain is not a self-sufficient technology. Automated contracts only are self-feasible in simple cases, but when complexity arises, they go to thirds.

Real estate contracts and entitlements are complex, unlike contracts and entitlements to obtain the payment of a simple credit. Registries are the intervention tool of state in the real estate transactional system In order to avoid conflicts, providing security and agility to real estate transactions.

Blockchain can be a useful tool at the service of institutional strength of the Real Estate Registry.

PALABRAS CLAVE: Cadena de bloques. Contratos automatizados. Lenguaje máquina. Registro de la Propiedad. Inteligencia artificial. Debilidad institucional. Regla de consenso. Indefensión. Fe pública registral. *Tokenizacion*. Titularidades *in rem*.

KEY WORDS: Blockchain. Automated contracts. Machine language. Property Registry. Artificial intelligence. Institutional weakness. Consensus rule. Defenselessness. Registral public faith. Tokenization. In rem entitlements.

formáticos redactados en el lenguaje propio de la programación, el denominado lenguaje máquina, distinto del lenguaje humano: 4.2.1.1. El problema de la comprensibilidad cuando el acuerdo solo se elabora en lenguaje máquina sin «transcripción» en lenguaje humano. 4.2.1.2. El lenguaje de programación obedece a una lógica *booleana* por lo que los contratos automatizados no admiten cláusulas que necesiten de interpretación para ser verificadas. 4.2.1.3. No todas las proposiciones son computables y trasladables a un algoritmo porque los sistemas axiomáticos y algoritmos son intrínsecamente limitados. 4.2.1.4. Los problemas que plantean las relaciones entre los contratos automatizados y los oráculos. 4.2.1.5. Los problemas que plantea la conservación de estos contratos a largo plazo. *4.2.2. El conflicto o dilema entre autoejecutabilidad y complejidad contractuales*: 4.2.2.1. Referencia al ámbito inmobiliario. 4.2.2.2. Referencia al estado actual del desarrollo de la Inteligencia Artificial —IA—. 4.2.2.3. La existencia de una correlación negativa entre el valor de los derechos y la complejidad de las transacciones. *4.2.3. Cuando los contratos no son autoejecutables es necesaria la intervención de un tercero:* 4.2.3.1. Los incidentes DAO —*Decentraliced Autonomous Organization.* 4.2.3.2. El *Bitcoin Cash. 4.2.4. La necesidad de determinar la legislación aplicable y la conveniencia de homogeneizar su regulación*.—V. LA DEBILIDAD DEL DISEÑO INSTITUCIONAL DE LA TECNOLOGÍA DE LA CADENA DE BLOQUES: LOS INCENTIVOS DE LOS DIFERENTES ACTORES DE LA RED NO ESTÁN ALINEADOS: 5.1. Introducción. 5.2. Los incentivos de los mineros. 5.3. La existencia de intereses contrapuestos entre los diferentes participantes. 5.4. No hay ninguna autoridad competente para tomar decisiones ni responsable de los daños causados.—VI. LA TECNOLOGÍA DE LA CADENA DE BLOQUES NO ES UN SISTEMA AUTOMÁTICO —Y, POR TANTO, AUTOSUFICIENTE— DE TRANSMISIÓN DE TITULARIDADES *IN REM*: 6.1. Distinción entre sistemas automáticos y sistemas automatizados. 6.2. La cadena de bloques no es autosuficiente sino que sustituye unos operadores por otros.—VII. LLEGADOS A ESTE PUNTO, DEBEMOS PLANTEARNOS SI EL CONJUNTO FORMADO POR LOS CONTRATOS AUTOMATIZADOS Y LA TECNOLOGÍA DE LA CADENA DE BLOQUES PUEDEN DESEMPEÑAR LAS FUNCIONES DE LOS REGISTROS DE LA PROPIEDAD INMUEBLE: 7.1. Premisas básicas. Titularidades *in personam*, titularidades *in rem* y fe pública registral. 7.2. ¿Puede el conjunto formado por los contratos automatizados y la cadena de bloques producir un efecto similar a la fe pública registral, esto es, similar a los efectos que producen el parágrafo 892 del Código civil alemán —BGB— o el artículo 34 de la Ley Hipotecaria española? 7.3. ¿Puede la denominada regla del consenso de la tecnología de los bloques encadenados eliminar la necesidad de supervisión

I. INTRODUCCIÓN

El *World Economic Forum* ha calificado la tecnología de la cadena de bloques — *blockchain*— como *megatendencia*[1], lo que es una afirmación generalmente aceptada.

En esta misma línea, la resolución del Parlamento Europeo de 3 de octubre de 2018 sobre tecnologías del libro distribuido y *blockchain-building trust with disintermediation (2017/2772(RSP)* (48):

«…requiere a la Comisión para que explore la mejora de los servicios públicos tradicionales, incluidos entre otros la digitalización y descentralización de los registros públicos, registro de la propiedad, concesión de licencias, de certificados para los ciudadanos (p.ej.: certificados de nacimiento o de matrimonio) y gestión de la migración, en particular mediante el desarrollo de usos concretos —casos piloto—; requiere también a la Comisión para que explore aplicaciones de las TLD[2] *que mejoren procesos relacionados con la privacidad y confidencialidad del intercambio de datos, así como el acceso a los servicios del gobierno electrónico usando una identidad digital descentralizada».*

Siguiendo esta misma corriente, algunos autores creen que la cadena de bloques es una revolución comparable a la aparición y desarrollo de los ordenadores personales o al desarrollo y popularización de Internet[3].

Sin embargo, no todas las opiniones son tan entusiastas. ROUBINI, por ejemplo, afirma[4]:

«La cadena de bloques ha sido anunciada como una panacea potencial para todas las cosas, desde la pobreza y el hambre hasta el cáncer. De hecho, es la tecnología más hiperpublicitada —y menos útil— de la historia de la humanidad».

Otros autores la consideran como una vía hacia la anarquía[5] y otros, en fin, como una vía hacia el autoritarismo[6]. Aunque la cadena de bloques surge en un entorno libertario[7], como un instrumento para liberarse de los fallos y de los abusos de los estados y, en general, de los sistemas centralizados y jerarquizados, sin embargo, puede acabar siendo el mayor instrumento de conocimiento y de control de la actividad de los individuos del que jamás hayan dispuestos los estados[8].

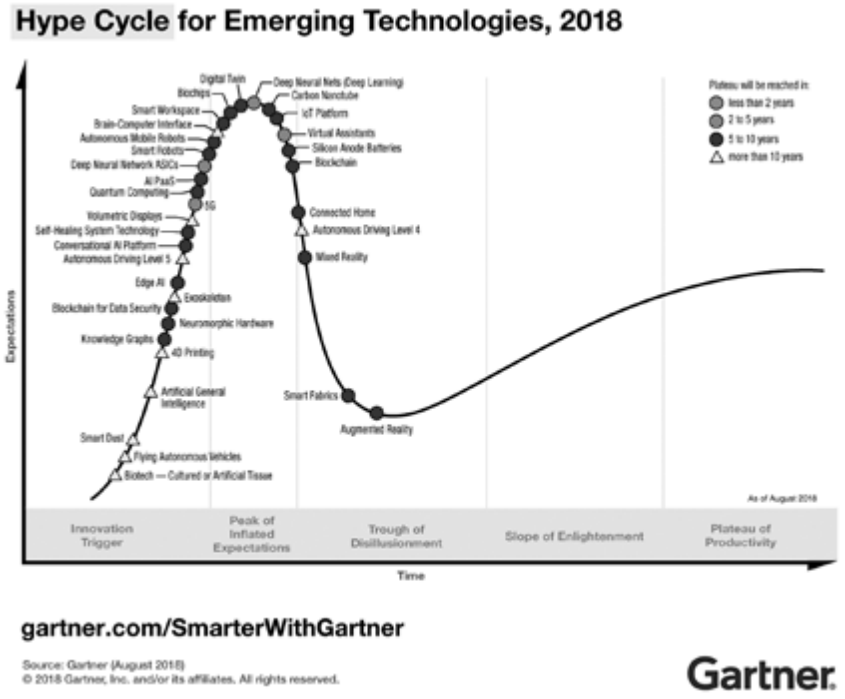
En todo caso, en los pasados años, esta tecnología ha despertado unas expectativas claramente sobredimensionadas, pero, sin embargo, no ha logrado cumplir las promesas realizadas por sus creadores y defensores. Por ello, su validez y aplicabilidad práctica sigue siendo cuestionada en muchos sectores.

En la actualidad, no obstante, parece que las aguas comienzan a bajar más tranquilas en esta materia. Así, mientras que a lo largo de los años 2016 y 2017 los anuncios de proyectos que giraban en torno a la tecnología de la cadena de bloques eran constantes, tanto por parte de empresas como de administraciones o entidades supranacionales, la realidad es que, pocos de esos proyectos han llegado finalmente a implementarse con éxito y aún menos han llegado a suponer una verdadera *revolución* respecto de la situación previa.

Como consecuencia de ello, durante 2018, una de cada cinco compañías que operaban en el sector de la cadena de bloques y de las criptomonedas han desaparecido[9] y, por otro lado, el número de menciones de la tecnología de la cadena de bloques en los informes de resultados financieros de las principales empresas se ha reducido drásticamente ya que, mientras que en el primer y segundo trimestre del 2017 las empresas del índice S&P 500 llegaron a citar dicha tecnología hasta en ciento setenta y tres ocasiones, en el último trimestre del pasado año este número no ha superado las treinta y cinco[10] menciones.

Muchas son las razones que explican esta evolución. Algunas de ellas están directamente relacionadas con el sector en el que esta tecnología nació y en el que tiene una mayor implantación —las criptodivisas— como son, por ejemplo, la alta volatilidad de las mismas[11], su abandono por los inversores[12], el anonimato que las caracteriza —lo que permite que sean el refugio ideal para negocios fraudulentos y el blanqueo de capitales—, así como, también, los fracasos y estafas que se han producido en numerosas ofertas de inversión para la creación de nuevas monedas —ICO's— y que han motivado su prohibición en algunos países[13, 14] e, incluso, China ha planteado la posibilidad de prohibir totalmente el minado de criptodivisas en su territorio[15] —en el cual se concentra el 71% de los grandes centros de minado—. Todo ello ha tenido un efecto directo y negativo en muchas iniciativas.

Otra de las causas es la *normalización* de las expectativas iniciales que despertó la cadena de bloques. El ciclo de adopción de una tecnología emergente suele seguir una curva típica a lo largo del tiempo, la cual es actualizada periódicamente por algunas entidades especializadas, como la consultora Gartner con su *Gartner Hype Cycle for Emerging Technologies*, que puede verse en el gráfico siguiente[16] y que refleja la situación de diversas tecnologías en el pasado 2018:



Puede observarse cómo tras una primera etapa de importante y rápido crecimiento en las expectativas creadas por una nueva tecnología, aquellas suelen experimentar un drástico descenso —según la curva anterior, la tecnología de la cadena de bloques se encontraría en esta fase— para pasar a una última fase de estabilización, pero ya a un nivel inferior al máximo que se había alcanzado inicialmente.

Todo lo anterior no quiere decir que la cadena de bloques esté muerta, sino que pasará con ella lo que ha ocurrido en muchos otros casos y, de esta forma, de ser considerada como la panacea universal, a la que se refería

ROUBINI, y que además otorgaba un halo de modernidad a todo aquel que la utilizase, progresivamente irá bajando al nivel del resto de tecnologías y tendrá, con sus virtudes y defectos, que competir con ellas. Habrá materias, supuestos o problemas a los que la cadena de bloques se adapte mejor y otros a los que no.

En esta materia, como en tantas otras, conviene apartarse de los fundamentalismos. Los precedentes históricos demuestran que, aunque los avances tecnológicos han sido fundamentales para el progreso humano y han dado solución a muchos problemas, ninguno de dichos avances ha logrado solucionarlos todos, sino que, al contrario, han planteado otros nuevos y así ha ocurrido, por ejemplo, con la energía nuclear, los medios de transporte, la manipulación genética, la inteligencia artificial, etc.

Por ello, deben abandonarse posiciones inamovibles y analizar si la aplicación de una determinada tecnología a un problema concreto mejora apreciablemente la situación anterior frente a otras tecnologías también aplicables, o si, por el contrario, la empeoran.

La cadena de bloques se presenta como una tecnología autosuficiente, confiable por ser pública e inmodificable, que pretende sustituir no solamente a otras tecnologías sino a instituciones surgidas precisamente para generar confianza en las transacciones impersonales y, en última instancia, a los propios estados. Sin embargo, a pesar del tiempo trascurrido desde su lanzamiento — en 2008 por el probable pseudónimo Satoshi NAKAMOTO— la brecha existente entre las expectativas generadas por sus heraldos y la realidad apenas se ha reducido.

Uno de los nudos gordianos que dificultan el desarrollo de la cadena de bloques consiste en que, si es una tecnología autosuficiente que, además, permite ocultar la verdadera identidad de las partes implicadas, puede utilizarse como instrumento para vulnerar la ley y evitar así la exigencia de responsabilidades legales.

Por ello, como sostienen algunos autores, para que la cadena de bloques pueda desarrollar su potencial —sea cual sea su alcance real— y evitar fallos que pueden resultar catastróficos, los sistemas basados en ella necesitan integrase en las instituciones legales[17]. Cuál acabe siendo el resultado de esa interacción reciproca será distinto en cada caso.

Estamos de acuerdo con *The European Union Blockchain Observatory and Forum*[18] cuando afirma que todas las nuevas tecnologías significativas, en la medida en la que han resultado ser catalizadoras de un cambio social, en algún momento han entrado en conflicto con la infraestructura legal y regulatoria existente, pero que la ley tiene una gran experiencia de adaptación al cambio y, al mismo tiempo, la historia muestra que la tecnología también está dispuesta a adaptarse a la ley donde esta refleja los valores y el consenso de la sociedad.

Puede que, en determinados casos, la cadena de bloques acabe sustituyendo a operaciones o instituciones actualmente vigentes, mientras que, en otros, propicie modificaciones o sea un eficaz instrumento de *enforcement* y, en otros, en fin, carezca de utilidad.

Partiendo de esta perspectiva y aunque la cadena de bloques ha sido calificada como una tecnología de usos infinitos[19], centraremos nuestra atención en las interacciones potenciales entre esta tecnología y los Registros de la Propiedad. Para que tales interacciones puedan resultar fructíferas son necesarios los denominados contratos inteligentes —*smart contracts*—. Nos parece más apropiado denominarlos *contratos autoejecutables* o, mejor aún, *automatizados*, pues, para su ejecución, requieren, en la mayor parte de los casos, al menos en los relacionados con el ámbito inmobiliario, recurrir a los denominados *oráculos,* como veremos en su momento. Esta es la razón del título elegido para este artículo: «*Contratos automatizados, Cadenas de Bloques y Registros de la Propiedad*».

Es importante subrayar que la cadena de bloques no es una nueva tecnología sino una combinación de diferentes tecnologías conocidas desde hace tiempo, tales como redes persona a persona —*peer-to-peer*—, criptografía asimétrica, mecanismos descentralizados de consenso, etc.[20]. Pero lo más característico de la cadena de bloques es la filosofía en la que se basa y la combinación que realiza de dichas tecnologías para conseguir los objetivos perseguidos.

La cadena de bloques pretende hacer realidad lo que MAY definió en 1988 como *criptoanarquía*. El desarrollo de Internet y los avances en la criptografía de clave pública y privada permitirían a los individuos liberarse del Estado así como de cualquier autoridad central y contratar electrónicamente entre ellos directamente, sin necesidad de terceros de confianza, sin conocer su verdadero nombre ni su identidad legal. Para ello habría que desarrollar, entre otros instrumentos, protocolos criptográficos que evitasen el engaño[21]. Ello convertiría a la cadena de bloques en una base de datos que, a diferencia de las anteriores, no estaría gestionada por ninguna autoridad central, sino, colectivamente, por una red de ordenadores entre pares, usualmente denominados *nodos*.

Bitcoin[22] aparece en 2008 precisamente como reacción frente a la política monetaria seguida por los gobiernos y los bancos centrales en relación con la crisis financiera que se inició a finales de 2007 en los Estados Unidos al explotar la burbuja de las denominadas hipotecas *subprime*. Se trataba de crear una criptomoneda que funcionara al margen de gobiernos y bancos centrales. Para ello, Satoshi NAKAMOTO[23] recurrió a la tecnología de la cadena de bloques. Es necesario, por ello, distinguir las criptomonedas —que son digitales— del dinero digital, que es producido y está regulado por una autoridad central —el Banco Central Europeo, en el caso del euro—, y, por

ello mismo, es dinero de curso legal, es decir, con poder liberatorio —confer.: artículo 1170 del Código civil—, algo que no sucede con las criptomonedas salvo acuerdo entre las partes[24].

Esta tecnología nació inicialmente para transmitir *bitcoins*, una moneda virtual que, como tal, es una unidad de medida del valor económico de las cosas, que solo existe en la red de la cadena de bloques —*on-chain*—, y no necesita tener existencia física, sino, tan solo, estar representada por signos, normalmente numéricos. Posteriormente, la plataforma *Ethereum* la ha aplicado al intercambio de criptomonedas por cosas[25], las cuales tienen existencia física fuera de la cadena —*off-chain*— por lo que deben ser previamente digitalizadas para que puedan formar parte del tráfico dentro de la cadena. Conseguir que dichos activos físicos consten descritos con exactitud dentro de la cadena —es decir, la coordinación *off-chain-on-chain*— presenta un alto grado de complejidad y, normalmente, la necesidad de recurrir a terceros —oráculos—.

Este intercambio de criptomoneda por cosa requiere también el recurso a los denominados contratos automatizados o *smart contracts* que, como tales, se postulan como autosuficientes, una afirmación que, como veremos, es excesivamente pretenciosa, especialmente en el ámbito inmobiliario, requiriendo también para su ejecución el recurso a oráculos.

Tanto las *criptomonedas* como los activos físicos necesitan ser representados digitalmente para que la cadena de bloques pueda operar. A esta representación digital se le suele denominar *token.* Salvo advertencia en contrario, reservaremos esta expresión para referirnos a los símbolos digitales que remiten a la identificación de los activos con existencia física, que suelen denominarse *asset tokens*, v.gr.: inmuebles. Este tipo de *tokens* genera, entre otros efectos, un peculiar problema de interacción entre los mundos *on-chain* y *off-chain* al que nos referiremos posteriormente.

II. LAS PRINCIPALES OPORTUNIDADES Y DESAFÍOS DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DESDE LA PERSPECTIVA DE LOS REGISTROS DE LA PROPIEDAD INMUEBLE

2.1. Introducción

Las nuevas tecnologías han generado y siguen generando a velocidad creciente una gran cantidad de datos de todo tipo, con potencial suficiente para obtener información, fenómeno conocido como macrodatos o *Big Data*. Este gran volumen de datos no es posible analizarlo por los procedimientos tradicionales, lo que, a su vez, ha generado nuevas tecnologías de

análisis de datos que permiten encontrar, entre otras cosas, patrones repetitivos en las conductas humanas. Se observa que si se produce A, entonces, a menudo, también se produce B. Ello permite generar algoritmos, es decir, conjuntos de instrucciones o reglas para resolver los problemas que nos interesen. Además, también permite desarrollar y aprovechar cada vez más la denominada inteligencia artificial, la cual puede sustituir a la humana en un número creciente de actividades.

Según KAY J.[26], los activos físicos de las naciones son principalmente casas. La propiedad residencial representa alrededor del 60% del valor del *stock* de capital del Reino Unido y Francia, el 50% del de Alemania y el 40% de los activos físicos de Estados Unidos. El resto está formado, aproximadamente en las mismas proporciones, por propiedad comercial, infraestructura y activos comerciales. Todos esos activos aparecen en los Registros de la Propiedad, los cuales, además, indican quiénes son sus propietarios y el estado de cargas, en el caso de los registros de derechos.

Además, según el mismo autor, la financiación de la compra de propiedad residencial es el elemento principal del mecanismo de asignación de capital de una economía moderna. A ello hay que añadir que, actualmente, la mayoría de las casas son propiedad de quienes viven en ellas. Las personas que compran una vivienda por primera vez suelen solicitar una hipoteca por un porcentaje sustancial, normalmente entre el 60 y el 100% del valor de la propiedad. Estas hipotecas también constan en los Registros de la Propiedad. Y no solo eso, también las limitaciones dispositivas de origen negocial, judicial o administrativo admisibles en diversos países.

Todo ello da una idea del enorme valor de los Registros de la Propiedad como *bases de datos* y las posibilidades de conocimiento que abre su tratamiento digital.

En plena revolución digital, desde la perspectiva de los *macrodatos,* los Registros de la Propiedad son bases de datos muy valiosas, por lo que es inevitable que grandes compañías multinacionales no solamente quieran poder acceder a ellas, incluso gratuitamente, sino apoderarse de las mismas, gestionarlas y obtener el mayor rendimiento privado de ellas.

Los Registros de la Propiedad son, ciertamente, bases de datos, pero no son solo ni principalmente bases de datos a las que aplicar algoritmos ni están diseñados para serlo. Su función y su finalidad específicas son distintas al hecho de ser una base de datos en el sentido indicado y, en nuestra opinión, dicha función y finalidad no deben subordinarse a su posible utilidad como bases de datos útiles para otras funciones u otros fines distintos de los específicamente registrales.

Partiendo de estos presupuestos, vamos a hacer referencia a algunas de las oportunidades y algunos de los desafíos que los contratos automatizados,

así como la tecnología de la cadena de bloques, presentan para los Registros de la Propiedad tal y como los conocemos.

Al analizar esta cuestión hay que partir de la base de que entre los economistas es un lugar común considerar que es deseable alcanzar el mayor grado posible de automatización en cualquier actividad económica porque favorece un incremento de productividad.

Y, dentro del ámbito institucional y, concretamente, del referido al ámbito de los derechos de propiedad sobre bienes inmuebles, parece existir la creencia de que los Registros de la Propiedad inmueble son instituciones automatizables —y, por tanto, sustituibles por procedimientos tecnológicos— con especial facilidad y, en consecuencia, son un campo especialmente idóneo para aplicar la tecnología de la cadena de bloques[27].

Todo ello hace surgir la cuestión de a qué se debe esa creencia. En nuestra opinión, la razón radica en que los no expertos en Derecho —y, lamentablemente, en ocasiones, también algunos profesionales del Derecho— suelen creer que los Registros de la Propiedad son simples buzones y, por lo tanto, los Registros de la Propiedad electrónicos simples buzones electrónicos.

A esta visión contribuye la concepción, no siempre explicitada, de que los Registros de la Propiedad se limitan a publicar procesos transmisivos consumados extrarregistralmente sin que, por lo tanto, formen parte del proceso transmisivo. La única función del Registro de la Propiedad consistiría, entonces, en «gestionar» la publicación de esos datos lo más rápida y fielmente posible.

Esta visión y esta concepción, convierten, así, a los Registros de la Propiedad inmueble en especialmente aptos para ser automatizados.

Ello tiene consecuencias negativas en todos los órdenes, mereciendo la pena resaltar, a los efectos de este artículo, la de generar unas expectativas difícilmente realizables sobre el alcance de la tecnología de los bloques encadenados en relación a estos Registros, además de dificultar una adecuada inteligencia sobre la función de los mismos, obstaculizando, de este modo, un enfoque adecuado sobre las posibilidades y alcance de dicha tecnología en relación a los Registros de la Propiedad inmueble.

Por esta razón es necesario dejar claro que los Registros de la Propiedad no son principalmente bases de datos ni buzones electrónicos, no siendo ninguna de ellas su principal característica, es decir, la característica que los define como tales. En efecto, los Registros de la Propiedad inmueble son:

1. En primer lugar, sistemas públicos —en el sentido de que forman parte del poder público— para la producción de un tipo singular de «datos», especialmente en el caso de los Registros de derechos, unos datos que solo el Estado puede producir: las denominadas titularidades *in rem*, y, por tanto, con efectos *erga omnes,* especialmente en el caso de los Registros de derechos.

La inscripción en un registro de derechos es un acto de soberanía —*Hoheitsakt* lo denomina la doctrina alemana[28]—. Por ello, como afirma DE OTTO con referencia al sistema español —afirmación extensible a cualquier sistema registral de derechos— la inscripción contiene una declaración del poder público sobre la existencia de derechos, es decir, sobre la identidad del propietario, así como sobre la extensión de su derecho[29].

Para conseguirlas, los Registros de la Propiedad se convierten, inevitablemente, en pieza esencial del sistema de transmisión de los derechos de propiedad sobre bienes inmuebles. Para ello, los Registros de la Propiedad, especialmente los registros de derechos, usan sofisticadas tecnologías, tanto legales como institucionales.

2. En segundo lugar, son sistemas públicos —en el sentido de que su contenido puede ser consultado— para permitir y administrar el conocimiento de su contenido a todas aquellas personas que se hallen legitimadas para conocerlo y en la medida en que la ley lo permita en cada caso.

3. Ello significa que los Registros de la Propiedad inmueble desempeñan el papel de una especie de *guardabarreras*[30], es decir, el papel de verificar si los procedimientos de transmisión se adecúan a la ley; el papel de *guardián o custodio* de los asientos registrales, que prueban la titularidad y cargas; el papel de *suministrar protección* a las titularidades tanto de derechos de propiedad como de las cargas recayentes sobre los inmuebles; y el papel de *indemnizar* en caso de error.

Sin estas características, los sistemas registrales no desempeñarían la función de proveedores de *inputs* prácticamente incuestionables en la práctica judicial y, en consecuencia, transaccional que desempeñan.

De este modo, los Registros de la Propiedad, ahorran costes de información y de transacción a los agentes económicos y contribuyen al funcionamiento eficiente de los mercados, haciendo que las titularidades sean seguras y, al propio tiempo, fácilmente transmisibles[31].

2.2. Escenario actual de la tecnología de la cadena de bloques aplicada a los registros inmobiliarios

Nos parece conveniente poner de manifiesto, pese a la intensa publicidad promovida por la industria de esta tecnología, así como por determinadas agencias registrales nacionales, que, a día de hoy, no hay ningún país que haya implantado un *Land Registry Blockchain*, esto es, un sistema de cadena de bloques que desempeñe las funciones que hoy desempeñan los sistemas registrales.

Así, en Georgia, por ejemplo, la tecnología de los bloques encadenados se utiliza solo para archivar los documentos y para tener copias de seguridad de los asientos. En este caso, y en otros similares, como el sueco al que nos referiremos a continuación, se habla, sin embargo, de *Land Registry Blockchain*, induciendo a confusión.

Por ello, es necesario destacar el rigor con el que se pronuncia el informe sobre el proyecto piloto llevado a cabo en el condado de Cook, que comprende la ciudad de Chicago, el cual concluye que la tecnología *blockchain* podría ser utilizada para la contratación privada y la presentación en el Registro solo si se conserva el marco legal existente, según el cual «*el registro oficial del condado es el único registro oficial*»[32], lo que está lejos de las pretensiones de quienes proponen soluciones persona-a-persona sin intervención alguna de terceros independientes. Conviene subrayar que el Cook County cuenta con un registro de documentos.

Suecia ofrece un caso significativo. El proyecto de *Land Registry Blockchain* afecta exclusivamente a la fase de contratación o *conveyacing*, pero no a la del Registro. El *Lantmäteriet* conserva integras sus facultades para decidir qué accede al Registro y qué no. En el proyecto han participado tanto el Registro sueco como entidades privadas: *ChromaWay*, que aportaba el conocimiento y la tecnología *blockchain*, la consultora *Kairos Future*, *Telia* como prestadora de servicios de comunicación e identificación digital y, también, dos bancos: *Landshypotek* y *SBAB* para todo lo relacionado con la tramitación y concesión de hipotecas.

En la descripción funcional del proyecto[33] se señalaba que este pretendía abarcar todo el ciclo de vida en la transmisión y constitución de derechos sobre inmuebles, salvo por lo que respecta a los procedimientos ejecutivos que, al menos inicialmente, seguirían funcionando en la forma tradicional. La operativa del Registro, como se ha dicho, tampoco se veía alterada más que por la inclusión de la nueva tecnología.

De esta forma, en el supuesto, por ejemplo, de la compraventa de inmuebles se contemplaban todos los procedimientos y documentos del ciclo de vida del contrato: desde que el titular decide vender su inmueble hasta que esta venta se produce y, en su caso, se constituye una hipoteca para financiar la adquisición por el comprador. El sistema soportaría, por tanto, las relaciones entre vendedor e inmobiliaria, entre esta y los posibles compradores, en su caso los precontratos de compra, la compraventa final, el depósito de este título en el Registro, así como el de hipoteca, etc.

Todos los documentos que se generaban en estos procedimientos eran electrónicos, pero, no obstante, lo que se almacenaba en la cadena de bloques que el proyecto implementaba, no eran los propios documentos sino los *hashes* o huellas electrónicas que se calculaban para cada uno de ellos[34]. De este modo se decía que siempre se podía comprobar y acreditar que una copia

de un documento se correspondía con el original que se hubiera generado, firmado y depositado en el Registro, mediante la simple comprobación de la coincidencia de los *hashes* de ambos.

Sin embargo, no parece que esta forma de operar suponga ventajas importantes frente a otras opciones tecnológicas que ya están, y llevan muchos años, en funcionamiento. En este sentido, puede tenerse en cuenta el caso español, en el que desde hace más de quince años la totalidad del procedimiento registral se puede tramitar de forma electrónica y telemática[35] y, así, es posible recibir telemáticamente por líneas de comunicación seguras y dedicadas, en cualquier Registro de la Propiedad, Mercantil o de Bienes Muebles, todo tipo de documentos electrónicos notariales, judiciales, administrativos o privados firmados electrónicamente y también se pueden remitir por la misma vía la notificación de la práctica de los correspondientes asientos de presentación, notas de calificación, notas de despacho, notas simples, certificaciones, minutas, etc., todo ello con sellado temporal electrónico conforme a la señal horaria oficial y con la firma electrónica del registrador o el sello electrónico del Registro[36], según los casos, y, finalmente, también es posible elaborar y firmar electrónicamente los asientos registrales a que den lugar los documentos presentados, así como las representaciones georreferenciadas de las fincas; de tal modo que la autenticidad, integridad y trazabilidad de todas estas operaciones quedan garantizadas por las tecnologías y por las firmas, sellos y sellados temporales electrónicos utilizados.

En cualquier caso, si se opta por la utilización de documentos electrónicos que también se firman y se sellan temporalmente de forma electrónica, estas firmas y sellos ya aseguran la autenticidad, integridad, trazabilidad y fecha de los documentos y permiten detectar si han sido modificados. Si, posteriormente, uno de esos documentos se deposita en el Registro —en el caso de sistemas registrales de depósito de títulos— el Registrador puede volver a firmarlo y sellarlo junto con la resolución que acuerda el depósito, acreditándose, así, la autenticidad de todo ello y, también, su integridad y fecha, sin que haga falta una cadena de bloques.

Por otra parte, de un documento electrónico se pueden generar tantas copias electrónicas como se quiera: cada una de ellas serán copias auténticas[37] ya que contendrán los mismos certificados de firma y sellados temporales que el documento original, permitiendo verificar su autenticidad, integridad, trazabilidad y fecha y si, además, se incluye en ellos un código seguro de verificación se pueden obtener las mismas garantías a partir de los traslados a papel de cualquiera de aquellos documentos electrónicos[38], sin necesidad, tampoco, de cadena de bloques.

Como hemos afirmado en el párrafo anterior, de estos documentos electrónicos pueden generarse tantas copias como se quiera y estas copias pueden almacenarse y custodiarse en múltiples localizaciones diferentes y

entregarse o permitir su acceso a ellas, telemática o personalmente, a todos los usuarios que se estime conveniente sin necesidad, nuevamente, de cadena de bloques.

Cabe señalar, además, que el cálculo de *hashes* tiene sus propias particularidades. Una de ellas es que alteraciones mínimas respecto del documento original generan *hashes* totalmente diferentes y otra es que a partir de un *hash* determinado es imposible obtener el documento que le corresponde.

De acuerdo con ello, en el caso de que se dispusiese del texto de un documento y se quisiese comprobar si este texto se corresponde con alguno de los documentos depositados en el Registro mediante la comparación de su *hash* con los almacenados en la cadena de bloques, sería muy difícil encontrar una coincidencia[39], salvo que se tratase de una copia idéntica del documento cuyo *hash* se almacenó en dicha cadena, en cuyo caso ya contaría con las firmas y sellos electrónicos, que garantizan su autenticidad, integridad, trazabilidad y fecha, y, si el documento a comparar no contase con dichas firmas y sellos electrónicos, su *hash* tampoco coincidiría nunca con el de ninguno de los documentos cuyos *hashes* se encuentran almacenados en la cadena de bloques, dado que estos últimos *hashes* se calcularon a partir de documentos con dichos elementos, por lo que no quedaría otro remedio que recurrir al cotejo visual.

Por otra parte, al tratarse de elementos interdependientes —los documentos y la cadena de bloques que almacena sus *hashes*—, desde el punto de vista de la seguridad, ambos elementos deberían estar soportados por sistemas informáticos diferentes, dotados, cada uno de ellos, de sus propios sistemas de seguridad y, además, debe tenerse en cuenta que en el caso de que alguno de los documentos se perdiese, no sería posible, por lo dicho anteriormente, reconstruirlos a partir de los *hashes* de la cadena de bloques.

No parece, por tanto, que los supuestos, que hasta ahora ha habido, de aplicación de esta tecnología a los sistemas registrales, hayan aportado algo que no se pueda conseguir por otros medios e incluso con mayor seguridad jurídica como más adelante se verá.

Por último, en la II Conferencia Anual de la International *Blockchain Real Estate Asociation (IBREA),* celebrada en Nueva York en 2017, se afirmó claramente que la tecnología de la cadena de bloques tiende a sustituir al notariado en tanto que autenticador documental, si bien se reconoció que, hoy por hoy, no puede garantizar la identidad de los contratantes. La cuestión de si la cadena de bloques —o, más precisamente, una de las tecnologías que la integran, cual es la firma electrónica— puede sustituir con ventaja la intervención notarial en el procedimiento registral —en el caso de un Registro de derechos— la tratamos más adelante.

Por lo que respecta al Registro de la Propiedad, se reconoció que en un país con un Registro inmobiliario de titularidades y cargas, es decir, de

derechos o fe pública, digitalizado y accesible *on-line*, el margen que queda para dicha tecnología es bastante reducido. Solo en ciertos países se podría crear un Registro privado paralelo al oficial, que dispensaría publicidad, que haría funcionar el mercado. Pero sin reconocimiento oficial, no hay prioridad. Solo con reconocimiento oficial la publicidad puede crear un valor.

Los proyectos, por tanto, se orientan preferentemente hacia aquellos estados sin Registro o con un Registro manifiestamente ineficiente, partiendo de la consideración de que en el tercer mundo el 70% del suelo se halla sin inmatricular, lo que representa una gran oportunidad de negocio[40].

III. EVOLUCIÓN PREVISIBLE DE DICHO ESCENARIO EN EL FUTURO PRÓXIMO. REFERENCIA A ALGUNOS DE LOS PRINCIPALES INTERROGANTES

Predecir cuál va a ser la evolución futura de la tecnología de la cadena de bloques aplicada a los registros inmobiliarios es difícil porque intervienen una considerable cantidad de variables de todo tipo. Nos centraremos, por ello, en su posible impacto en los sistemas transaccionales que cuentan con un Registro de Derechos. Haremos referencia también a aquellos que cuentan con un registro de documentos.

En este apartado nos referiremos a las cuestiones relacionadas con la identidad y capacidad de las partes, las repercusiones sobre el principio de libertad de forma contractual, el sistema de *numerus apertus* en la creación de derechos reales y algunos de los problemas que plantea la necesidad de *tokenizar* los activos físicos —con existencia fuera de la red— para que se pueda operar con ellos dentro de una plataforma de bloques encadenados.

3.1. Identidad y capacidad de las partes

En primer lugar, para que la cadena de bloques se imponga como sistema transaccional es necesario que consiga garantizar, por sí sola, la identidad y capacidad de los contratantes, lo que no es posible, conforme a la propia arquitectura del sistema, que permite que contraten dos o más direcciones electrónicas entre sí, sin saber quién hay detrás[41].

La cadena de bloques conecta *avatares*, no a las personas que supuestamente están detrás de los mismos, siendo esta, además, una de las características preferidas de los impulsores y partidarios de esta tecnología.

Si deben revelar su identidad, y, tanto por razones fiscales como de otro tipo, como el cumplimiento de normas de Derecho Privado y de Derecho

Público que regulan tanto el proceso contractual como el de transferencia, deben hacerlo, ello implica la intervención de terceros, normalmente de autoridades públicas, en el proceso transaccional, lo que rompe directamente la característica más definitoria de esta tecnología: la de ser un sistema entre pares o persona a persona, sin intervención de tercero alguno, ni privado ni público. La *autosuficiencia* que repele la necesidad de que intervenga cualquier tercero es la razón de ser del nacimiento de la tecnología de la cadena de bloques.

Para que la cadena de bloques sea admisible como tecnología transaccional en el ámbito registral es necesario identificar a transmitente y adquirente, así como su capacidad y poder de disposición y eso es algo que la cadena de bloques no puede hacer por si sola[42].

Para la determinación de la identidad, es necesario recurrir a algún sistema de identificación personal —v.gr. carta personal de identidad— y, a su vez, a alguna tecnología que permita saber que quien contrata a través de una dirección electrónica sea la persona que dice ser[43].

En efecto, el Reglamento UE (EIDAS) núm. 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior distingue entre firma electrónica simple, avanzada y cualificada. Por su parte, la Ley 59/2003 de Firma Electrónica distingue tres tipos de firma electrónica: simple, avanzada y reconocida. Su artículo 3.4 establece que: *«La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel»* y el artículo 25.4 del Reglamento EIDAS que: *«Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita».* Por ello, cuando utilizamos la expresión firma electrónica nos referimos solamente a la firma electrónica cualificada o reconocida, única modalidad de firma electrónica a la que se le reconoce equivalencia de efectos a la firma manuscrita.

Y aquí nos encontramos con el grave problema de que las firmas utilizadas por el protocolo *blockchain* no tienen la consideración ni de reconocidas ni de cualificadas porque no lo necesitan. Es más, repele estas modalidades de firma electrónica. Efectivamente, una de las características que distinguen las firmas electrónicas reconocidas o cualificadas, frente a los otros tipos, es que permiten identificar al firmante, pero, sin embargo, este no es un requisito del protocolo de la cadena de bloques, el cual persigue, precisamente, lo contrario, su anonimato.

Por ello, el Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, en su artículo 3 modifica la Ley 39/2015, de 1 de octubre, del Procedimiento

Administrativo Común de las Administraciones Públicas, añadiendo una Disposición Adicional Sexta conforme a la cual:

«*1. …en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.*

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública».

Según el Informe *Legal and Regulatory Framework of Blockchains and Smart Contracts*[44] la identificación no es un problema en el caso de las plataformas *blockchain* que requieren autorización para operar en ellas. Discrepamos de esta afirmación porque, si bien tales plataformas identifican quién ha dado de alta una determinada dirección electrónica, sin embargo, no pueden asegurar quién ha operado realmente usando esa dirección. Tales plataformas, además, no podrían funcionar como sistemas transmisivos al no ser de acceso público porque, como veremos, si la tecnología de los bloques encadenados pretende competir con los sistemas registrales de derechos, idealmente debería haber una única plataforma en cada jurisdicción. Cuestión distinta es que, adicionalmente, esa plataforma exigiera la identificación para poder operar en ella, lo que, sin embargo, no resolvería el problema de saber quién ha operado realmente.

Afirma igualmente el citado informe[45] que en el caso de las plataformas públicas —que no requieren identificarse para poder operar en ellas—, si bien no se puede identificar el fraude de identidad en el momento de la transacción, dedicando suficiente tiempo y esfuerzo, los intervinientes reales pueden ser identificados. Aunque ello fuera así, no impediría el fraude dado el carácter inmodificable y, por tanto, irreversible de las transacciones *blockchain* en donde se pretende que no rige otra ley que no sea la *lex criptographica*, que implica la pérdida de la acción reivindicatoria para el titular criptográfico privado de su derecho. Quizás por ello, reconoce el citado informe que, en la medida en la que se difunda el uso de las tecnologías de bloques encadenados, la seguridad en la identificación constituirá un problema[46].

Dificultades adicionales presenta la identificación en la contratación a través de representantes, sean legales o voluntarios, pues a las dificultades

anteriores hay que añadir las que derivan de la comprobación de la vigencia y suficiencia de la representación, algo que la tecnología de bloques encadenados no puede hacer por sí misma, por lo que, nuevamente, debería recurrir a algún oráculo.

Por esta razón —además de otras como la comprobación de su existencia, objeto social, etc.— también presenta mayores dificultades la identificación en la contratación cuando intervienen sociedades mercantiles[47]. Para ello, también es necesario recurrir a oráculos, típicamente a los Registros Mercantiles o a los Registros pertinentes en función de la persona jurídica de que se trate[48].

Por ello, nos parece relevante traer a colación que el artículo 13 ter de la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades, dispone en materia de reconocimiento de medios de identificación a efectos de los procedimientos en línea:

«1. Los Estados miembro velarán por que los siguientes medios de identificación electrónica puedan ser utilizados por los solicitantes que sean ciudadanos de la Unión en los procedimientos en línea contemplados en el presente capítulo:

a) los medios de identificación electrónica expedidos por un sistema de identificación electrónica aprobado por el propio Estado miembro;
b) los medios de identificación electrónica expedidos en otro Estado miembro y reconocidos a efectos de la autenticación transfronteriza de conformidad con el artículo 6 del Reglamento (UE) núm. 910/2014.

2. Los Estados miembro podrán denegar el reconocimiento de los medios de identificación electrónica si los niveles de seguridad de esos medios de identificación electrónica no cumplen las condiciones establecidas en el artículo 6, apartado 1, del Reglamento (UE) núm. 910/2014.

3. Todos los medios de identificación reconocidos por los Estados miembro se pondrán a disposición del público.

4. Cuando se justifique por razón de interés público en impedir el uso indebido o la alteración de identidad, los Estados miembro podrán, a los efectos de comprobar la identidad de un solicitante, adoptar medidas que requieran la presencia física de ese solicitante ante cualquier autoridad, persona u organismo habilitado en virtud del Derecho nacional para tratar cualquier aspecto de los procedimientos en línea a que se refiere el presente capítulo, incluido el otorgamiento de la escritura de constitución de una sociedad. Los Estados miembro se asegurarán de que solo pueda exigirse la presencia física

de un solicitante caso por caso cuando existan razones para sospechar una falsificación de identidad, y de que cualquier otra fase del procedimiento pueda completarse en línea».

Por su parte, el Reglamento UE (EIDAS) n.o 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, dispone en su artículo 6, apartado 1, en materia de reconocimiento mutuo:

«*1. Cuando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que:*

a) este medio de identificación electrónica haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9;
b) el nivel de seguridad de este medio de identificación electrónica corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad sustancial o alto;
c) el organismo público en cuestión utilice un nivel de seguridad sustancial o alto en relación con el acceso a ese servicio en línea.

Este reconocimiento se producirá a más tardar 12 meses después de que la Comisión publique la lista a que se refiere la letra a) del párrafo primero».

Para determinar la capacidad natural, por su parte, será necesario el recurso a algún oráculo —v.gr.: notario, en cuyo caso también podría desarrollar las labores de identificación— o a alguna tecnología —v.gr.: pruebas tales como preguntas o similares formuladas por el dispositivo a cuyo través se pretenda contratar que garanticen que responda la persona cuya capacidad se pretende comprobar—.

Para determinar la capacidad de obrar y el poder de disposición también sería necesario el recurso a oráculos, singularmente al Registro Civil —que constituye la prueba del estado civil— y al Registro de la Propiedad, cuyos asientos acreditan, a efectos del mercado, titularidad, poder de disposición,

cargas preferentes y causas de ineficacia de los actos y negocios anteriores, referentes al mismo bien que pueden privar a posteriores adquirentes de su adquisición negocial[49].

Todo ello sugiere que la tecnología de la cadena de bloques presenta serias dificultades para erigirse, por sí sola, en el elemento central de un sistema de apreciación de la identidad, de la capacidad y del poder de disposición, y, por lo tanto, en el elemento central de un sistema transaccional. Pone de manifiesto, asimismo, que, pese a lo que vienen proclamando sus heraldos, no es, en absoluto, un sistema autosuficiente.

3.2. El principio de libertad de forma contractual. La cadena de bloques como la única vía

En segundo lugar, para que dicha tecnología funcione como sistema transaccional que permita producir titularidades *in rem* sería necesario renunciar al principio de libertad de forma contractual así como de elección de procedimientos traslativos del dominio, debiéndose imponer el sistema de la cadena de bloques como sistema transaccional único en la jurisdicción que lo adoptase, negando validez y eficacia a cualquier otra forma contractual y modalidad traslativa del dominio dentro de la misma[50].

Asimismo, debería existir una única plataforma de bloques encadenados porque si hubiera varias plataformas *blockchain,* entonces, un inmueble *tokenizado* —del mismo o diferente modo— podría transmitirse desde una o varias direcciones electrónicas simultáneamente a través de las diferentes plataformas. Ello implicaría, en realidad, una intervención estatal o pública en el sistema transmisivo mayor que cualquiera de las conocidas hasta el momento, lo que no dejaría de ser una terrible paradoja para una tecnología nacida con pretensiones libertarias.

Significaría también que cualquier transacción realizada utilizando la tecnología de la cadena de bloques tendría, por sí sola, efectos traslativos y no solo contractuales. Además, tales efectos traslativos serían, teóricamente, irreversibles, puesto que *blockchain* es inmodificable. Ello convierte en crítica la determinación de la identidad, capacidad y poder de disposición del transmitente, así como de la identidad y capacidad del adquirente.

Podría, también, optarse por conservar la libertad de forma y de procedimiento transmisivo pero dotando de mayor valor probatorio a la documentación de la cadena de bloques, prescribiendo, por ejemplo, que las transacciones no realizadas a través de la cadena de bloques y que, por lo tanto, no consten en el libro inventario de transacciones —*ledger*— no serán oponibles a las que sí consten. En este caso, sin embargo, la fuerza de la cadena de bloques no derivaría de su fiabilidad directamente sino de una

norma legal y, además, deberían resolverse los problemas relacionados con la buena fe del tercero, al igual que en el artículo 32 de la Ley Hipotecaria, lo que exigiría, en su caso, la intervención judicial, negando así, nuevamente, el principio de autosuficiencia de la tecnología de la cadena de bloques.

Ello, a su vez, dificultaría notablemente la contratación transfronteriza, a no ser que las diferentes jurisdicciones adoptaran el sistema de cadena de bloques sometido a las mismas reglas, lo que, por sí, implicaría un sistema de cadena de bloques, regulado y sometido a los Estados, exactamente lo contrario de lo que dicha tecnología pretende. En esta línea, el *Legal and Regulatory Framework of Blockchains and Smart Contracts* propone que un primer paso podría ser elaborar una definición a nivel europeo de lo que se entiende por cadena de bloques y por *smart contracts*[51], lo que facilitaría una regulación armonizada de los mismos.

3.3. Imposibilidad de creación de nuevas figuras de *iura in rem* por vía transaccional

Aunque en la mayor parte de las jurisdicciones rige el sistema de *numerus clausus*[52] en materia de derechos reales, suele haber vías indirectas para que se puedan crear nuevas figuras de derecho real, de abajo hacia arriba y sometidas, finalmente, a la admisión por parte de la autoridad judicial. Ello facilita la innovación y, por lo tanto, el progreso.

Como sostienen MERRYLL, T.W. y SMITH, H.E.[53], la exigencia de tipicidad —en el límite, *numerus clausus*— en los derechos reales se comprende fácilmente si consideramos la costosa carga informacional que impone a los terceros todo el sistema de *iura in rem.* En efecto, para evitar su violación, un amplio e indefinido número de sujetos obligados a respetarlos tienen que conocer qué restricciones imponen tales derechos a sus comportamientos.

Por un lado, la tipificación extrema frustraría la consecución de muchos de los objetivos para los cuales han surgido la propiedad y los *iura in rem.* Por otro lado, sin embargo, una total libertad en la configuración de *iura in rem* generaría para los terceros altos costes de medición, de responsabilidades derivadas de errores y administrativos. Parece que el término medio entre ambos extremos sería el adecuado.

Teniendo en cuenta todos estos factores, lo relevante, como sostienen MERRILL, T.W. y SMITH, H.E. no es conseguir un *nivel máximo* de estandarización o tipificación de los *iura in rem* sino un *nivel óptimo* que no equivale a *nivel máximo*.

Desde esta perspectiva, el sistema de *numerus clausus* no debe ser contemplado tanto como una prohibición absoluta de creación de nuevos *iura in rem* cuanto como un dispositivo que mueve el sistema de *iura in rem* en

la dirección del nivel óptimo de estandarización, permitiendo un nivel positivo de diversificación de formas reconocidas de *iura in rem*. Tal dispositivo funciona como una presunción *iuris tantum* de innecesariedad de nuevos tipos *de iura in rem.* Tal es, como es conocido, el caso español. Por último, es necesario subrayar que los sistemas registrales, al disminuir los costes de información, permiten que el nivel óptimo de estandarización sea el menor cuando no el más bajo posible, lo que disminuye todos los demás costes, empezando por el de frustración[54].

Ello facilita la innovación. Esta constatación es, por otro lado, un sólido argumento a favor de los sistemas registrales que recogen ampliamente el contenido de los derechos reales, depurándolos de los elementos personales ínsitos en su negocio adquisitivo, en lugar de los sistema de encasillado, pues, en lugar de desaprovecharlas, optimizan las posibilidades que ofrece el sistema registral para acoger nuevas modalidades de derechos reales y, en consecuencia, facilitar la innovación[55].

¿Cómo sería posible en un sistema transmisivo de cadena de bloques? No es sostenible pensar que, para ello, bastaría con que ningún *peer* se opusiera. ¿Y si se opusiera? ¿No sería posible o haría falta buscar procedimientos de decisión? Ello requiere nuevamente la intervención de terceros o que las decisiones las tomen quienes tienen más poder dentro del sistema, y las tomarían conforme a sus propios intereses, como demuestra la experiencia, tal y como veremos más adelante. La intervención de un tercero, en todo caso, ya supone, por sí sola, una ruptura de la arquitectura de la cadena de bloques.

Desde luego, si hay que elegir entre cualquiera de esas opciones o la decisión por un juez independiente de un Estado democrático, parece que la opción es clara. Más adelante veremos cómo se han resuelto algunos de los incidentes habidos hasta ahora. A ello hay que añadir la tendencia a la concentración de la potencia de cálculo en pocas manos, lo que da a los denominados *mineros* un poder decisivo sobre la cadena de bloques, en un fenómeno parecido al que se está observando en Internet, en función de la apropiación y uso de datos personales por parte de muy pocas empresas de alcance global.

3.4. Algunos de los problemas planteados por la *tokenización* de los activos inmobiliarios

Señala GONZÁLEZ-MENESES, M. que, desde una perspectiva jurídica, la *tokenización* de activos inmobiliarios plantea dos cuestiones claves: a.—La interacción entre los mundos *on-chain* y *off-chain* y b.—La sustitución de la ley de circulación tradicional de un determinado tipo de activos, los

inmobiliarios, por una nueva ley de circulación caracterizada por la legitimación exclusivamente criptográfica[56].

En este apartado, trataremos la primera de estas cuestiones.

Tratándose de *tokens* que representan activos inmobiliarios y, por lo tanto, existentes fuera de la cadena de bloques, la tecnología de los bloques encadenados no puede garantizar de forma autosuficiente que el inmueble *tokenizado* existe realmente, ni que el emisor del *token* es su titular legítimo, ni que ese mismo inmueble no ha sido ya objeto de una anterior *tokenización* en el marco de la misma plataforma o de cualquier otra plataforma *blockchain*[57].

Para solventar estos problemas habría que acudir a procedimientos e instituciones *off chain*. Y, por lo tanto, son esos procedimientos e instituciones los que solventarían esos problemas de seguridad jurídica. Habría que recurrir a los procedimientos e instituciones que identifiquen físicamente las propiedades inmobiliarias —catastro y/o registro, o topógrafos—, atribuirles esa función con carácter exclusivo, no solamente en el procedimiento de inmatriculación en la cadena de bloques sino en el caso de modificación física de la propiedad inmobiliaria *tokenizada,* decretar la nulidad e inaccesibilidad a la cadena de bloques de cualquier *token* inmobiliario que no se atenga al procedimiento regulado de *tokenización* con carácter exclusivo y excluyente, imponer una única plataforma de la cadena de bloques dentro de una misma jurisdicción, etc., además de establecer el procedimiento traslativo de los bloques encadenados como el único admisible. Como vemos, la *lex criptographica* es del todo insuficiente para resolver estos problemas.

Hay que tener en cuenta que *blockchain* surgió para transmitir criptomonedas, es decir, monedas virtuales o digitales que vivieran al margen del control de cualquier autoridad monetaria. Como señala GONZÁLEZ MENESES[58], el peculiar funcionamiento de las criptomonedas como valores de titularidad anónima vinculada simplemente al conocimiento y control de una clave privada, las asemeja al dinero efectivo, el cual puede tener una vida puramente tabular. En efecto, puede ser así porque el *token* del dinero o de una criptomoneda representa una unidad de valor económico que, para funcionar, no necesita existir fuera de la cadena[59].

Pero cuando se trata de transmitir *tokens* que representan activos con existencia física fuera de la cadena —*asset tokens*—, las cosas se complican: la transmisión no puede ser puramente tabular porque, ordinariamente, afectará a la situación posesoria en aquellos casos en los que se transmitan titularidades sobre derechos reales —en nuestro caso inmobiliarios— que conllevan posesión. En estos casos, la cadena de bloques no puede garantizar por sí sola que la mutación posesoria se produzca. Para ello, en su caso, será necesario recurrir a terceros y, concretamente, al Estado representado por la autoridad judicial.

IV. ESPECIAL REFERENCIA A LOS *CONTRATOS AUTOMATIZADOS —SMART CONTRACTS—*. PROBLEMAS RELACIONADOS CON LOS MISMOS

Para que dicha tecnología sea operativa debe recurrir necesariamente a los impropiamente denominados contratos inteligentes —*smart contracts*,— así denominados por N. SZABO[60] a los cuales deberíamos denominar, más adecuadamente, *contratos autoejecutables* o, mejor aún, *automatizados*. SZABO los definió del siguiente modo:

«*Un contrato inteligente es un protocolo transaccional informatizado que ejecuta los términos de un contrato. La idea del contrato inteligente es satisfacer condiciones contractuales normales —como términos de pago, gravámenes, confidencialidad, e, incluso, recurso a la ley—, minimizar excepciones, tanto maliciosas como accidentales, y minimizar la necesidad de intermediarios. Los objetivos económicos son reducir las pérdidas por fraude, los costes de arbitraje y recursos legales, y otros costes transaccionales*»[61].

No son, en rigor, contratos, sino programas almacenados en una plataforma *blockchain* accesibles a una o más partes. Estos programas son, frecuentemente, autoejecutables y se valen de ciertas propiedades de la tecnología de la cadena de bloques, como dificultades para el engaño, descentralización, etc.[62].

Los contratos automatizados vienen a ser, por lo tanto, un conjunto de reglas que contienen respuestas automáticas cuando se producen determinados supuestos de hecho —v.gr.: introducir una moneda en una máquina que expende bebidas—, de modo que su ejecución sería automática. Esta tecnología solo opera de esta forma en casos muy simples, como el descrito, pero el desarrollo de la inteligencia artificial permitirá aplicarla a supuestos menos simples en el futuro.

La ejecución automática significa que no necesita la intervención de terceras personas, al menos, en hipótesis. En la realidad, sin embargo, los contratos automatizados requieren la intervención de terceros o intermediarios —desde los que redactan el código, hacen funcionar el sistema o almacenan los datos hasta los que elaboran las reglas o suministran información externa, como los oráculos, a los que nos referiremos posteriormente—, por cuya razón han sido calificados como contratos *no tan inteligentes*[63].

Significa también que, una vez iniciado el proceso, este deviene imparable e inmodificable, lo que resulta especialmente peligroso en caso de error porque la cadena de bloques ejecutaría las órdenes que integran el contrato automatizado y, por tanto, afectaría al valor o a los derechos sobre el activo en cuestión. De ahí que los errores o los fallos de seguridad sean particularmente peligrosos en el ámbito de los contratos automatizados.

Por ello, es frecuente que se introduzcan mecanismos para su paralización —*suicide*— en caso de activación errónea.

A efectos de este estudio, creemos que deben ser destacados determinados aspectos de este tipo de contratos. Dejando de lado los problemas relativos a la identificación, capacidad y poder de disposición de las partes contratantes, de los que hemos tratado anteriormente, trataremos a continuación de otros problemas que también deben ser abordados.

4.1. Dichos contratos han de ser públicos

Como observan DE FILIPPI P. y WRIGHT A.[64], cuando los contratos son tradicionales, redactados en lenguaje humano, las partes pueden acordar hacerlos públicos o mantenerlos reservados. Sin embargo, cuando se formalizan en lenguaje código a través de la cadena de bloques, debido a la naturaleza pública de esta tecnología, tanto el *code* de los contratos automatizados como las transacciones ejecutadas por los mismos se propagan a través de la red persona a persona, haciendo que sean visibles para todos los nodos de la red.

Puede alegarse que podría evitarse estableciendo un acceso selectivo a los mismos, pero ello, además de volver a romper la arquitectura de los bloques encadenados, plantea un grave problema.

Si el consenso[65] forma parte de la esencia de esta tecnología, no es posible que este se produzca sino cuando todos los ciudadanos, sometidos a una misma jurisdicción, tienen o pueden acceder al conocimiento de todos los actos o negocios jurídicos de finalidad traslativa o directamente traslativos.

La red, por ello, debería abarcar a todos los ciudadanos y, en última instancia, las transmisiones por vía de la cadena de bloques deberían ser, idealmente, las únicas legalmente admisibles si se pretende que la *lex criptographica* sea la ley de la transmisión, algo difícilmente imaginable, aunque solo fuera porque, para serlo, necesitaría una ley no criptográfica que lo estableciese y, además, que la tecnología de la cadena de bloques no fallase nunca o casi nunca, además de que solo se admitiera, en cada jurisdicción, una sola plataforma de bloques encadenados. En otro caso, las transacciones registradas en la cadena solo servirían como prueba —con un valor probatorio semejante al de la firma electrónica[66]— de la existencia de determinados contratos, pero sin poder acreditar la identidad de los contratantes —así como tampoco su capacidad ni su poder de disposición— sino solo el resto de su contenido, lo que constituye una severa limitación a su virtualidad como sistema transmisivo.

Si consideramos que es de esencia de la cadena de bloques que bastan dos direcciones electrónicas para contratar, sin necesidad de identificar a

quienes están detrás, y que, además, hoy por hoy, la tecnología no permite garantizar la identidad de quienes contratan, resultaría sorprendente que los países optasen por introducir sistemas abstractos, o por reconocer la validez de transferencias mediante la tecnología de la cadena de bloques desconectadas de sus contratos causales. A ello hay que añadir que en Alemania, país donde rige la doctrina del negocio abstracto, la doctrina es crítica con su mantenimiento[67]. No obstante, la noción de causa es, probablemente, una de las que más está evolucionando en los ámbitos doctrinal y jurisprudencial, sin que haya acuerdo entre los juristas europeos especializados en la construcción de un Derecho contractual europeo, objetivo que, hoy por hoy, parece difícilmente alcanzable[68].

4.2. Alcance real de la autoejecutabilidad. La necesidad de recurrir a oráculos

El segundo problema o, mejor, grupo de problemas que se plantea cuando analizamos los contratos autoejecutables son los relacionados con el alcance real de la autoejecutabilidad, necesaria para que la tecnología de la cadena de bloques sea operativa como sistema transmisivo, productor de titularidades *in rem,* pues la cadena de bloques es solamente el instrumento de *enforcement* de los contratos automatizados, por lo que si estos no son autoejecutables, quiebra el concepto mismo de cadena de bloques surgido para hacer innecesaria la intervención de terceros en el *íter* transmisivo, tanto en su fase contractual como en su fase de transferencia. En efecto, en sentido estricto, tanto la especificación de los derechos y obligaciones que integran el contrato como su ejecución deben realizarse a través de la plataforma.

4.2.1. Los contratos automatizados son programas informáticos redactados en el lenguaje propio de la programación, el denominado lenguaje máquina, distinto del lenguaje humano

4.2.1.1. El problema de la comprensibilidad cuando el acuerdo solo se elabora en lenguaje máquina sin «transcripción» en lenguaje humano.

Como sostiene FELIÚ REY[69], en un contrato autoejecutable esta expresión del acuerdo ha de realizarse mediante *lenguaje máquina* —es decir, lenguaje de programación— adecuado para su ejecución. Por tanto, resulta pertinente plantearse cómo asegurar la comprensión del clausulado y así la emisión consciente del consentimiento sobre las prestaciones —imprescin-

dible para la validez contractual— cuando el acuerdo solo se elabora en lenguaje máquina sin «transcripción» en lenguaje humano.

Esto resulta más complicado cuando estos tipos de contratos, además, se estandarizan y se ofrecen a una pluralidad de destinatarios, porque entonces entramos en el ámbito de las condiciones generales de contratación que activan los controles de incorporación, interpretación y contenido a las que están sometidas. Más aún, incluso en el caso de que no tuvieran la consideración de condiciones generales, cuando una de las partes tenga la condición de consumidor, le serán aplicables todas las normas de tutela y protección que correspondan, en particular, respecto a la abusividad de determinadas cláusulas —v.gr.: Ley 5/2019, de 15 de marzo, reguladora de los contratos de crédito inmobiliario—.

4.2.1.2. El lenguaje de programación obedece a una lógica *booleana* por lo que los contratos automatizados no admiten cláusulas que necesiten de interpretación para ser verificadas

Asumir que la programación de los contratos automatizados debe ser en lenguaje máquina tiene implicaciones significativas. Frente al lenguaje humano, que juega con matices y ambigüedades, el lenguaje máquina no las permite. Las decisiones obedecen a una lógica *booleana*, es decir, se estructuran en instrucciones condicionales, *si A entonces B, si C entonces D*. Por ello, este tipo de contratos no admite cláusulas que necesiten de interpretación para ser verificadas[70]. Piénsese en expresiones tales como variación de las bases esenciales del negocio, buena fe, hecho de Dios, consumidor medio, diligencia debida, honrado comerciante o padre de familia, etc.

Esto implica que, a día de hoy, dado el estado actual de la técnica, no será posible codificar cualquier obligación en un contrato automatizado, por las propias limitaciones del lenguaje para describir la obligación, «comprenderla», comprobar o verificar su cumplimiento y, en su caso, llevar a cabo las actuaciones programadas en caso de incumplimiento, o, al menos, no será posible plantearla en los mismos términos y con la misma extensión[71].

Los contratos tradicionales, en lenguaje humano, contienen muchos conceptos de un carácter eminentemente subjetivo e imprecisos desde el punto de vista de su posible sistematización y parametrización y, por tanto, de difícil encapsulamiento en un algoritmo ejecutable en un ordenador en cuanto que respecto de dichos conceptos no es posible conocer, *a priori,* todas las variables que han de intervenir en la formulación de la valoración a la que dichos conceptos se refieren, al ser distintas para cada caso concreto y, por otro lado, pueden existir otros supuestos en los que dichas valoraciones

únicamente podrán adoptarse a partir, no de variables concretas, sino de meros elementos circunstanciales, indiciarios, etc.

Por ello, hay que tener en cuenta, como sostiene el Informe *Legal and Regulatory Framework of Blockchains and smart contracts,* que dependiendo de la complejidad del acuerdo puede ser extremadamente difícil codificar adecuadamente los términos del mismo, de modo que un contrato automatizado podría ejecutarse de acuerdo con lo escrito en lenguaje tradicional pero, sin embargo, comportarse de un modo diferente porque el lenguaje máquina no ha traducido correctamente o no tenía capacidad para traducir lo escrito en el lenguaje tradicional. Por esta razón, según el referido Informe, las auditorías para comprobar la validez y viabilidad de los *smart contracts* devienen importantes, lo cual plantea la cuestión de si tales auditorías deberían ser simples requerimientos o deberían tener, además, algún tipo de reconocimiento legal para garantizar la validez de un *smart contract*, cuestión que está por decidir[72].

4.2.1.3. No todas las proposiciones son computables y trasladables a un algoritmo porque los sistemas axiomáticos y algoritmos son intrínsecamente limitados

Pero, además de lo anterior, como exponemos a continuación partiendo de las matemáticas y acabando en los algoritmos, no todo es computable. Efectivamente, en 1931 el lógico-matemático checo Kurt GÖDEL publicó un artículo titulado: *«Sobre las proposiciones formalmente indecidibles de los Principia Mathematica*[73] *y sistemas relacionados I.»*[74] en el que se recogen sus dos teoremas de incompletitud[75] mediante los que demuestra el carácter incompleto de la matemática —primer teorema— y la imposibilidad de probar que la matemática esté libre de contradicciones —segundo teorema—[76].

En concreto, el primer teorema señalaba, simplificadamente, que dentro de un sistema matemático de axiomas consistentes —es decir, sin contradicciones entre ellos—, y lo bastante potente como para tener algún interés, habrá verdades matemáticas que puedan formularse dentro de dicho sistema pero que, sin embargo, su certeza no puede ser demostrada mediante dichos axiomas ni las reglas/teoremas deducidos de los mismos, es decir, el sistema es incompleto.

El segundo teorema es un caso particular del primero y demuestra que, precisamente, la proposición que afirma la consistencia del sistema —es decir, que no tiene contradicciones internas— es una de aquellas cuestiones indecidibles.

Por tanto, un tratamiento axiomático de las teorías matemáticas no puede agotar el campo de verdades de la matemática, dado que existirán

proposiciones aritméticas verdaderas que no pueden ser deducidas formalmente de ningún conjunto de axiomas mediante un conjunto cerrado de reglas de deducción o inferencia[77].

El impacto que estos teoremas causaron en el mundo matemático de la época fue profundo. Hasta entonces se tenía una fe ciega en el método axiomático/deductivo y, de hecho, ya se buscaba —David HILBERT, entre otros— la completa formalización del propio sistema deductivo.

Sin embargo, los teoremas de GÖDEL demostraron que aquella fe era incorrecta, al concluir que los sistemas formales son o bien incompletos o bien inconsistentes y que el método axiomático posee ciertas limitaciones intrínsecas que excluyen la posibilidad de que los sistemas matemáticos puedan llegar a ser plenamente axiomatizados ni que pueda establecerse su consistencia lógica interna.

Cabe, no obstante, que se añada un nuevo axioma o regla a un sistema formal como los descritos, de tal forma que este nuevo elemento permita demostrar la certeza de alguna de estas cuestiones indecidibles. Sin embargo, con ello, lo que se tendría no sería más que un nuevo sistema, formado por el inicial más el axioma añadido, en el que también podrían formularse nuevas proposiciones que podrían ser verdaderas pero cuya certeza no puede ser demostrada en base a las reglas y postulados de este sistema ampliado. En última instancia, lo que este teorema significa es que nunca se podrá alcanzar un conocimiento completo de un sistema formal dado, en base, únicamente, a una descripción axiomática del mismo y a procedimientos o razonamientos exclusivamente deductivos o lógicos.

Como ejemplos de proposiciones que se han demostrado indecidibles[78], se pueden señalar, entre otros, la hipótesis del continuo de CANTOR[79], el *Entscheidungsproblem* o problema de la decisión[80] o el décimo problema de HILBERT[81].

GÖDEL formuló estos teoremas en relación a sistemas matemáticos, pero desarrollos posteriores los generalizaron a sistemas algorítmicos como los ejecutables en un ordenador. En 1936, con pocos meses de diferencia pero independientemente, tanto ALONZO CHURCH[82] como ALAN TURING[83] consiguieron desarrollar, desde el punto de vista de la lógica formal, conceptos como funciones recursivas, funciones efectivamente calculables y algoritmos. TURING, además, definió y diseñó —¡una década antes de que se fabricase el primer ordenador!— las denominadas máquina de TURING y máquina universal de TURING que son conceptualizaciones de ordenadores ideales capaces de ejecutar algoritmos. Finalmente, sobre esta base, tanto CHURCH como TURING, demostraron que estos formalismos —los referentes a las funciones recursivas, a las efectivamente calculables así como los relativos a los algoritmos y en el caso de TURING, además, a la máquina de TURING— son equivalentes a los formalismos

de GÖDEL y que existen proposiciones que ningún algoritmo ejecutable en un ordenador podrá resolver[84] y, en concreto, lo demuestran para el *Entscheidungsproblem*.

No obstante todo lo anterior, GÖDEL creía que la mente humana tiene una forma intuitiva, no solamente computacional, de alcanzar la verdad, de tal forma que sus teoremas no limitaban el conocimiento verdadero que los seres humanos pueden llegar a alcanzar[85].

TURING, por su parte, en un primer momento, consideró que el cerebro humano funciona esencialmente igual que una computadora, aunque tendría una complejidad mucho mayor. La diferencia, por tanto, entre ambos sería solo una cuestión de complejidad, no de naturaleza esencial. No obstante, posteriormente, modificó aquella postura y defendió que el cerebro humano tiene, en realidad, capacidades que no son alcanzables por una computadora y que ciertas herramientas cerebrales, como, por ejemplo, la imaginación, intuición, etc., suponen una diferencia real entre mente humana y ordenador mecánico.

Existen, por tanto, problemas, cuestiones, proposiciones, etc., que no son trasladables a algoritmos y resolubles por un ordenador y no por su mayor o menor dificultad, la potencia de cálculo requerida o el tiempo necesario para su resolución, sino porque los sistemas axiomáticos y algorítmicos son intrínsecamente limitados; y si esta limitación existe respecto de ámbitos inherentemente formalizables y objetivos, como la matemática, cabe esperar mayores dificultades en ámbitos con un alto grado de subjetividad, como el Derecho.

Volviendo, no obstante, a los problemas concretos que plantean los contratos automatizados, es necesario estudiar aspectos adicionales, como son sus relaciones con los oráculos[86] y la conservación de estos contratos a lo largo del tiempo.

4.2.1.4. Los problemas que plantean las relaciones entre los contratos automatizados y los oráculos

Respecto del primer punto cabe preguntarse quién asumirá la responsabilidad en caso de que alguno de los oráculos utilizados por un contrato inteligente proporcione un dato erróneo —ya sea deliberada o accidentalmente— o si sus sistemas sufren una caída, un retraso al suministrar un concreto dato o un ataque o un mal funcionamiento y alguna de estas circunstancias, u otras semejantes, desencadena una ejecución automática de una cláusula del contrato que no debería haberse producido, causando perjuicios para alguna de las partes, que pueden ser de difícil o imposible reparación.

4.2.1.5. Los problemas que plantea la conservación de estos contratos a largo plazo

Por otro lado, la conservación de los contratos inteligentes en el tiempo es, también, una cuestión de capital importancia, sobre todo en el ámbito de la contratación inmobiliaria en el que los contratos se caracterizan, precisamente, por su larga duración.

Estos contratos estarán implementados en un concreto lenguaje informático, entendible por los programadores, que, luego, deberá ser traducido al lenguaje que el ordenador en el que se ejecute entienda —mediante su compilación o interpretación por una máquina virtual—.

Todas estas herramientas, por otro lado, experimentan una evolución tecnológica constante y, además, tienen dependencias respecto de la arquitectura y *hardware* de las máquinas en las que se ejecutan, de sus sistemas operativos, bases de datos, librerías, etc.; elementos todos ellos que, a su vez, tienen sus propios procesos de evolución tecnológica, que pueden ser muy breves, con lo que será necesario llevar a cabo frecuentes procedimientos de actualización, migración e, incluso, modificación o recodificación de los contratos existentes. Los mismos procesos de evolución tecnológica y brevedad en sus actualizaciones experimentarán los sistemas en los que se ejecuten los servicios proporcionados por los oráculos que utilice un concreto contrato, lo que, adicionalmente, puede dar lugar a cambios en la forma, vía formato o estructura, en la que estos servicios proporcionen la información, a lo que el contrato automatizado también deberá adaptarse para evitar ejecuciones incorrectas.

Todo lo anterior introduce nuevas y múltiples fuentes de error y de problemas de seguridad pero, también, plantea otros problemas, no ya de carácter tecnológico sino jurídico, como: ¿qué consentimientos serían necesarios para llevar a cabo estas tareas?, ¿bastaría que la persona o entidad que implementa y gestiona el sistema los realizase por su cuenta?, ¿sería necesario recabar el consentimiento de todos los que hayan firmado algunos de los contratos?, ¿qué pasa con los contratos en los que alguno de los otorgantes se oponga, aunque los otros no?, ¿qué pasa si alguna de estas incidencias exigen la modificación del código de los contratos ya firmados por los otorgantes y, por ello, en principio, inalterables?, ¿y, si como consecuencia de la migración, recodificación o instalación de actualizaciones que solucionen fallos de programación, se introducen nuevos fallos o el funcionamiento del contrato migrado no es exactamente igual que el del anterior?, etc.

Todos los anteriores problemas conducirán, inevitablemente, a la reducción de los contratos a lo técnicamente posible de forma confiable, a la necesidad de suscribir seguros junto con los propios contratos automatizados como medio para hacer frente a los riesgos tecnológicos y los problemas de

responsabilidad expuestos, así como a una fuerte estandarización no solo de contratos sino también de cada posible cláusula. Efectivamente, en un entorno de exclusiva, o mayoritaria, contratación por medio de contratos automatizados, y con el fin de minorar los riesgos indicados, se acabaría codificando y comprobando concienzudamente cada posible cláusula y los contratos se irían conformando como una especie de *Lego*, añadiendo las concretas implementaciones informáticas de las cláusulas que, a lo largo del tiempo, y en su utilización en numerosos contratos preexistentes, hayan demostrado no ser una fuente de errores, lo que, por otro lado, producirá problemas en cuanto a la capacidad de adaptación al ágil y cambiante tráfico económico.

Un escenario como este, sin embargo, choca con la libertad de empresa y de contratación propias de una moderna economía de mercado, que se fundamenta en la libertad individual y la autonomía de la voluntad, consagradas en el artículo 16 de la Carta de los Derechos Fundamentales de la Unión Europea y que, por ejemplo, en el ordenamiento jurídico español no solamente se reconoce en la Constitución —artículo 38: «*Se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio…*»— y en el propio Código civil —artículo 1255: «*Los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público*»— sino también en la legislación hipotecaria que establece un sistema de libre constitución de derechos reales y, así, el artículo 2.2 de la Ley Hipotecaria señala que: «*En los registros expresados en el artículo anterior se inscribirán: … 2.º. Los títulos en que se constituyan, reconozcan, transmitan, modifiquen o extingan derechos de usufructo, uso, habitación, enfiteusis, hipoteca, censos, servidumbre y otros cualesquiera reales*» y en el artículo 7 de su reglamento que: «*Conforme al artículo 2.º de la Ley no solo deberán inscribirse los títulos en que se declare, reconozca, transmita, modifique o extinga el dominio o los derechos reales que en dichos párrafos se mencionan, sino cualesquiera otros relativos a derechos de la misma naturaleza, así como cualquier otro pacto o contrato de trascendencia real que, sin tener nombre propio en derecho, modifique, desde luego o en lo futuro, algunas de las facultades del dominio sobre bienes inmuebles o inherentes a derechos reales*».

No parecería lógico, por tanto, optar por una concreta solución técnica que suponga o que obligue a reducir las libertades de las que disfrutan los ciudadanos y que el ordenamiento jurídico les reconoce —sobre todo cuando existen otras opciones que permiten preservarlas— ya que ello significaría atribuir a la tecnología el carácter de elemento esencial, y no accesorio o instrumental —que es su verdadero sentido—, lo que conduciría, finalmente, a que solamente se pudiesen establecer aquellas relaciones contractuales

que fuesen posibles técnicamente y en el modo y forma que la tecnología determinase, lo cual es inaceptable.

4.2.2. El conflicto o dilema entre autoejecutabilidad y complejidad contractuales

4.2.2.1. Referencia al ámbito inmobiliario

En efecto, lo expuesto pone de manifiesto que existe un conflicto entre autoejecutabilidad y complejidad contractuales. Ello explicaría por qué la cadena de bloques se está desarrollando especialmente en el ámbito de las finanzas[87] y, en particular, en determinadas áreas como las de los derivados[88], los cuales han alcanzado tal grado de estandarización que, en realidad, son *legal commodities*[89].

En el ámbito inmobiliario, sin embargo, las cosas se desarrollan muy distintamente. En efecto, suelen ser transacciones más complejas basadas en una relación contractual que suele prolongarse en el tiempo —contratos relacionales[90]—. En los bienes inmuebles, además, pueden coexistir simultáneamente diversos tipos de *property rights* y, además, en muchas ocasiones las prestaciones se desarrollan a lo largo del tiempo y están sometidas a condiciones, es decir, al cumplimiento de acontecimientos futuros e inciertos, cuya apreciación no siempre es automatizable.

Hay que suponer, sin embargo, que un desarrollo progresivo de la inteligencia artificial permitirá que puedan ser autoejecutables transacciones cada vez menos simples.

Ello exige hacer una referencia al estado actual de desarrollo de la inteligencia artificial.

4.2.2.2. Referencia al estado actual del desarrollo de la Inteligencia Artificial —IA—

Puede afirmarse que todavía falta un largo camino por recorrer para que una inteligencia artificial pueda sustituir plenamente y con unas garantías mínimas a un operador jurídico, salvo que este realice tareas simples y de carácter repetitivo, lo que facilita su automatización.

Al igual que ocurriera previamente con las cadenas de bloques, así como con tantas otras tecnologías emergentes, la inteligencia artificial, actualmente, está de moda y experimentando una auténtica burbuja de expectativas. De este modo, se puede comprobar que cualquiera que sea el parámetro o la magnitud a la que se atienda —número de proyectos de investigación,

de publicaciones, volumen de inversión, menciones en la industria, en la política, etc.—, la inteligencia artificial no para de crecer[91].

Este ambiente ha provocado que, al igual que ocurrió en el cambio de siglo cuando las empresas estaban obsesionadas con añadir la expresión.*com* a su nombre, hoy en día esto está sucediendo con la expresión *inteligencia* artificial o *IA*. ¿El motivo?, posicionarse mejor en el mercado, sobre todo, ante los inversores. Y parece que esta estrategia está dando resultado ya que un reciente estudio[92] afirma que aquellas *startups* que dicen usar inteligencia artificial reciben entre un 15% y un 50% más de financiación que el resto, a pesar de que el 40% de dichas marcas, en realidad, no trabajan en nada relacionado con la IA.

Sin embargo, a pesar de que hoy en día la IA es una tecnología emergente no puede decirse que sea nueva ni, tampoco, que sea realmente inteligente.

Suele citarse la Conferencia de Dartmouth, celebrada en 1956 en la Universidad del mismo nombre, como la que marcó el arranque de esta materia, aunque, en realidad, sus inicios son anteriores[93]. En dicha Conferencia los padres de la disciplina —Allen NEWELL, Herbert SIMON, Marvin MINSKY, Arthur SAMUEL y John MCCARTHY, este último fue el que le propuso el nombre de inteligencia artificial— sentaron sus bases en aspectos muy diversos como el procesamiento en lenguaje natural, las redes neuronales, los sistemas expertos, etc.

La conferencia finalizó en un ambiente de franco optimismo y así, por ejemplo, H. SIMÓN declaraba que en los 20 años siguientes las máquinas serían capaces de realizar el trabajo de cualquier hombre, mientras que MINSKY afirmaba que el problema de crear inteligencia artificial estaría sustancialmente solucionado durante su generación y, efectivamente, en los años 60 la IA vivió una época de esplendor con continuos desarrollos y avances pero, a pesar de ellos y del optimismo inicial, el objetivo de alcanzar una inteligencia artificial semejante o equiparable a la humana se demostró inalcanzable, con lo que las inversiones comenzaron a cortarse, las líneas de investigación a cerrarse y se entró en el periodo denominado *invierno de la IA*, que se extendió durante toda la década de los 70 y hasta finales de los 80, momento en el que la disciplina, poco a poco, resurge y comienzan a desarrollarse conceptos como *learning*, *deep learning*, inteligencia computacional, etc.

De esta época es también la caracterización tradicional de los diferentes tipos de Inteligencia Artificial[94] que distingue entre:

— *IA débil*: Se encuadrarían en esta categoría los sistemas dedicados a resolver problemas muy concretos y delimitados. Si se les enseña una nueva tarea *olvidarán* cómo hacer la anterior —olvido destructivo—. Son sistemas reactivos, sin ningún tipo de iniciativa ni capacidad de adaptación.

Se programan por humanos y no razonan —solo computan—. Se pueden citar como ejemplos de sistemas IA débiles los relacionados con juegos como DeepBlue —ajedrez—, AlphaGo —Go—, Watson —Jeopardy—, etc. pero, también, lo son los asistentes de voz, los de movilidad autónoma, etc.

Es en este nivel donde se han producido todos los avances que hasta ahora se han llevado a cabo en el campo de la IA. No obstante, todos ellos tienen más que ver con la potencia de computación que con la inteligencia. Se trata de sistemas que, respecto de una sola y concreta tarea, son mucho más eficientes computacionalmente que los humanos y, por tanto, están relacionados, más que con una inteligencia general, con un aspecto mucho más concreto y limitado de esta, que podría identificarse como una inteligencia procedimental o mecánica.

Prueba de ello es la llamada paradoja de MORAVEC[95], formulada por H. MORAVEC, R. BROOKS y M. MINSKY y que pone de manifiesto la aparente contradicción que supone el que, por un lado, pueda lograrse que los ordenadores lleven a cabo tareas que, *a priori*, son consideradas como difíciles por los humanos y hasta el punto de vencer a estos —como ocurre con el ajedrez, el *go*, etc.— pero, por otro lado, que sea difícil o imposible lograr que las máquinas alcancen determinadas habilidades de carácter perceptivo, motriz o lingüístico, que sí tienen, por ejemplo, los niños de corta edad, como la capacidad de reconocer personas o animales[96], de distinguir objetos[97], de moverse por un espacio con obstáculos[98], de poder realizar múltiples tareas o la ironía, el sarcasmo, el humor, etc. Así, los niños pequeños no necesitan ser entrenados en millones de imágenes de, por ejemplo, gatos antes de que puedan reconocerlos en una imagen. Es más, entenderán inmediatamente el concepto abstracto de gato, lo que, además, luego les servirá para identificarlos en contextos diferentes, lo que una IA, de momento, es incapaz de hacer.

— *IA general*: Categoría introducida con posterioridad a las otras dos y que se refiere a sistemas capaces de resolver cualquier tarea intelectual que se les presente y no solamente una como los del caso anterior. Son proactivos, flexibles, autoprogramables, capaces de adaptarse y de formular juicios y razonar ante una situación de incertidumbre a partir del aprendizaje y el entrenamiento previo. No existe, hoy en día, ningún sistema de este tipo.

— *IA fuerte*: En este caso se trataría de sistemas que tendrían las mismas características que los de la categoría anterior, pero, además, serían autoconscientes, con capacidad subjetiva propia, así como para sentir emociones. Tampoco existe, a día de hoy, ningún sistema de esta clase.

Como decíamos anteriormente, los únicos sistemas de IA existentes actualmente son IA débiles sin que, de momento, se tenga idea alguna de cómo implementar un sistema de IA general o de IA fuerte. Uno de los motivos es que se desconoce el funcionamiento del único modelo que tenemos para

poder implementar sistemas de aquellos dos tipos: el cerebro humano y, tampoco, de cómo surgen en él las distintas cualidades mentales como la consciencia, la comprensión, el pensamiento, el razonamiento abstracto, el simbólico o, incluso, el ilógico o absurdo —además del deductivo, mecánico o procedimental que las máquinas sí han alcanzado—, la intuición, la imaginación, la creatividad, el sentido común, etc.

En este sentido, cabría preguntarse si el cerebro, la mente humana, es o no computable, es decir, formalizable en un algoritmo, o conjunto de ellos, ejecutables en un ordenador. Se trata, sin embargo, de una cuestión no resuelta —puede que nunca lo sea— y muy controvertida, existiendo reputados defensores de una y otra postura. Como ejemplos de autores que defienden que la mente humana es esencialmente superior a un ordenador, además de los ya citados anteriormente: GÖDEL o TURING, se pueden citar al físico-matemático R. PENROSE[99] o el filósofo J. R. LUCAS[100] y entre los que sostienen la postura contraria, es decir, que el cerebro es fundamentalmente una computadora compleja y que, al menos teóricamente, es posible que los ordenadores lleguen a equipararse a aquel, pueden mencionarse a D. HOFSTADTER[101] o a D. DENNETT[102].

Lo que si es cierto es que los sistemas de IA actuales únicamente han logrado simular las partes computables de la inteligencia humana, como el cálculo, el razonamiento procedimental, deductivo o mecánico, etc., y que, por medio de estas herramientas, dichos sistemas han demostrado ser muy buenos en determinadas tareas como la búsqueda de patrones, la categorización y búsqueda de relaciones en grandes volúmenes de datos que, en principio, parecen inconexos, etc. Sin embargo, no es posible encontrar en ellos atisbo alguno de cualquiera de las otras cualidades mentales antes indicadas.

En este sentido, debe tenerse en cuenta, en primer lugar, que todos los algoritmos de IA existentes han sido, y lo siguen siendo, creados, desarrollados, implementados y perfeccionados por seres humanos, no por máquinas, y, en segundo lugar, que estos sistemas son incapaces de *elaborar* productos originales que requieran el concurso de aquellas últimas habilidades y, así, por ejemplo, la IA no podría crear, en el ámbito de las artes, estilos como el arte abstracto o el cubismo —aunque si puede recrear el estilo de artistas de estos movimientos en base a sus obras— no directamente conectados con la realidad o, en relación con las ciencias, soluciones, en principio absurdas, como los números complejos o imaginarios[103] y que, sin embargo, son imprescindibles en la matemática —además de en la propia matemática compleja, son utilizados en sectores como la geometría, las ecuaciones diferenciales, la topología, etc.— pero, también, en el resto de las disciplinas científicas como la física —relatividad, mecánica cuántica, etc.—, la ingeniería —aeronáutica, electromagnetismo, electrónica, electrotecnia, mecánica de fluidos, telecomunicaciones, etc.—, etc.

En cualquier caso, los éxitos actuales de la tecnología de la IA no se basan tanto en avances significativos en su base conceptual, que sigue siendo más o menos la misma que hace 30 años, sino en la mejora exponencial que se ha producido en cuanto a la capacidad para obtener, almacenar, procesar y analizar ingentes cantidades de datos.

Por medio de estas operaciones, los sistemas de IA tratan inmensos volúmenes de datos relativos a supuestos o casos previos tanto de la materia concreta a analizar como de sus resultados y, en base a algoritmos de optimización —con los que se busca maximizar o minimizar determinadas variables—, van *aprendiendo* y construyendo árboles de decisión que les servirán para proponer soluciones a los nuevos casos que puedan plantearse. No obstante, estas soluciones serán propuestas de carácter puramente estadístico, en el sentido de ser las más probables teniendo en cuenta la información previamente *aprendida* y la lógica del algoritmo utilizado, por lo que no debería esperarse que sean correctas en todo caso.

Debe tenerse en cuenta, como hemos indicado anteriormente, que la simple ejecución de algoritmos no implica que en estos sistemas exista comprensión alguna acerca del problema que están tratando, por lo que atribuirles el carácter de inteligentes parece, cuando menos, exagerado. En 1980, J. SEARLE propuso[104] el experimento mental de la *habitación china*[105] para ilustrar esta idea.

Existen, además, limitaciones que afectan a los algoritmos de IA. En primer lugar, están las limitaciones, ya vistas, que afectan a cualquier sistema algorítmico, puestas de manifiesto por GÖDEL, CHURCH y TURING y, también, las dificultades relacionadas con la formalización algorítmica de materias eminentemente subjetivas, pero, en segundo lugar, los algoritmos utilizados en el ámbito de la IA tienen limitaciones y problemas específicos, como, por ejemplo, las siguientes:

— No es posible implementar ningún algoritmo de aprendizaje universal o genérico que, en todo caso, pueda proporcionar resultados correctos a los supuestos que se le planteen en base, únicamente, a la información que haya obtenido de los datos con los que ha aprendido. Es lo que resulta del teorema NFL para la optimización[106] que demuestra que existe una probabilidad no despreciable de que los algoritmos de este tipo —independientemente de cómo se hayan programado— proporcionen resultados totalmente erróneos cuando se les presenten nuevos supuestos que no se correspondan exactamente con aquellos con los que se ha alimentado al sistema para que aprendiese. Corolario de lo anterior es que los datos, por sí solos, no son suficientes, sino que habrán de ir acompañados necesariamente de conocimiento sobre la materia concreta que se está abordando y que habrá de introducirse, si ello fuera posible, en el algoritmo, lo que requerirá la intervención humana.

El teorema, sin embargo, no da indicación del tipo de conocimiento que será necesario introducir, sino que esta será una cuestión que dependerá de cada caso y habrá de determinarse por medio de prueba/error.

— En segundo lugar, y como consecuencia de la forma de operar de estos algoritmos, los resultados que proporcionan suelen presentar sesgos que tienen dos causas o fuentes principales: los datos de aprendizaje y la elección e implementación concreta del propio algoritmo.

Respecto de la primera de estas causas, las soluciones que proporcionan los algoritmos de IA son muy sensibles a los datos con los que se los alimenta de tal forma que puede ocurrir que aprendan en base a supuestos insuficientes o no relevantes para el caso concreto, bien porque ello se haga a propósito o porque se crea que los proporcionados son los únicos relacionados con la materia a tratar, porque se desconozca cuáles pueden ser los más importantes o porque no se disponga de datos relevantes, y se empleen otros sustitutivos, o se primen supuestos no directamente relacionados. Este tipo de riesgos, además de dar lugar a resultados inexactos, hace que las soluciones propuestas tengan sesgos en favor de los resultados de los supuestos con los que el sistema ha aprendido y, así, ha provocado que, entre otros calificativos, se haya acusado a los sistemas de IA de racistas[107], machistas[108], de perjudicar a los consumidores[109], de discriminar, e incluso matar a los pobres[110], etc.

La segunda de las causas está relacionada con la calidad de los algoritmos utilizados y los posibles errores o desviaciones en su codificación o en las ponderaciones e importancia que estos algoritmos atribuyen a cada uno de los supuestos de aprendizaje, ya se hayan producido intencionada o inadvertidamente, lo que, indudablemente, puede tener consecuencias dramáticas para los titulares de los intereses sobre los que se decide y constituye un medio por el que puede introducirse la manipulación política, social o dar lugar a resultados discriminatorios[111]. Un ejemplo de ello es el sistema COMPAS que es una herramienta de IA utilizada en los tribunales estadounidenses para evaluar la probabilidad de que un condenado pueda reincidir y que condiciona la probabilidad de que le sea otorgada, o no, la libertad condicional. El sistema no utiliza la raza del sujeto en su evaluación, pero sí tiene en cuenta otros criterios sesgados como el código postal. Los resultados que proporcionan pueden ser considerados racistas porque, en la práctica, atribuyen mayores índices de peligrosidad a afroamericanos que a blancos[112].

— Por último, los algoritmos de IA una vez que han sido codificados y empiezan su aprendizaje en base a los miles de supuestos de muestra que se le proporcionan, comienzan también, a comportarse autónomamente, en el sentido de que van estableciendo ponderaciones y construyendo sus propios árboles de decisión, lo que dificulta o imposibilita saber u obtener una justificación de por qué el algoritmo ha adoptado una determinada decisión, en relación con un nuevo caso que se le ha presentado[113]. Esta

circunstancia, por otra parte, plantea dificultades a la hora de determinar a quién debe atribuírsele la responsabilidad por los perjuicios causados por las decisiones erróneas del algoritmo de entre todos los que intervienen en la implementación y funcionamiento del sistema, a saber: el diseñador del algoritmo, su programador, quien haya seleccionado los casos en base a los cuales el sistema aprenderá, la persona que haya introducido en él estos precedentes, el operador del sistema, etc.

Estos y otros riesgos son algunas de las razones que explican que los poderes legislativos hayan comenzado a ocuparse de estos temas. Así, por ejemplo, en el ámbito europeo, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos[114] reconoce, en su artículo 22[115], el derecho de los ciudadanos a no ser objeto de una decisión basada, únicamente, en un tratamiento automatizado de la información, a poder reclamar intervención humana y a poder oponerse a la decisión adoptada e impugnarla. Además, el mismo Reglamento, esta vez en su artículo 15.1.h[116], también reconoce el denominado «derecho a la explicación»[117], es decir, el derecho a obtener información significativa sobre la lógica del algoritmo aplicado, en caso de que se hayan producido decisiones automatizadas que afecten a las personas, incluidas las elaboraciones de perfiles.

Pero no solo los legisladores, también los fabricantes tecnológicos —entre ellos *Amazon, Apple, Facebook, Google, IBM, Microsoft, Nvidia*, etc.— y organizaciones humanitarias —como Amnistía Internacional o *Human Rights Watch*— advierten de los riesgos de la utilización de estos algoritmos en el ámbito jurídico[118], tomando como ejemplo el sistema COMPAS antes mencionado, e incluso, han reclamado que dejen de aplicarse[119] por sus sesgos, imprecisión y opacidad y, también, por las graves consecuencias que tienen para los afectados.

Es necesario recordar que los operadores jurídicos con facultades jurisdiccionales o ejecutivas están obligados a resolver las pretensiones que se les presenten mediante resoluciones que, ya sean estimatorias o desestimatorias, habrán de estar motivadas, basadas en hechos y fundamentos de derecho y tener en cuenta las pruebas practicadas y las circunstancias concurrentes. Estas resoluciones, además, habrán de expedirse en todo caso, aun cuando no existan precedentes del caso concreto de que se trate o, aunque exista un cambio o una laguna legal en las normas aplicables.

No parece, por tanto, que con el estado actual de la materia sea aconsejable, ni tampoco deseable, que la adopción de decisiones que pueden afectar profundamente a la libertad y al resto de derechos fundamentales de una persona, a sus relaciones personales o a su patrimonio se encomiende a un conjunto de algoritmos, de ejecución implacable, fría, despiadada e irresponsable, en los que solamente se puede llevar a cabo una formalización parcial

de los conceptos subjetivos que integran el derecho; que adoptan sus decisiones no en base a razonamientos jurídicos sino en base a precedentes, que, como tales, devienen inútiles en caso de un cambio en la legislación o en la interpretación jurisprudencial o doctrinal de la norma y cuyos supuestos de hecho, pruebas y circunstancias pueden coincidir, o no, con los del caso a resolver o que puede que no sean los más pertinentes para ello o que, incluso, contribuyan a alejarlos todavía más de la solución correcta; que desconocen, no comprenden ni utilizan conceptos como justicia, ética, equidad, etc.; que tampoco tienen comprensión alguna del problema a resolver ni de las consecuencias de las posibles soluciones y que, como toda justificación de las decisiones que adopten, solo proporcionarán una mera probabilidad estadística de acierto que, además, tampoco estará del todo claro cómo han obtenido.

En definitiva, debe tenerse en cuenta que la inteligencia artificial implica la cesión del control humano en favor de las máquinas y de los algoritmos, que en ellas se ejecutan, los cuales no sienten ni comprenden ni se arrepienten ni responden ante nadie ni son capaces de evaluar la proporcionalidad de una decisión. Por todo ello, la aplicación del ordenamiento jurídico no debería dejarse en manos de algoritmos; la supresión de aquel control humano minaría permanentemente nuestros derechos, libertades y seguridad. Lo anterior, sin embargo, no quiere decir que esta tecnología deba considerarse como un enemigo, pero para que esto sea así será necesario que no se sustituya nuestro juicio por el suyo.

4.2.2.3. La existencia de una correlación negativa entre el valor de los derechos y la complejidad de las transacciones

Vaticinar, hoy por hoy, cuál sería el límite de la complejidad contractual autoejecutable no es fácil y ni siquiera posible, pero difícilmente podrán ser autoejecutables los contratos relacionales, frecuentes en el ámbito inmobiliario.

Puede afirmarse, por último, que existe una correlación negativa entre el valor de los derechos y la complejidad de las transacciones, por lo que, en este ámbito, los contratos automatizados y la cadena de bloques se desarrollan más fácilmente en transacciones de bajo valor[120].

4.2.3. Cuando los contratos no son autoejecutables es necesaria la intervención de un tercero

Será necesaria, por lo tanto, en un amplio rango de supuestos, la intervención de terceros. Ello no solamente rompe el concepto de la cadena

de bloques como sistema autosuficiente persona a persona en el ámbito contractual, sino que pone al descubierto su principal debilidad: la institucional, lo que no debería sorprendernos. En efecto, si la tecnología de los bloques encadenados es infalible, solo debería regir la *lex criptographica*, pero, dado que la realidad muestra que no lo es, debe estar sometida al Estado de Derecho, como cualquier otra tecnología y, en general, cualquier comportamiento humano. La cadena de bloques, sin embargo, carece de tecnología institucional en caso de fallo porque, supuestamente, no falla. En todo caso, aunque la hubiera previsto, quedaría subordinada al Derecho.

Que el diseño institucional sea la principal debilidad de la cadena de bloques es especialmente significativo porque esta tecnología no incorpora ninguna nueva tecnología electrónica o física, sino que, partiendo de las existentes, las interrelaciona alineando, pretendidamente, los diferentes intereses en juego de modo que sean, supuestamente, convergentes. Sin embargo, como veremos seguidamente, no consigue que tal convergencia de intereses se produzca. Para demostrarlo, haremos referencia, en primer lugar, al modo como se han solucionado algunos de los principales incidentes habidos hasta ahora, para centrarnos después en la figura de los mineros y en los conflictos de intereses entre los diferentes agentes intervinientes.

4.2.3.1. Los incidentes *DAO —Decentraliced Autonomous Organization—*

El primer incidente conocido en la plataforma *Ethereum* tuvo lugar en 2016. Esta plataforma es considerada por muchos como el paradigma de los *smart contracts* y su objetivo es implementar el principio de la *lex criptographica*, conforme al cual *code is law*[121], lo que significa que el código criptográfico, por sí solo, provee una autoejecutabilidad completa y repele su sometimiento a cualquier normatividad proveniente de un tercero, sea privado o público, incluido el Estado. En la realidad, sin embargo, las cosas se desarrollan muy distintamente, como puso de manifiesto el incidente sucedido en 2016.

Ante un fraude ocurrido en una cadena de transacciones, el equipo directivo de la plataforma decidió ejecutar una *hard fork,* esto es, una modificación en el *software* para revertir transacciones previas consideradas inválidas. Ello significaba la negación misma de la inmutabilidad de las transacciones, así como de su autoejecutabilidad y, en definitiva, del principio *code is law* decididas, además, por un escaso número de afectados y, por lo tanto, de interesados, nada neutrales para resolver el conflicto. Evidenció, asimismo, la existencia de una autoridad central, no elegida por nadie y sin autoridad legal alguna, con un innegable grado de poder que, además, usó en su propio beneficio. Ello dio lugar a que la comunidad se

dividiera y fundara una nueva criptomoneda, teóricamente fiel a las esencias del sistema, denominada *Ethereum Classic* (ETC), aunque solo hasta cierto punto porque, al menos para los casos de fraude, admite el recurso ante los tribunales[122].

Este tipo de fraudes puede ocasionar graves perjuicios, específicos de los contratos inteligentes, tanto como consecuencia de la irrevocabilidad de las transacciones como de que, potencialmente, pueden afectar a todos los contratos que residan en la misma plataforma. Efectivamente, mientras que un fallo en un programa tradicional se soluciona instalando un parche o bien modificando su código fuente, recopilando e instalando la nueva versión y, en su caso, reconstruyendo datos, en el caso de los contratos inteligentes esto no es tan sencillo ya que las transacciones en la cadena de bloques no pueden revertirse por lo que la única forma de arreglar las consecuencias de un fallo de programación, además de modificar el código fuente como en el caso tradicional, es reescribir la historia, algo que, teóricamente, el protocolo de los bloques encadenados no permite.

Este incidente en el proyecto DAO fue posible porque había un fallo de programación en su código que permitió, solo un mes después de que el proyecto echase a andar, extraer *ether's* de unos 11.000 usuarios hasta alcanzar el equivalente de unos 50 millones de dólares. En este sentido, no se trató de un ataque en el sentido clásico, sino que el atacante, cuya identidad, a día de hoy, todavía es desconocida, simplemente hizo uso de una posibilidad —que era un error de programación— que el código ofrecía y así lo recalcó él mismo en una carta abierta que hizo pública en Internet[123], en la que, además, amenazaba con tomar medidas legales en caso de que las monedas que había conseguido le fuesen *robadas*, *incautadas* o *congeladas*.

Después de todo, como dice el slogan de la plataforma *Ethereum*, el código es la ley y, por tanto, si el código permite llevar a cabo una determinada acción por un tercero —aunque se trate de un error de programación—, una vez que los contratos han sido firmados por los otorgantes, teóricamente, estos han consentido todas las posibilidades que ofrece el código que integra dicho contrato y, al ser el código la ley del contrato, aquella acción es legal y debe ser permitida.

La historia pudo repetirse de nuevo. En enero de 2019, un día antes de una actualización planificada del *software* de la plataforma *Ethereum*, la compañía de seguridad *ChainSecurity*, especializada en auditoría de seguridad de contratos inteligentes, notificó a los gestores de dicha plataforma que la actualización provocaría, nuevamente, que algunos contratos quedasen expuestos a la misma vulnerabilidad que afectó al proyecto DAO[124]. Igualmente, una sola auditoría llevada a cabo en marzo del pasado año ha detectado vulnerabilidades de diverso tipo en decenas de miles de contratos de la plataforma[125].

En cualquier caso, los anteriores no han sido los únicos incidentes con los contratos inteligentes de *Ethereum*. Así, entre otros, se puede señalar el que ocurrió a principios de noviembre del 2017, cuando otro fallo de programación en las denominadas *Parity Wallets* supuso la inutilización de los contratos y la congelación de 280 millones de dólares en *ethers*[126]. A diferencia del caso anterior, en este supuesto el *bug* fue activado accidentalmente por un usuario que, además, había notificado días antes a la plataforma la existencia del mismo. En cualquier caso, llovía sobre mojado ya que en julio del mismo año otro fallo en las *Parity Wallets* permitió el robo de 32 millones de dólares en *ethers*[127] y, hace relativamente poco tiempo, entre los días 5 y 7 del mes de enero de 2019, la plataforma *ethereum classic* sufrió un ataque del 51% mediante el cual los atacantes anularon y reorganizaron bloques, llevaron a cabo dobles gastos, etc., hasta conseguir un equivalente total aproximado de 1,1 millones de dólares[128].

Por otra parte, BEDNAREK, A.[129] ha puesto de manifiesto la realización de otro tipo de ataque a la plataforma, aunque puede afectar a todo sistema que se base en el protocolo de las cadenas de bloques, y que consiste en la búsqueda sistemática de claves privadas.

Las claves privadas en la plataforma *Ethereum* tienen una longitud de 256 bits, por lo que el número de posibles claves privadas es de 2^{256}, que es un número mayor que el de átomos que se estima que tiene el universo conocido.

Hay que recordar que para operar con sistemas basados en el protocolo *blockchain* los usuarios habrán de disponer de una o más parejas de claves y que cada una de estas parejas está compuesta por una clave privada y otra pública[130].

Estas parejas de claves suelen generarse mediante los programas cliente que hacen las veces de monedero, y que se pueden instalar en un ordenador, tableta o teléfono personal, o bien mediante las cuentas abiertas en los sistemas de las entidades que prestan servicios de compra, venta y cambio de criptomonedas. Lo único que protege a los usuarios frente a que su misma pareja de claves se genere por sistemas distintos y se asignen a personas diferentes es la estadística, ya que es altamente improbable que se generen claves iguales, dado el elevado número de claves privadas posibles —en el caso de *Ethereum:* 2^{256}, como hemos visto anteriormente—.

No obstante, dentro de este conjunto de posibilidades, existen claves privadas que son más *débiles* que otras, en el sentido de que tienen una baja aleatoriedad, como aquellas en las que todos, o casi todos, los caracteres que las conforman son iguales[131]. Este tipo de claves pueden generarse bien porque el *hardware* criptográfico o el programa monedero que las genere tengan una baja calidad, bien por un defecto de programación, bien porque el usuario haya seleccionado una determinada clave privada que le sea

fácilmente memorizable con el fin de evitar el riesgo de perder las monedas en caso de avería, pérdida, robo, etc., del soporte en el que hubiese almacenado dicha clave privada, o bien para no tener que almacenarla en ningún soporte y, así, evitar accesos indebidos a estos.

Mientras que a partir de una clave pública no puede obtenerse su clave privada asociada, para obtener la clave pública que se corresponde a una determinada clave privada, solo tenemos que aplicar a esta última una función criptográfica.

Teniendo en cuenta lo anterior, el ataque consiste en elaborar listados de posibles claves privadas débiles, calcular las claves públicas que les corresponden y comprobar, en la cadena de bloques —que es pública—, si alguna de estas claves públicas se ha utilizado alguna vez. Si es así, significa que dicho par de claves, pública y privada, se han asignado a algún usuario y como el atacante tiene ambas claves puede acceder a la cuenta de aquel y reenviarse las monedas que contenga a una cuenta propia.

En el estudio indicado anteriormente, BEDNAREK A. muestra que, efectivamente, existen cuentas basadas en claves privadas débiles o *adivinables* y, también, atacantes dedicados a vaciar estas cuentas en la forma descrita en el párrafo anterior y, de hecho, uno de ellos llegó a reunir de esta forma un equivalente superior a 54 millones de dólares[132].

4.2.3.2. El *Bitcoin Cash*

En 2017 se planteó un conflicto en el seno de la comunidad *Bitcoin* sobre el tamaño de los bloques[133]. El protocolo de *Bitcoin* lo fijó en un tamaño relativamente bajo, a efectos de evitar ataques de denegación de servicio, lo que, sin embargo, disminuye la velocidad de procesamiento, haciendo que la de *Bitcoin* sea mucho menor que la de los operadores financieros ordinarios.

Con esta situación, el citado conflicto puso de manifiesto el conflicto existente entre los diversos intereses en juego. Efectivamente, se observa que los desarrolladores están interesados en el perfeccionamiento y mejora del rendimiento del protocolo. Los usuarios, por su parte, también están interesados en tiempos cortos para la confirmación de sus transacciones, pero, igualmente, en comisiones lo más bajas posibles, mientras que las compañías y los mineros desean aumentar sus ingresos en el corto plazo, así como disminuir sus costes; y esta contraposición de intereses ha dado lugar a una auténtica guerra civil y a la adopción de soluciones *hard fork*, al igual que en el caso de *Ethereum.*

A los efectos de este trabajo, interesa destacar que, con motivo de este conflicto, también se ha puesto de manifiesto la monopolización de la práctica totalidad de la capacidad de minado por unos pocos grupos, que se

oponen a cualquier modificación que pueda alterar su estatus actual, lo que supone, además, la pérdida de control de *Bitcoin* por parte de los usuarios que era, precisamente, uno de los objetivos iniciales; también la falta de claridad respecto de la cuantía de las comisiones a pagar por la realización de las transacciones y su previsible rápido crecimiento en el futuro; la falta de democracia en la comunidad *Bitcoin,* etc.[134].

Todo ello pone de manifiesto la existencia de fallos básicos de tecnología institucional ante los que los usuarios están indefensos, en manos de quienes dominan las plataformas y cuyos intereses solo pueden ser defendidos, en última instancia, por el Estado. A estos conflictos pasamos a referirnos seguidamente.

4.2.4. La necesidad de determinar la legislación aplicable y la conveniencia de homogeneizar su regulación

Hoy por hoy, los contratos automatizados carecen de una regulación específica en nuestro país.

Cierto es que, como sostiene LEGERÉN-MOLINA[135], la idea con la que surgieron estas cadenas era establecer un sistema de pagos alternativo al vigente —eliminando la necesidad de intermediarios— al ser una base de datos descentralizada y permanente y, en cierta medida, que «actúa fuera de las fronteras del Derecho». Pero cierto es también que cuando surjan problemas en la ejecución —*bugs* en el código, por ejemplo—, ha de arbitrarse algún sistema de reclamación; dificultad que se agrava por el hecho de que en las cadenas de bloques intervienen personas de diferentes jurisdicciones. En tal sentido, en algunos Estados se está desarrollando legislación tanto sobre las cadenas de bloques como sobre los contratos automatizados.

Por ello, el primer Informe sobre *Legal and Regulatory Framework of Blockchaions and Smart Contracts*, elaborado por el *European Union Blockchain Observatory and Forum,* publicado el 27 de septiembre de 2019[136] propone, entre otras recomendaciones, definir legalmente, a nivel de la Unión Europea, qué debe entenderse tanto por *smart contracts* como por *blockchain*, así como armonizar su regulación, dando prioridad a los problemas planteados por las mismas relacionadas con el entorno digital y la protección de datos.

Mientras tanto, en nuestro país, hemos de acudir a la normativa general de los negocios jurídicos y contratos, a la que regula la contratación electrónica, la relativa a los servicios de la información, a pesar de que no den respuesta acabada a todos los eventuales problemas, así como, en su caso, la legislación de condiciones generales, la protectora de los consumidores y de blanqueo de capitales, entre otras.

V. LA DEBILIDAD DEL DISEÑO INSTITUCIONAL DE LA TECNOLOGÍA DE LA CADENA DE BLOQUES: LOS INCENTIVOS DE LOS DIFERENTES ACTORES DE LA RED NO ESTÁN ALINEADOS

5.1. Introducción

Una institución es un conjunto de normas de todo tipo que definen lo que está permitido y lo que está prohibido en un determinado campo y, por lo tanto, modulan la conducta humana[137]. Para que ese conjunto de normas genere el comportamiento deseado es necesario que los incentivos de los diferentes participantes se ajusten a fin de que cada uno de ellos adopte el comportamiento esperado y, en el caso de no ser así, exista una autoridad que sancione los comportamientos no permitidos y, de este modo, desincentive, en última instancia, la adopción de tales comportamientos.

Como hemos visto, la tecnología de la cadena de bloques presenta debilidades sustanciales en ambas vertientes de su diseño institucional, lo que es especialmente grave porque no incorpora ninguna nueva tecnología electrónica, sino que se vale de las existentes, pero, afirmando que ha generado un diseño institucional que alinea los intereses de los participantes hasta tal punto que impide los comportamientos deshonestos y, por lo tanto, hace innecesaria la intervención de terceros. En este apartado vamos a centrarnos en estos aspectos.

5.2. Los incentivos de los mineros

El objetivo de Satoshi NAKAMOTO cuando publicó su artículo[138], en el que presentaba el primer diseño del sistema *Bitcoin*, era el establecimiento de una red de intercambio de valor, global, descentralizada, caracterizada por la privacidad, sin intermediarios y configurándola como una especie de organismo autorregulado en el que los distintos intereses en juego se reforzarían unos a otros, todo ello en beneficio de los usuarios, que serían el centro del sistema.

En este diseño los mineros desempeñan un papel crucial, ya que son los actores mediante los que se introducen nuevas monedas en el sistema y, además, sobre ellos descansa toda la labor de garantizar la seguridad mediante el minado de los bloques y la construcción de la propia cadena de bloques.

Desde este último punto de vista, cuanto mayor sea el número de mineros, es decir, cuanto mayor sea la capacidad total de minado que en un momento dado exista en el sistema, mayor será la dificultad para resolver la búsqueda matemática mediante la que se minan los bloques y, por tanto,

menor será la probabilidad de que un minero o un grupo de mineros, puedan llevar a cabo con éxito un ataque del 51%.

De este modo, el sistema será tanto más seguro cuanto mayor sea la capacidad de cálculo de la que disponga, pero, idealmente, también sería necesario que dicha capacidad se encuentre distribuida entre un elevado número de mineros, de tal forma que ninguno de ellos, por sí solo o conjuntamente con otros, pueda atacar el sistema con ciertas garantías de éxito.

Si se cumplen estas condiciones se desactivan las eventuales intenciones de burlar al sistema, por parte de un minero que quisiese hacerlo, al no tener capacidad suficiente para ello, ya sea por sí solo o aún asociándose con otros. De esta forma se *fuerza* a que los intereses de todos los mineros se encuentren alineados con los objetivos que persigue el protocolo *Bitcoin.*

En los primeros días del sistema, dichas condiciones, efectivamente, se cumplían. *Bitcoin* todavía tenía escaso valor y los mineros tenían un carácter principalmente doméstico, utilizando sus propios ordenadores personales para llevar a cabo las labores de minado, cumpliéndose así el sueño libertario de Satoshi, de producir dinero *cultivándolo* domésticamente.

No obstante, conforme el valor de la moneda subía, un número cada vez mayor de mineros ingresaba en el sistema, lo que, a su vez, provocó que la probabilidad de que un minero concreto consiguiese minar un bloque disminuyese, pero, al mismo tiempo, también provocó que los gastos aumentasen. Para salvar estos inconvenientes, los mineros comenzaron a profesionalizarse y a asociarse y, así, compartir ganancias y gastos. De esta forma, a día de hoy, el minado de bloques se ha transformado en una actividad totalmente industrializada, lo que, además, ha supuesto la práctica expulsión de los mineros domésticos u ocasionales.

Efectivamente, la creciente complejidad técnica y, también, los crecientes recursos financieros, materiales y humanos necesarios para minar las monedas favorecen la aparición de superestructuras o grupos de mineros y de grandes granjas con miles de máquinas especializadas, dedicadas exclusivamente al minado de criptomonedas y ello hasta tal punto que, en los meses anteriores a la fecha de este artículo, más del 50% de la capacidad de minado mundial estaba en manos de, únicamente, tres de estos grupos y solamente nueve de ellos reunían, aproximadamente, el 80% de la capacidad total de minado[139].

Como consecuencia de lo anterior, no solo se ha producido una progresiva y efectiva centralización, en contra de los postulados y objetivos iniciales con los que se había diseñado el protocolo, sino, también, que los mineros comenzaran a desarrollar comportamientos que pueden considerarse no conformes con aquellos objetivos y los intereses de los usuarios e, incluso, abusivos.

Lo anterior, sin embargo, no debería sorprender ya que, en esta materia, como en toda actividad humana, siempre habrá alguien dispuesto a lucrarse

a costa de otros y los únicos impedimentos que pueden evitar que lo hagan son la dificultad y los costes necesarios para lograrlo, así como la probabilidad de ser detectado y sancionado, la cual, en este caso, es bastante baja dado el anonimato que caracteriza el protocolo.

Así, pueden encontrarse actuaciones encuadrables en lo que podría denominarse comportamientos abusivos derivados del carácter cuasi monopolístico de las grandes agrupaciones mineras, así como de la actividad lobista de empresas que se desenvuelven en torno a los mineros —fabricantes de *hardware* especializado en minado [ASIC's], etc.—, que buscan, principalmente, el mantenimiento de su *status quo*, oponiéndose a toda alteración que vaya en detrimento de sus ingresos, para lo cual no han dudado, incluso, en acosar a los disidentes. Estas actitudes se han producido en, entre otros momentos, la denominada guerra por el tamaño de los bloques, suponen un obstáculo insalvable para el desarrollo y la evolución tecnológica del sistema y ocasionan perjuicios a los usuarios.

Pero, además, los mineros también están realizando actuaciones deshonestas como, por ejemplo, los ataques del 51% que recientemente han comenzado a producirse.

Por lo que respecta a la guerra por el tamaño de los bloques, cabe señalar que, en un principio, no se fijó un tamaño máximo para los bloques, sino que este era libre. Sin embargo, ello facilitaba la realización de ataques de denegación de servicio, consistentes en que cualquier minero podría crear bloques de, por ejemplo, varios *gigabytes* integrados por micro-transacciones fraudulentas[140], lo que provocaría que los nodos de la red perdiesen la mayor parte de su tiempo y capacidad descargando, verificando y retransmitiendo bloques; dejándolos sin tiempo ni recursos para confirmar las transacciones regulares y, por otra parte, también daría lugar a la expulsión de los pequeños mineros sin recursos suficientes para adquirir máquinas que pudiesen soportar aquella carga y minar bloques tan grandes, provocando, con ello, la centralización del sistema.

No obstante, fijar un tamaño bajo de bloque tiene sus propios inconvenientes ya que abriría la puerta a otro tipo de ataques, los denominados *ataques de inundación,* que tratan de saturar el sistema, también con micro-transacciones fraudulentas, de tal forma que la mayoría de las transacciones existentes en un momento dado en el «depósito» de transacciones sin confirmar, de donde los mineros obtienen las transacciones que van a incluir en los nuevos bloques, serían este tipo de transacciones, con lo que las legítimas tendrían muchas dificultades para ser incluidas en una nueva propuesta de bloque, dado el reducido tamaño de estos.

Finalmente, como solución de compromiso, a mediados de 2010 se fijó el tamaño de 1Mb, aunque, debe tenerse en cuenta que este tamaño es un tamaño máximo, es decir, puede haber bloques más pequeños y, de hecho,

hasta enero y marzo de 2017 no se produjeron los primeros bloques de 0,98 Mb y 0,99 Mb, respectivamente, y, hasta octubre de 2017[141], no se minó el primer bloque de 1 Mb.

Sin embargo, este tamaño de bloque tiene como consecuencia que la capacidad máxima de procesado de transacciones por unidad de tiempo se reduce a, aproximadamente, siete transacciones por segundo, frente a los operadores financieros tradicionales que tienen velocidades de procesamiento de decenas de miles por segundo[142].

Para remediar este problema, a lo largo de 2015 se formularon diversas propuestas para aumentar el tamaño de los bloques[143]: *Bitcoin Classic, Bitcoin Unlimited, Segregated Witnes*, etc. Una de las más ambiciosas era la denominada *Bitcoin XT*, de G. ANDRESEN y M. HEARN, que habían sido desarrolladores principales de *bitcoin*, y consistía en aumentar el tamaño de los bloques de 1 Mb a 8 Mb en una primera fase, para duplicarlo posteriormente cada dos años, hasta alcanzar los 8.192 MB, añadiendo, además, mejoras en el protocolo.

No obstante, para que cualquiera de estas propuestas fuese adoptada era necesario que se aceptase e instalase por la mayoría de los mineros. Sin embargo, estos se opusieron fuertemente a la mayoría de ellas — y, sobre todo, a *Bitcoin XT* que era una de las que mayor tamaño de bloque proponía— incluso realizando ataques coordinados a los nodos que las instalasen.

Finalmente, como consecuencia de todo ello, a principios de 2016 M. Hearn, comunicaría su retirada[144] denunciando la monopolización de la práctica totalidad de la capacidad de minado por unos pocos grupos que sistemáticamente se oponían a cualquier modificación que pudiera alterar su *status,* la pérdida de control de *bitcoin* por parte de los usuarios, la falta de claridad respecto de la cuantía de las comisiones a pagar, la falta de democracia en la comunidad *bitcoin* y, en definitiva, el, a su juicio, carácter fallido del sistema.

En cualquier caso, el problema persistía y, conforme el tamaño de los bloques se iba acercando a 1 Mb, las comisiones también comenzaron a aumentar. Así, mientras que la media de las comisiones que los mineros recibieron por día durante 2014 fue de 12,86 *bitcoins* y de 22,22 *bitcoins* en 2015, comenzó a aumentar considerablemente a partir de entonces, alcanzando una media de 67,19 *bitcoins* en 2016 y de 268,37 *bitcoins* en 2017 y, en días concretos de este último año, se llegaron a pagar, también en media por día: 588 *bitcoins* el 30 de mayo; 783 *bitcoins* el 13 de noviembre o 1495 *bitcoins* el 22 de diciembre[145]. Estas últimas cantidades llegaron a representar el 42% de las retribuciones totales que los mineros recibían —comisiones más retribución por el minado de bloques—. A partir de 2017, no obstante, las ganancias por comisiones comenzaron a descender bruscamente hasta la media actual, en 2019, de 57,93 *bitcoins*.

Lo anterior demuestra que los usuarios estaban dispuestos a pujar unos contra otros por un recurso que cada vez se hacía más escaso: el espacio en los bloques, con el fin de que sus transacciones fuesen confirmadas e incluidas en ellos cuanto antes. Es el tradicional juego de oferta y demanda, de tal forma que la cuantía de las comisiones en cada momento vendrá determinada por la intersección de la demanda de espacio en los bloques para incluir las transacciones y la oferta de dicho recurso, que es fijo, lo que limita el número máximo de transacciones que pueden incluirse en cada uno.

En relación con ello, debe tenerse en cuenta, además, la asimetría que existe en el protocolo de los bloques encadenados entre las políticas de retribución y las de pago de comisiones, ya que, mientras que para la retribución de los mineros se establecen normas estrictas que determinan su reducción a la mitad cada vez que se minan 210.000 bloques, no existen directrices claras en cuanto al pago y a la cuantía de las comisiones ya que nada obliga a un usuario a pagar una cuantía mínima, pero tampoco nada obliga a los mineros a incluir en un bloque las transacciones que no vayan acompañadas del pago de alguna comisión, ni tampoco existe un tope máximo para la cuantía de estas. Todo ello hace que en periodos en los que se realicen un gran número de transacciones, lo que, en principio, parecería deseable, desde el punto de vista del éxito del sistema, el importe de las comisiones pueda crecer descontroladamente y que, por otro lado, la confirmación de aquellas transacciones que no vayan asociadas al pago de alguna comisión, o en las que el importe de estas sea bajo comparadas con las demás, pueda quedar pospuesta indefinidamente dentro de dichos periodos.

En consecuencia, los usuarios están interesados en bloques más grandes, pero no los mineros, ya que ello les supondría una menor recaudación por comisiones, las cuales, además, cada vez adquirirán mayor importancia dada la retribución decreciente que obtienen por minar bloques y, únicamente estarían dispuestos a admitir aumentos en el tamaño de los bloques en la cuantía mínima necesaria para evitar la huida de usuarios del sistema, como así ha ocurrido.

Efectivamente, uno de los motivos que explican el descenso brusco en las comisiones —además de la pérdida de valor de la moneda a partir de finales de 2017, principios de 2018— fue la activación, a partir del 23 de agosto de 2017, de una de las propuestas de modificación del sistema antes indicada, la denominada: SegWit —*Segregated Witness*— consistente en una modificación mínima del protocolo *Bitcoin* que supone el aumento efectivo del tamaño de los bloques pero sin necesidad de realizar un *hard fork* sino un *soft fork* —a diferencia de, por ejemplo, *Bitcoin Cash* que supuso un *hard fork*, también en agosto del 2017— y, por tanto, manteniendo la compatibilidad con la cadena existente en ese momento. Esto se consigue, simplificadamente, mediante la reorganización y optimización de los datos

de las transacciones, principalmente de sus firmas, lo que produce un efecto equivalente a aumentar el tamaño de los bloques a, aproximadamente, 2 MB.

Esta modificación fue apoyada por el 99,95 % de la red y fue adoptada como solución de compromiso para evitar la fuga de usuarios, también por no suponer más que un aumento mínimo de tamaño y por no requerir la realización de un *hard fork*; no obstante, su utilización está siendo muy gradual, de tal forma que, a día de hoy, las transacciones SegWit todavía no han superado el 55% del total[146]. En cualquier caso, el cambio supuso el aumento del indicado recurso escaso del espacio en los bloques y, por tanto, la disminución de su «precio». Parece, por otra parte, que esta modificación ha sido suficiente, al menos por el momento, ya que el tamaño del bloque más grande que se ha minado desde entonces es de 1,305 MB[147].

5.3. La existencia de intereses contrapuestos entre los diferentes participantes

De todo lo anterior puede deducirse la existencia de intereses contrapuestos entre los diversos actores intervinientes. Por un lado, como hemos señalado anteriormente, están los de los programadores y desarrolladores del sistema que buscan, básicamente, perfeccionarlo y mejorar, entre otros factores, su seguridad y su «productividad» y hacia este fin estaban encaminadas las propuestas de aumento del tamaño de los bloques antes mencionadas. Los usuarios, por su parte, buscan la rápida confirmación de sus transacciones, pero, también, unas comisiones lo más bajas posible, por lo cual también les interesan bloques de mayor tamaño. Finalmente, los intereses de los mineros son, fundamentalmente, la disminución de los costes y el aumento de sus ingresos en el corto plazo, pero estos intereses se ven perjudicados con bloques de mayor tamaño ya que:

— Ello supone un mayor número de transacciones que verificar, transmitir e incluir en cada bloque que, al ser más grande, también será más difícil de minar, por lo que aumentarán los recursos de computación necesarios para mantener los tiempos medios de minado que tenían antes del aumento de tamaño y, por tanto, para mantener su retribución media, lo cual supone mayores costes de operación.

Debe tenerse en cuenta que durante 2016 y 2017, dada la popularidad creciente y el aumento de valor del *Bitcoin*, los grandes grupos de mineros acometieron importantes inversiones con el fin de incrementar su capacidad de cálculo. Luego sobrevino la caída de valor de la moneda sin que todavía hubiesen amortizado aquellas inversiones; las cuales, por otro lado, podrían resultar inútiles en caso de que, para aumentar el tamaño de los bloques,

fuese necesario llevar a cabo un *hard fork*, al no mantenerse la compatibilidad del nuevo protocolo respecto del anterior, ya que las máquinas especializadas de minado —ASIC's— que utilizan, podrían no funcionar en el nuevo escenario o hacerlo con mucha menor productividad.

— Por otro lado, cuanto más grandes son los bloques, mayor es el riesgo de minar un bloque huérfano, es decir, un bloque que se incluya en una rama que acabe siendo desechada. Minar un bloque huérfano supone, para los mineros, una pérdida de tiempo, recursos y dinero.

— Unos mayores requisitos del *hardware* y una mayor tasa de bloques huérfanos pueden desestabilizar la generación de bloques y el cálculo de la dificultad del minado, lo que hará el sistema más inseguro.

— Con bloques de mayor tamaño el número de bloques necesarios para incluir las transacciones pendientes disminuye y, con ello, la probabilidad de conseguir minar un bloque y, por tanto, de ser retribuido por el sistema.

— Como se ha visto, la utilización de bloques más grandes supone, también, la disminución en la cuantía de las comisiones, ya que habrá menos competencia por el espacio en ellos, al ser este «recurso» más abundante. Y ello en un contexto en el que la retribución por el minado de bloques irá disminuyendo progresivamente.

Estas y otras razones explican la dura oposición de los mineros y de las empresas relacionadas con ellos a cualquier modificación del sistema que pase por aumentar el tamaño de los bloques y, en general, a cualquier otra mejora o perfeccionamiento del protocolo que pueda afectar a sus intereses. De esta forma, desarrollan comportamientos y prácticas monopolísticas, oponiéndose y desincentivando las mejoras del producto y, especialmente, aquellas que puedan suponer una reducción de precios permanente, de tal forma que los usuarios se verán abocados a pagar más y por una peor calidad.

Pero, además de lo anterior, recientemente, han comenzado a producirse ataques directos al sistema por parte de mineros. Efectivamente, los ataques del 51%, que hasta hace poco se consideraban posibilidades meramente teóricas o, en el peor de los casos, altamente improbables, ya se están produciendo.

Recordemos que, mediante este tipo de ataques, un minero o un grupo de mineros que reúnan más del 50% de la capacidad de minado existente en un momento dado, podrán llevar a cabo una serie de ataques sobre la cadena de bloques como evitar que determinadas transacciones sean confirmadas, reescribir el historial de transacciones, utilizar las mismas monedas para realizar múltiples pagos, etc.

En todo caso, debe tenerse en cuenta que, si bien reunir una capacidad de cálculo superior al 50% del total garantiza que se puedan llevar a cabo los anteriores ataques, el contar con una capacidad inferior a dicho porcen-

taje, pero, sin embargo, significativa, también permitirá atacar la cadena de bloques, no con total garantía de éxito —como en el caso de los ataques del 51%—, pero si con altas probabilidades de alcanzarlo[148].

Uno de los primeros ataques de este tipo ocurrió ya en 2013, con la moneda *Feathercoin*[149], que en aquel momento era la sexta criptomoneda más importante, pero es en tiempos más recientes cuando ha comenzado a aumentar su número. Así, desde mediados de 2018, se pueden mencionar, entre otros, los ocurridos con las siguientes monedas: *bitcoin Gold*[150] —respecto de la que los atacantes lograron hacerse con un equivalente a 18,6 millones de dólares—, *Verge Currency*[151] —en dos ataques sucesivos, con pocas semanas de diferencia, fueron sustraídos el equivalente a 1,1 y 1,75 millones de dólares, respectivamente—, *ZenCash*[152] —en este caso se sustrajo el equivalente a 550.000 dólares—, *Monacoin*[153] —aproximadamente cien mil dólares—, a finales de 2018 también fue atacada la moneda *Vertcoin*[154] —otros cien mil dólares— y, en enero de 2019, fue el turno de *Ethereum Classic*[155] —1,1 millones de dólares—.

Es cierto que algunas de las anteriores monedas no eran muy importantes en cuanto a su capitalización, tráfico y capacidad de minado que las sostenían, lo que facilita los ataques, pero, sin embargo, la última de las indicadas, *Ethereum Classic*, estaba dentro del top 20[156] por su capitalización en el mercado, en el momento de ser atacada. De todas formas, debe tenerse en cuenta que esta mayor facilidad para atacar las cadenas de bloques soportadas por capacidades de minado no muy elevadas es semejante a la que afecta a sistemas que pueden hacer uso de cadenas de bloques privadas —por ejemplo para gestionar un registro inmobiliario— en los que el número de nodos mineros es mucho más reducido que en el caso de las criptomonedas, y en los que a un agente deshonesto, ya sea interno o externo al propio sistema, le bastará con hacerse con el control de un número comparativamente mucho más reducido de nodos para llevar a cabo este tipo de ataques.

En cualquier caso, existen factores que permiten prever un número creciente de ataques en el futuro[157] como, por ejemplo:

— Que con el paso del tiempo la tecnología se va conociendo mejor, cada vez hay un mayor número de expertos en ella y los ataques que se producen son cada vez más sofisticados.

— La progresiva disminución de la retribución que los mineros reciben por minar bloques.

— La aparición de hardware de minado capaz de minar diversas monedas indistintamente[158].

— El descenso del precio del hardware de minado principalmente por la aparición de un gran mercado de segunda mano de este tipo de máquinas

como consecuencia del cierre de granjas de minado que han dejado de ser rentables al disminuir el valor de las criptomonedas[159].

— La proliferación de entidades que permiten alquilar grandes capacidades de minado[160].

— La explosión cámbrica en el número de criptomonedas, de tal forma que a día de hoy superan ampliamente las dos mil[161].

— La influencia de factores externos como la progresiva extensión a este sector de la legislación antifraude y contra el blanqueo de capitales, lo que provoca la huida de usuarios, la disminución del valor de las monedas y, con ello, de la rentabilidad del minado. También la posible prohibición de la actividad minera que se está estudiando en algunos países, como el caso chino antes mencionado, y que supondría la desaparición, de un día para otro, del 70% de la capacidad de minado mundial.

En definitiva, y si bien en el diseño del sistema se habían intentado compatibilizar los diversos intereses en juego, de tal forma que el ejercicio de sus propios intereses egoístas, pero lícitos, por cada uno de los actores intervinientes redundaría en beneficio de todo el sistema; la aparición de circunstancias no previstas inicialmente o que han supuesto una desviación de los parámetros de diseño del protocolo como: la progresiva profesionalización, industrialización y centralización de la minería, unido a la toma de conciencia —por parte de los propios mineros— de su carácter esencial para el sistema y su defensa de este *status,* la aparición de un nuevo mercado del que obtener ingresos —el del tamaño de bloque—, así como todos los indicados en la relación anterior; han provocado que los incentivos de cada uno de aquellos actores hayan dejado de estar alienados y, como consecuencia de ello, que hayan aparecido mineros dispuestos a atacar el sistema en beneficio propio si existe una mínima posibilidad de éxito.

De esta forma, las servidumbres de la realidad han superado al diseño, por lo que no puede darse por sentado que el protocolo *blockchain* garantizará, en todo caso, que solo se desplegarán actitudes irreprochables, independientemente de las circunstancias concurrentes, sino, que, como se ha visto, estas circunstancias han determinado que los mineros hayan comenzado a actuar más estratégicamente y a desarrollar comportamientos abusivos y deshonestos.

5.4. No hay ninguna autoridad competente para tomar decisiones ni responsable de los daños causados

Teóricamente, la cadena de bloques opera de un modo completamente descentralizado y, por lo tanto, sin autoridad central alguna que vigile o

controle las transacciones. Son los propios participantes los que desempeñan esa función. En consecuencia, en caso de conflicto, como señala LEGERÉN-MOLINA[162], no habrá una entidad a quien reclamar y que deba de hacer frente a la responsabilidad que eventualmente pudiese surgir, sea civil, penal o de otro tipo. Como señala GÓMEZ GÁLLIGO[163] no solo no hay una autoridad supervisora sino tampoco responsable.

Como consecuencia, en la realidad, cuando se plantea un conflicto, como cualquiera de los enumerados a lo largo de estas páginas, los resuelven quienes tienen *poder* para hacerlo, aunque no tengan *autoridad* para ello. Siempre hay alguien que tiene poder para ello porque el sistema nunca es completamente descentralizado, sino que siempre hay una clave matriz originaria que permite su monitorización. Y la realidad demuestra que quien tiene el poder lo usa siempre en su propio beneficio.

Por ello, estamos de acuerdo con LEGERÉN-MOLINA[164] en que este hecho invitará, como parece sensato, a que los potenciales intervinientes —especialmente, cuando pretendan invertir gran cantidad de tiempo o dinero— deliberen de manera detenida la conveniencia de participar o no en cadenas de bloques de carácter público.

Todo ello pone de manifiesto que la tecnología de la cadena de bloques no es autosuficiente, y que, por lo tanto, requiere la intervención humana. También pone de manifiesto que no es tan descentralizada como se pretende, sino que se halla, en última instancia, bajo un poder incontrolado —un «dictador benevolente»—, por lo que tampoco tiene un contenido inmodificable, sino que, por el contrario, puede ser modificado en caso de que así convenga a los intereses de quienes tienen el poder para hacerlo.

Para que la cadena de bloques pueda, por tanto, resultar socialmente útil, debemos olvidar la pretensión de sus impulsores originarios de sustituir las instituciones por la tecnología y, por el contrario, someterla a las exigencias del Estado de Derecho, utilizándola, en la medida de lo posible y conveniente, para aumentar la eficacia y la eficiencia institucionales.

VI. LA TECNOLOGÍA DE LA CADENA DE BLOQUES NO ES UN SISTEMA AUTOMÁTICO —Y, POR TANTO, AUTOSUFICIENTE— DE TRANSMISIÓN DE TITULARIDADES *IN REM*

6.1. Distinción entre sistemas automáticos y sistemas automatizados

Como hemos visto, los contratos automatizados necesitan la cooperación de terceros en un amplio número de escenarios, en mayor medida cuanto mayor sea su complejidad, la cual, generalmente, se halla en función directa de la cuantía, siendo los contratos inmobiliarios de cuantía y, por tanto,

complejidad, comparativamente elevadas. Por ello, en ese ámbito, en una abrumadora mayoría de casos, estos terceros son humanos. Probablemente, en un futuro previsible continuarán siendo humanos.

Cuando nos referimos a la intervención humana en relación con los Registros de la Propiedad, en función de su alcance, hemos de distinguir entre registros automáticos y registros automatizados[165].

Un Registro de la Propiedad es automático cuando el procedimiento registral es iniciado mediante una aplicación y se desarrolla sin intervención de ninguna autoridad registral.

Un Registro de la Propiedad es automatizado cuando los procedimientos registrales son conducidos electrónicamente pero necesitan de la intervención de la autoridad registral para que se pueda variar el contenido de los asientos registrales, o, en general, en diferentes fases y aspectos del procedimiento registral —v.gr. emitir una certificación—.

Bitcoin requiere la intervención de los denominados *mineros. Ethereum* y, en general, la tecnología de la red de bloques encadenados que implican el intercambio de criptomonedas por activos *tokenizados* con existencia fuera de la red también requieren mineros o figuras semejantes. Una de las principales funciones de los mineros consiste en ordenar los bloques encontrando la solución a un problema matemático consistente en calcular correctamente un *hash*. En consecuencia, la cadena de bloques no es un sistema automático sino automatizado.

El minero que resuelve en primer lugar dicho problema es recompensado en *bitcoins* o en la criptomoneda que corresponda. No obstante, como hemos expuesto anteriormente, esta no es la única fuente de ingresos de los mineros. También obtienen ingresos provenientes del pago de comisiones por las partes contratantes. Aunque el pago de comisiones no es obligatorio para confirmar las transacciones, sí lo es para acelerar el proceso de validación y, de este modo, aumentar las posibilidades de obtener la titularidad en el caso de que haya habido *doble disposición*, denominada *doble gasto* en el entorno de la cadena de bloques.

Como hemos expuesto, actualmente, no es obligatorio el pago de comisiones para obtener la validación contractual. Solamente es obligatorio para aumentar la velocidad con la finalidad de aumentar las probabilidades de obtener dichas validaciones. Sin embargo, cuando el sistema de recompensa por el cálculo del *hash* finalice, las comisiones por acelerar dichas validaciones serán la única fuente de ingresos de los mineros y, previsiblemente, las comisiones serán más elevadas[166]. De hecho, entre las principales razones que indujeron a M. HEARN a abandonar la comunidad se hallaba la falta de transparencia en las comisiones y su previsible incremento futuro, así como la falta de democracia en la comunidad *Bitcoin*, es decir, la falta de control de la cadena de bloques por sus usuarios[167].

Llegados a este punto, es necesario tener en cuenta que, como hemos subrayado anteriormente, esta estructura de incentivos de los mineros alimenta comportamientos perversos, porque los incentivos de los diferentes protagonistas, como hemos visto, no se hallan alineados. De hecho, la raíz del problema de los incidentes mencionados anteriormente era, de un lado, el conflicto de intereses entre los mineros, interesados en un menor tamaño de los bloques para, de ese modo, incrementar sus ingresos y, de otro lado, los desarrolladores del *code* y usuarios, interesados en bloques de mayor tamaño por razones de rendimiento, seguridad y cuantía de las comisiones y, finalmente, las compañías alrededor de la cadena de bloques con intereses principalmente coincidentes, aunque no siempre, con los de los mineros.

Algo similar sucedió en el ámbito de *Ethereum*. Por diseño, toda operación procesada por la *Ethereum Virtual Machine* es ejecutada por todo nodo activo en la red *Ethereum*.

Para prevenir abusos, el protocolo *Ethereum* carga una pequeña comisión —denominada *gas*— por cada paso computacional. Para prevenir fluctuaciones excesivas de los precios, el precio del *gas* no es fijo sino que es ajustado por los mineros dinámicamente basándose en el precio de mercado del *ether*[168].

Dado que *Bitcoin Blockchain* solamente puede almacenar una cantidad limitada de información por cada transacción y dado que *Ethereum Blockchain* cobra por cada paso computacional en un programa de contrato autoejecutable o *smart contract*, a menudo es prohibitivamente caro construir aplicaciones descentralizadas que confíen en *blockchain* como instrumento de archivo[169] lo que, a nuestro juicio, constituye una grave limitación que puede desincentivar su implantación en diferentes entornos.

Es necesario, en conclusión, llamar la atención sobre el hecho de que la cadena de bloques necesita intermediarios —aunque no sea el Estado sino ciudadanos o empresas privadas—, lo que significa que no es un sistema de persona a persona, a pesar de ser esta una de sus características más resaltadas.

6.2. La cadena de bloques no es autosuficiente sino que sustituye unos operadores por otros

Lo que, en realidad, hace la cadena de bloques es sustituir unos operadores —entre los que se encuentra el Estado— por otros —mineros, desarrolladores, oráculos, etc.—.

Pero, además, será necesario que alguno de estos operadores esté investido de alguna autoridad para poder forzar la solución a situaciones para las que el protocolo no está preparado.

Ocurre así, por ejemplo, en los supuestos de incapacidad por pérdida de facultades mentales o, también, en los casos de fallecimiento de un usuario con una o varias cuentas de monedas virtuales y que no hubiera compartido con nadie esta información ni, por tanto, las claves correspondientes, lo que, por otra parte, es lo recomendable desde el punto de vista de la seguridad.

En esta situación, los allegados o herederos de dicho usuario, con la configuración actual del sistema —caracterizada por el anonimato y falta de cualquier autoridad que controle su funcionamiento—, no tienen forma de saber si el incapacitado o causante tenía o no cuentas en monedas virtuales, cuántas ni cuales. Alternativamente, puede que, si tuvieran conocimiento de que, efectivamente, tenía aquel tipo de cuentas e incluso puede que sepan cuáles son, por conocer los identificadores —las claves públicas— de dichas cuentas; pero, tanto en este último caso como en el previo, si no conocen las claves privadas correspondientes, serán incapaces de acceder a las monedas, dado que el protocolo no proporciona ninguna vía a la que acudir para forzar su transmisión o su conversión en moneda real. La misma situación se plantearía no solo en los anteriores supuestos sino también en el caso de pérdida de las claves privadas por parte de su titular.

Precisamente, una situación semejante a la descrita ha alcanzado, recientemente, cierta repercusión mediática. Concretamente, el CEO de la mayor empresa de criptomonedas de Canadá, *QuadrigaCX*, falleció en diciembre de 2018 llevándose consigo las claves privadas de las cuentas en las que almacenaba, en diversas monedas virtuales —*bitcoin, litecoin, etherum, ripple, dogecoin*, etc., los fondos depositados por sus inversores —aproximadamente unos 145 millones de dólares pertenecientes a cerca de 90.000 depositantes— imposibilitando el acceso a las mismas[170].

Esta persona era muy consciente de los riesgos de seguridad a los que, empresas como la suya, se encuentran expuestas —no en vano se estima que un equivalente a unos mil setecientos millones de dólares en criptomonedas en 2018[171] y mil doscientos millones solo en el primer cuatrimestre de 2019[172] han sido robados o estafados en alguna forma mediante ataques a cuentas en empresas que prestan servicios de monederos, de inversión, de cambio de criptomonedas, etc., y todo ello cuantificando, solamente, los incidentes que han transcendido— y, así, todos los terminales que utilizaba: ordenadores, móviles, tabletas, etc., estaban encriptados; guardaba los fondos depositados en su empresa en carteras frías —no conectadas a Internet, salvo por el tiempo imprescindible para realizar alguna transferencia— y a las que solo él tenía acceso. Irónicamente, todas estas medidas, así como el propio funcionamiento del protocolo *blockchain*, han provocado la bancarrota[173] de la empresa y la pérdida de los fondos por los depositantes.

La solución que se ofrece para este tipo de situaciones, por parte de los defensores de la tecnología, es compartir las claves privadas con otras

personas —lo que evidentemente tiene sus propios riesgos— o ponerlas bajo la custodia de personas o entidades ante las que pueda acreditarse el fallecimiento del titular de aquellas claves para luego entregárselas a quien este hubiera dispuesto o depositarlas en entidades que presten servicios denominados «*dead man switch*», de tal forma que si, en los intervalos temporales acordados, el titular no realiza determinada acción —acceder a una página *web* específica, contestar a un mensaje, correo electrónico, etc.— se supone que ha fallecido y la transmisión de las claves se realiza automáticamente a quien se hubiese especificado al contratar el servicio, todo ello a cambio del pago de una cantidad periódica.

Estas soluciones, además de suponer nuevos costes y riesgos, ya que abren la posibilidad al ataque, robo o uso indebido de estas cuentas y de las claves que custodian así como a que se produzca la transmisión de las claves sin que el fallecimiento haya, efectivamente, ocurrido; en realidad implican la aparición de nuevos intermediarios —lo que, como hemos dicho, va en contra de la filosofía del sistema— y, por otra parte, no resuelve el problema en aquellos casos en los que no se haya adoptado alguna de estas medidas, con lo que, con el paso del tiempo, se irá incrementando el número de monedas inmovilizadas por estas causas. No parece que este, si no se modifica, pueda ser un sistema que pueda gestionar, razonablemente, no solo un sistema de pago o inversión sino, tampoco, de contratación inmobiliaria.

Además, en relación con este último ámbito de la contratación inmobiliaria, una red *blockchain*, persona a persona y autogestionada —es decir, sin autoridad alguna que pueda resolver los conflictos— plantea otros problemas:

— ¿Qué ocurre si un propietario pierde su clave privada?, ¿pierde con ello sus facultades de disfrute y disposición sobre su propiedad? Parece que lo lógico sería que, para resolver este tipo de casos, se estableciese algún tipo de procedimiento ante una determinada autoridad para que se restableciesen sus derechos. No obstante, si dicha autoridad, como resultado del indicado procedimiento, puede hacer eso, y dado que el reclamante ha perdido la prueba de su propiedad, su clave privada, también se abre la posibilidad a que no lo haga o incluso a que se la atribuya a un tercero.

— ¿Qué ocurre si un tercero se hace con la clave privada de un propietario —por ejemplo, por robo, descuido, por la vía de las búsquedas de claves privadas antes indicada respecto de la plataforma *Ethereum,* etc.— y ese tercero transmite la finca a su favor, o al de otra persona, quedando esta transmisión *inscrita* en la cadena de bloques?, ¿qué vía puede utilizar el verdadero propietario para recuperar su propiedad según el protocolo *blockchain*?

— ¿Qué pasa en caso de que sea necesario llevar a cabo un procedimiento ejecutivo sobre una finca como consecuencia de un embargo o de la

realización de una garantía constituida sobre el inmueble? Presumiblemente el titular de la finca no se mostrará muy dispuesto a colaborar en dichos procedimientos o a entregar la clave privada al adjudicatario de la finca, por lo que será necesaria la intervención de alguna autoridad que proteja todos los intereses en conflicto y, en su caso, fuerce la transmisión de dicha clave.

— ¿Qué pasa en caso de «ocupación» ilícita de una propiedad? La clave privada no protegerá al propietario frente a esta circunstancia, sino que tendrá que ser, nuevamente, algún tipo de autoridad la que coercitivamente restablezca la situación anterior[174].

— ¿Qué pasa en caso de que se produzca un *hard fork* en la cadena de bloques que almacena los derechos sobre las fincas? En estos supuestos, para cada finca «inscrita» habrá dos *tokens* diferentes en cadenas distintas que se están refiriendo al mismo inmueble en la realidad, es decir, se producirá una doble inmatriculación masiva, lo que dará lugar a conflictos respecto de los derechos que recaen sobre ellas y, nuevamente, será necesaria una autoridad que los resuelva y establezca el procedimiento general a seguir en estos casos.

— Etc.

Cabe señalar que ninguno de estos problemas se produce en un sistema registral tradicional y que, en definitiva, si se necesita y se confía en una autoridad que resuelva los conflictos, también se podrá confiar en ella para gestionar el sistema registral.

VII. LLEGADOS A ESTE PUNTO, DEBEMOS PLANTEARNOS SI EL CONJUNTO FORMADO POR LOS CONTRATOS AUTOMATIZADOS Y LA TECNOLOGÍA DE LA CADENA DE BLOQUES PUEDEN DESEMPEÑAR LAS FUNCIONES DE LOS REGISTROS DE LA PROPIEDAD INMUEBLE

7.1. Premisas básicas. Titularidades *in personam*, titularidades *in rem* y fe pública registral

Aunque hay sistemas registrales de diversos tipos, nos centraremos, sobre todo, en los registros de derechos, con una breve referencia final a los registros de documentos.

Para responder adecuadamente a esta cuestión, debemos partir de una serie de premisas básicas:

Los contratos solo producen efectos *inter partes* y, por lo tanto, solo sirven para ordenar las relaciones entre A y B, pero no las relaciones con C y, en general, con todos los demás, denominados terceros.

Las titularidades *in rem* se caracterizan porque no pueden ser alteradas *inter privatos* sin la voluntad de su titular, a diferencia de las titularidades *in personam,* las cuales sí pueden ser alteradas contra la voluntad de su titular, siendo sustituidas por la indemnización correspondiente.

Las titularidades *in rem* son más valiosas que las titularidades *in personam* porque impiden que terceros puedan influir tanto en la titularidad como en el contenido de los derechos. Ello es así porque las titularidades *in rem* se hallan protegidas por una regla de propiedad mientras que las titularidades *in personam* lo están por una regla de responsabilidad[175].

Las titularidades *in rem* sobre derechos reales inmobiliarios solo pueden ser adquiridas mediante usucapión o mediante un sistema adquisitivo basado en un registro de derechos. No basta un contrato, aunque vaya seguido de tradición y, por tanto, tampoco un contrato autoejecutable pues solo serviría para transmitir una titularidad obligacional, es decir, con efectos solamente *inter partes.* La razón estriba en que, en un contexto de contratación impersonal, cual es el propio de una economía de mercado, en ausencia de un registro de derechos, no es posible tener la seguridad de que se está adquiriendo de alguien con poder de disposición sobre la cosa. El registro de derechos suministra al adquirente esa seguridad.

Por definición, gracias a la fe pública registral, la inscripción suministra al mercado la identidad del titular del *ius disponendi* y, además, identifica las causas de anulación o resolución del derecho del mismo que, en caso de producirse, se impondrían al derecho del adquirente, ahorra a los adquirentes potenciales, es decir, al mercado, costes de información y, por tanto, de transacción ya que, como es sabido, los primeros están en la base de los segundos. Una sentencia de adquisición por usucapión no suministra al mercado esa información porque no suministra al adquirente la información de si el titular según la sentencia ha dispuesto de su derecho y, en el caso de que adquiera del titular según la sentencia, no queda protegido frente a quien haya adquirido de un titular registral con facultades de disposición y demás requisitos exigidos en nuestro ordenamiento por el artículo 34 de la Ley Hipotecaria.

La fe pública registral, —que conlleva la adquisición de las titularidades inmobiliarias con efectos *erga omnes*—, la establece el artículo 34 de la Ley Hipotecaria. Parte de la regla básica del sistema transmisivo propio del Derecho común, en nuestro caso, contrato más *traditio*, consagrado por el artículo 609 del Código civil, pero le exige tres requisitos complementarios[176]:

1. El adquirente negocial debe adquirir de quien sea titular registral y tenga facultades para transmitir.
2. Debe hacerlo a título oneroso y, además, de buena fe, y
3. Debe solicitar y obtener la inscripción del derecho negocialmente adquirido, lo que incluye la titularidad sobre el mismo.

En Derecho alemán, el requisito de la adquisición del titular registral deriva de los parágrafos 873 y 892.1 del BGB, el primero referente a la necesidad de inscripción o *Eintragung* para que se produzca la adquisición y el segundo referente a la *Gutglaubenswirkung,* que engloba tanto la presunción de exactitud como la fe pública registral. El requisito de la onerosidad no se exige de una forma expresa, sino que deriva de que, conforme al parágrafo 822 BGB, la acción de enriquecimiento injusto puede alcanzar a los adquirentes a título gratuito.

Finalmente, el parágrafo 892.1 BGB, a diferencia del artículo 34 de la Ley Hipotecaria, no exige que el adquirente inscriba su adquisición para que tenga lugar la *Gutglaubenswirkung* o fe pública registral. Ello puede explicarse por el hecho de que en dicho sistema la inscripción es explícitamente constitutiva *inter contrahentes*, conforme al parágrafo 873 BGB 94, por lo que no es necesario volver a exigirla para que opere la *Gutglaubenswirkung*. En el sistema del Código civil —artículos 609 y 1095 —, sin embargo, la inscripción no es explícitamente constitutiva y, por ello, el artículo 34 de la Ley Hipotecaria, se ve obligado a exigirla, lo que revela el auténtico alcance de la inscripción dotada de fe pública en el sistema registral español.

Los requisitos de onerosidad y buena fe se deben a que la fe pública registral solo opera en relación a los denominados actos de mercado, en los que ambos requisitos deben estar presentes. El primero se basa en la aplicación del principio *qui certat de damno evitando anteponendus est qui certat de lucro captando*. El segundo se basa en que cabe que en el Registro de la Propiedad haya inexactitudes que, de ser conocidas por el tercero, este no debe poder beneficiarse de dicho conocimiento, ni siquiera en perjuicio de un adquirente anterior meramente negocial. Cuestión distinta es cuáles son esas inexactitudes.

¿Por qué se exigen los otros dos requisitos? Tales requisitos adicionales, el primero y el tercero de los enumerados anteriormente, son los que implican la *publificación*[177] del sistema transmisivo tabular. ¿Debería bastar con ello? No y por ello se requiere, además, que inscriba su adquisición, es decir, que solicite que el Estado le reconozca explícitamente como dueño. La razón de su exigencia hay que buscarla en el significado de la inscripción en un Registro de derechos.

La inscripción es un documento público que contiene una declaración formal de reconocimiento por el Estado de la titularidad de un derecho real sobre un bien inmueble, lo que implica, entre otras cosas, la atribución de una titularidad *in rem* o inatacable, si concurren las circunstancias exigidas por el sistema registral.

La inscripción dotada de fe pública registral es, así, el instrumento a través del cual el Estado suministra al mercado la identidad del *verus dominus*, que no es otro que el *dominus* reconocido como tal por el Estado mediante una inscripción dotada de fe pública registral, pues el adquirente negocial no inscrito es solo eso, un adquirente meramente negocial o privado.

Queda, por tanto, saber si la tecnología de la cadena de bloques podría hacer las veces de la fe pública registral, es decir, crear titularidades *in rem* y, además, facilitar su transmisión manteniendo la naturaleza de la titularidad y, por lo tanto, su eficacia *erga omnes*.

7.2. ¿Puede el conjunto formado por los contratos automatizados y la cadena de bloques producir un efecto similar a la fe pública registral, esto es, similar a los efectos que producen el parágrafo 892 del Código civil alemán —BGB— o el artículo 34 de la Ley Hipotecaria española?

Con la finalidad de facilitar la exposición, vamos a prescindir de la necesidad de establecer un procedimiento inmatriculador en la red de la cadena de bloques, lo que, por sí solo, ya es un gran desafío. También prescindiremos de la regulación de los contratos que funcionen al margen de dicha red en relación a los *property rights* inmobiliarios que, una vez inmatriculados, ya consten en los nodos, para centrarnos en la cuestión de si, hipotéticamente, podrían darse a los contratos de finalidad traslativa que figuraran en dichos nodos los mismos efectos que tienen hoy los asientos registrales en un registro de derechos sin intervención de tercero de confianza alguno por ser incompatible —idealmente— con la propia naturaleza de la filosofía que inspira la cadena de bloques.

Con la finalidad de abordar adecuadamente esta cuestión, nos referiremos a ella, en cada una de las fases del proceso adquisitivo en cualquier sistema que cuente con un registro de derechos, si bien brevemente.

1. En la fase de formación del contrato de finalidad traslativa, existe el problema de que dicha tecnología este problema no permite identificar al *verus dominus*. En efecto, un adquirente negocial es solo eso, alguien con un derecho personal sobre la cosa adquirida negocialmente. Para ser dueño se requiere, como primera providencia, que el transmitente lo sea y ningún contrato es suficiente, por sí solo, para acreditarlo. Además, la cadena de bloques ni siquiera permite conocer la identidad de las partes contratantes, así como su capacidad y poder de disposición. Tampoco puede saberse, en consecuencia, si han prestado consentimientos válidos, especialmente si consideramos que los contratos automatizados no están redactados en lenguaje humano sino en *lenguaje máquina*. Para superar este problema debería desaparecer la protección del anonimato, uno de los aspectos identificadores de la tecnología de los bloques encadenados así como acreditar la identidad y capacidad mediante el recurso a *oráculos*[178], lo que implica la negación del principio de autosuficiencia de la cadena de bloques.

No parece que la cadena de bloques pueda asumir, en esta fase del procedimiento, el papel reservado ordinariamente a registros civiles, registros

mercantiles, notarios, *solicitors* y demás *conveyancers.* Debe recordarse, además, que estos, para identificar adecuadamente a los contratantes, ordinariamente recurren a comprobar su carta de identidad, expedida por el Estado.

2. Los contratos referentes a inmuebles normalmente no son breves ni simples. Suelen ser, además, relacionales, es decir, integrados por prestaciones que se llevarán a cabo después del contrato, a lo largo de un periodo de tiempo más o menos largo. Por ello, son difícilmente estandarizables y autoejecutables. Por ejemplo, a lo largo de la vida del contrato —compraventa con precio aplazado, préstamos hipotecarios a largo plazo— pueden variar las circunstancias esenciales y producir la aplicación de la cláusula *rebus sic stantibus.* La ejecución del contrato, su novación o resolución tendría que decidirla también un *oráculo* que, normalmente, será la autoridad judicial.

3. Por lo que se refiere a la función de control legal de la autoridad registral en relación a que dicho acto o contrato se ajusta a Derecho y, por lo tanto, es válido y eficaz así como que se han cumplido todas las normas de Derecho Público que se proyectan sobre la transacción —fiscales, medioambientales, urbanísticas, antiblanqueo, etc.—, igualmente, hoy por hoy, no parece fácilmente automatizable, especialmente en la medida en que dicha función conlleve una cierta labor de ponderación, inevitable en cuanto que se aplican normas abstractas a casos concretos. Esa función solo podría hacerla un *oráculo* técnicamente cualificado e institucionalmente neutral, investido de autoridad pública, como es el registrador, al menos en el estadio actual y previsible en un horizonte razonable de desarrollo de la inteligencia artificial.

El control de legalidad que realiza la autoridad registral en relación con los actos y contratos de finalidad traslativa dentro del procedimiento registral, tiene distinto alcance en los diferentes países, incluso en países con registros de derechos.

En España, por ejemplo, existe un sistema contractual y transmisivo causal, así como un sistema de *numerus apertus* de derechos reales y, finalmente, un registro de derechos. Estas características explican el alcance de la calificación registral en España.

Sin embargo, en Alemania, con un registro de derechos, pero con un sistema transmisivo relativamente abstracto, el alcance del control de legalidad de la autoridad registral no es el mismo sino menor.

En relación con la función del registrador en un sistema Torrens —que conlleva un registro de derechos— Thomas R. afirma:

«Lo que no es comprendido fácilmente es la función de control que desempeña el registrador.

Un sistema registral inmobiliario, especialmente si es de fe pública registral, no es un sistema franco de proceso de datos, basada en el principio nemo dat. *El registrador es el* gatekeeper *que garantiza derechos legales definitivos.*

El registrador tiene la función de asegurar que solo los contratos que se ajustan a la ley, con la debida autorización, son aceptados por el Registro[179]*».*

Las facultades calificadoras del registrador varían en los diferentes países en función de las características del sistema contractual y transmisivo en general, así como del tipo de Registro, el cual es una parte del entero sistema de adquisición.

Esta función es necesaria para fortalecer la seguridad jurídica, y, considerando las características de los diferentes sistemas anteriormente mencionadas, solo puede ser desempeñada por un *oráculo* cualificado, institucionalmente neutral e investido de autoridad pública, como el registrador, al menos en el estado actual y en el horizonte previsible de desarrollo de la inteligencia artificial.

Ni las partes ni sus representantes son capaces de autocontención. Por esta razón, no pueden tomar decisiones que afecten a terceros, como son los asientos registrales, especialmente cuando estamos ante un registro de derechos[180].

7.3. ¿Puede la denominada regla del consenso de la tecnología de los bloques encadenados eliminar la necesidad de supervisión legal por parte del registrador?

En el desempeño de sus funciones los registradores representan los intereses de los terceros ausentes en la transacción. Jerónimo GONZÁLEZ, afirmó, por ello, ya en 1928, que el registrador es «el Fiscal que representa los intereses de los terceros ausentes»[181].

Si, por definición, en un escenario de plataforma única de bloques encadenados como sistema único de contratación y transmisión, todas las transacciones son públicas e inmodificables, y quienes no estén de acuerdo pueden oponerse porque consideran vulnerados sus derechos, entonces puede alegarse que en ese escenario no habría ausentes indefensos y, por lo tanto, no haría falta nadie que los representara. ¿Es así? En nuestra opinión, no y a demostrar esta afirmación están destinados los argumentos que siguen.

7.3.1. Consenso y cadena de bloques

7.3.1.1. El significado del consenso en el ecosistema de la cadena de bloques

El término consenso en el ecosistema de la cadena de bloques surge inicialmente con referencia exclusiva a las operaciones con *Bitcoin*, es decir, a las operaciones con un activo que solamente existe en la red, no fuera de la misma, puesto que es una criptomoneda. En este contexto, consenso sig-

nifica que existe confianza entre los participantes en la red en que los libros inventarios —*ledgers*—, son precisos y consistentes[182] o, más exactamente, en su contenido, es decir, que el contenido del *ledger* refleja los actos que han tenido lugar dentro del mismo.

El principal problema con el que se encuentra una criptomoneda consiste en que puede ser replicada y, por tanto, transmitida a diferentes individuos, pagando, así, con unas mismas monedas, diferentes adquisiciones —«doble gasto»—. Los bloques encadenados hacen que sea difícil conseguirlo porque es un listado con todas las unidades de *Bitcoin* con sus respectivos dueños, de modo que cuando un *bitcoin* cambia de manos, el *ledger* es reescrito para reflejar la transacción[183].

El acuerdo en que este mecanismo es confiable para evitar estos fraudes es a lo que se refiere el término consenso en el contexto de *bitcoin.*

Debe observarse que no se identifica a los contratantes sino solamente a los *avatares* que contratan o, más exactamente, a sus direcciones electrónicas —las cuales pueden pertenecer o no a los contratantes o, incluso, pueden pertenecer a una misma persona— así como a las criptomonedas y sus movimientos dentro de la red, único lugar donde pueden moverse porque solo tienen existencia virtual, estando controlados igualmente sus mecanismos de creación y su número máximo. La cadena de bloques permite, así, controlar los movimientos de *Bitcoin* o de otras criptomonedas. La huella de estos movimientos es, teóricamente, imborrable e inmodificable y, además, es pública, en el sentido de que la pueden ver todos los nodos de la red. La cadena de bloques, sin embargo, no controla ningún aspecto legal, el cual le es completamente ajeno porque, idealmente, solo se rige por la *lex criptographica.*

Uno de los desafíos más serios con el que se encuentra el sistema es, por lo tanto, el de evitar que haya cuentas falsas[184]. Para ello, la cadena de bloques usa dos instrumentos: uno criptográfico y otro basado en la teoría de juegos.

El mecanismo criptográfico es el de clave pública y privada —como el usado por la firma electrónica—. Todo usuario tiene dos claves: una clave pública para encriptar los mensajes y otra privada para desencriptarlos. Puede compartir su clave pública sin que ello implique que pueda ser descubierta su clave privada, y, por tanto, desencriptar el mensaje. Expuesto de un modo elemental, la firma electrónica y el encriptado de un mensaje funciona del siguiente modo[185]: 1.— El remitente firma el mensaje electrónico que quiere enviar usando su clave privada, creando así un *hash* único. 2.— Se encripta el mensaje usando la clave pública del destinatario y se envía el mensaje a dicho destinatario, el cual lo desencripta usando su clave privada. 3.— El destinatario usa la clave pública del remitente para inspeccionar el *hash*. Ello le permite ver que el mensaje solo ha podido ser

firmado con la clave privada del remitente y que el mensaje es exactamente el que el remitente firmó.

La cadena de bloques es, como sabemos, una especie de Libro Inventario digital que registra cada cambio en la propiedad de cada *Bitcoin*, verificando cada transacción, usando un método similar al de la firma electrónica. El hecho de que cada transacción gravada es una firma digital asociada a una dirección electrónica significa que todos pueden visualizar cada movimiento de cada *Bitcoin* y que dichos movimientos —*teóricamente*— no pueden ser alterados.

El otro mecanismo, basado en la teoría de juegos, tiende a ajustar incentivos, de modo que no sea rentable no cooperar o, si se prefiere, intentar engañar al sistema y aprovecharse del mismo defraudando la confianza depositada por los demás participantes en la seguridad del mismo.

Merece la pena resaltar que, así como la cadena de bloques, de hecho, no usa ninguna nueva tecnología electrónica, sino que las combina con un objetivo determinado, sin embargo, sí es novedoso que use, además de tecnología electrónica, el ajuste de incentivos de todos los participantes para asegurar el buen funcionamiento de la red, lo que muestra la importancia de combinar adecuadamente tecnología electrónica e institucional para conseguir los resultados deseados.

Mediante la utilización de la técnica criptográfica, descrita resumidamente con anterioridad, puede probarse que solamente el poseedor de la clave privada pertinente puede haber enviado el mensaje también pertinente.

Como ya hemos expuesto, para reforzar la confianza, la cadena de bloques introduce unos actores especialmente relevantes, los denominados mineros, de modo que, como sostiene Werbach K., sustituyen la confianza en el comportamiento honesto de cada uno de los agentes que usan *Bitcoin* por la confianza en los mineros, los cuales son responsables, entre otros menesteres, de verificar las transacciones[186], verificaciones que se limitan a los aspectos que exponemos a continuación.

Los mineros verifican grupos de transacciones que se agrupan en bloques y, los más diligentes, obtienen una recompensa en *bitcoins*. Puede haber mineros deshonestos pero, para que el sistema funcione, basta con que la mayoría no lo sea[187], pues, en el caso de que se detecte una doble disposición, el sistema opta por la rama de la cadena que sea más larga, es decir, que esté integrada por más bloques. Este hecho, también recibe la denominación de consenso. Esto no significa, sin embargo, que el sistema cuente con el consentimiento del primer adquirente ni que lo proteja.

Para desincentivar que los mineros sean deshonestos en la verificación de transacciones, la tecnología de la cadena de bloques impone a los mineros, como condición para poder obtener la recompense en *bitcoins*, que resuelvan unos enigmas criptográficos, los cuales les permiten obtener el

hash que identifica a cada bloque[188]. Para obtenerlo, un minero necesita invertir en capacidad computacional, lo que implica un gasto considerable que, hipotéticamente, desincentiva un comportamiento engañoso porque los costes de engañar —supuestamente— serían mayores que los beneficios[189].

7.3.1.2. El alcance del consenso en el sistema transmisivo de la cadena de bloques

Expuesto lo anterior, nos hallamos en condiciones de delimitar el alcance del término consenso cuando lo utilizamos en el ecosistema de la cadena de bloques, lo que es necesario porque su uso puede inducir fácilmente a error, ya que sugiere que en el *iter* transmisivo regido por los bloques encadenados y, por lo tanto, por la *lex criptographica,* existen consentimientos explícitos o implícitos de todos los posibles afectados, es decir, de todos los sometidos a la misma jurisdicción o soberanía y que, sin dicho consentimiento, la transacción no es posible. Y eso, sencillamente, no es cierto[190].

Como hemos expuesto, la tecnología de la cadena de bloques no puede identificar a los contratantes físicos. En Internet contratan sus avatares digitales y la cadena de bloques no puede identificar al contratante físico ni, por tanto, establecer correspondencia alguna con su avatar digital. Es más, para los entusiastas de la tecnología de los bloques encadenados, una de las principales ventajas del sistema es, precisamente, que les permite ocultar su identidad real, por lo que resulta especialmente atractivo para todos quienes quieren realizar transacciones sorteando las limitaciones legales.

En segundo lugar, tanto en la versión tradicional del protocolo, que únicamente permite transferir criptomonedas —v.gr.: *Bitcoin*— como en versiones más desarrolladas, que permiten intercambiar criptomonedas por cosas o servicios, v.gr.: *Ethereum*—, la expresión consenso, no se refiere a que exista un acuerdo explícito entre todos los potenciales afectados, sino solamente a la realización de unas comprobaciones —teóricas— muy limitadas.

En efecto, cuando se habla del consenso en relación a *Bitcoin,* este término no se refiere más que a las denominadas *validaciones* —comprobaciones— que se realizan de cada transacción por el resto de nodos de la red. Es necesario subrayar que estas validaciones se circunscriben a comprobar que la cuenta desde la que transfiere un número determinado de *bitcoins* existe y tiene, al menos, esa cantidad, así como la coincidencia de las firmas y la existencia de la cuenta de destino. Pero no se extienden más allá. Así, no se extienden a los elementos esenciales del contrato, que pueden ser determinantes de su nulidad como, por ejemplo, la efectiva identidad del ordenante —que quien ordenó dicha transacción era, efectivamente,

el dueño de la cuenta— ni a que, aun siéndolo, el consentimiento ha sido libremente prestado, a la licitud del pago, etc.

En el caso de *Ethereum*, al igual que en el caso de *bitcoin,* se comprueba que los avatares —no los contratantes físicos— han suscrito un contrato y, después, el resto de nodos verifican la coincidencia de las firmas, que están todos los consentimientos —de los avatares, no de los contratantes físicos— definidos en el contrato autoejecutable, que los eventos previstos se han producido o no y que se han ejecutado las consecuencias previstas para cada caso, que es a lo que alcanza el consenso de los nodos que realizan estas verificaciones.

Eso es lo que cubre la denominada regla del consenso de la tecnología de los bloques encadenados.

Si, por ejemplo, deseamos adquirir un activo inmobiliario, la tecnología de la cadena de bloques no es suficiente para garantizar, por si sola, ni la existencia de tal activo ni la exactitud de sus linderos. Para ello, necesitaría acudir a *oráculos*, sean agrimensores, topógrafos, catastros o profesionales e instituciones semejantes[191].

7.3.2. El presunto consenso en el caso de doble venta y la solución fork choice

No obstante, es frecuente afirmar que, en el caso de «doble gasto», el protocolo de los bloques encadenados resuelve el conflicto a través del denominado *consenso.*

El «doble gasto» puede ser una expresión adecuada para referirse a una doble disposición de *bitcoins* con diferentes personas. En el caso de que la doble disposición no sea de una criptomoneda sino de la titularidad de un activo que existe físicamente fuera de la red de bloques encadenados —v.gr.: una casa— creemos que sería más apropiado utilizar expresiones como «doble venta» o «doble disposición». En todo caso, procederemos a analizar si, en el caso de doble venta, el protocolo de los bloques encadenados lo resuelve mediante el denominado *consenso*.

En primer lugar, como se ha expuesto reiteradamente, la cadena de bloques no puede identificar a los contratantes físicos. En Internet contratan sus avatares digitales y *blockchain* no puede identificar al contratante físico ni, por tanto, establecer correspondencia alguna con su avatar digital.

En segundo lugar, tanto en la versión tradicional del protocolo, que únicamente permite transferir criptomonedas virtuales —v.gr.*: Bitcoin*—, como en versiones más desarrolladas, que permiten intercambiar criptomonedas virtuales por cosas o servicios, v.gr.: *Ethereum*—, cuando se habla de consenso, se refiere a unas comprobaciones —teóricas— muy limitadas, como hemos expuesto.

Además, no basta con ello. Como sabemos, la validez y eficacia de un contrato exige la concurrencia de unos elementos esenciales determinantes de su validez o nulidad, así como de su eficacia o ineficacia, a los que el protocolo no se extiende ni se puede extender.

Sin embargo, es un lugar común afirmar que la cadena de bloques es un sistema público y distribuido sin, supuestamente, intermediarios. En esta situación y teniendo en cuenta el diseño general del sistema, las transacciones son comunicadas progresivamente de un nodo a otro, pero el protocolo no puede asegurar que el orden en el cual un nodo recibe una transacción es el mismo orden en el que fue enviada.

Debido a las diferencias de velocidad en la propagación a través de la red, habrá nodos que recibirán la transacción posterior antes que la enviada anteriormente —y considerarán inválida la recibida en segundo lugar— y viceversa, resultando de ello una falta de acuerdo acerca de qué transacción debe considerarse válida[192].

La cadena de bloques es, simplemente, el instrumento para resolver este tipo de problemas, pues no son más que instrumentos para ordenar las transacciones.

Sin embargo, esta cuestión adquiere una mayor complejidad cuando la cadena de bloques se bifurca en ramas y, sobre todo, si, al mismo tiempo, se producen situaciones de doble disposición.

Las ramas son una consecuencia del funcionamiento del sistema y se producen solo cuando, una vez que un minero ha minado un bloque y lo difunde por la red de nodos —para que estos lo confirmen y lo incorporen a su copia de la cadena como último bloque— y antes de que este bloque llegue a todos los nodos de la red, otro minero —al que no le ha llegado todavía aquel bloque minado— consigue minar otro bloque diferente y, a su vez, lo difunde por la red como nuevo bloque de la cadena.

Cuando ambos bloques, se difundan por todos los nodos, estos verán que en los dos se hace referencia al mismo bloque como bloque anterior a ellos en la cadena de bloques lo que provoca la creación de dos ramas. Si hubiese más de dos bloques que se hubiesen minado en la forma expuesta habrá tantas ramas como bloques minados en estas condiciones, las cuales subsistirán hasta que todas, salvo una de ellas, sean anuladas.

Por otro lado, en caso de doble, triple, etc. disposición el sistema garantiza que solo una de las transacciones será considerada como válida —aunque no tiene por qué ser la primera que se haya efectuado— mediante las confirmaciones de las transacciones.

Así, una vez que se realizan las transacciones, estas pasan al *pool* de transacciones pendientes de confirmar para que los mineros las integren en nuevos bloques. De esta forma, si en dicho *pool* se encuentran varias transacciones —por simplificar, supongamos que son solo dos— que se

han realizado con las mismas monedas —doble gasto—, se pueden dar las siguientes situaciones:

— Que una de las transacciones se incluya en un bloque minado que se integre definitivamente en la cadena de bloques mientras que la otra permanece en el *pool* porque ningún otro minero la ha seleccionado para formar parte de un bloque antes de que aquel se haya integrado en la cadena. En este caso, cuando esta transacción no confirmada llegue a ser elegida y verificada por un minero para integrarla en un nuevo bloque verá que las monedas que utiliza son las mismas que las de una transacción ya integrada en la cadena y será rechazada.

— Que una de las transacciones se incluya en un bloque minado, pero antes de que este se integre definitivamente en la cadena de bloques —por no haber llegado a todos los nodos— otro minero mina un bloque diferente en el que se ha incluido la otra transacción. En este caso, cada transacción formará parte de bloques distintos que darán lugar a ramas diferentes de la cadena y ambas subsistirán como válidas hasta que una rama, por ser más corta que la otra, sea anulada, con lo que todas las transacciones que formaban parte de los bloques de la rama corta volverán al *pool* de transacciones pendientes, y cuando la transacción de este *pool* que integraba el doble gasto —junto con la que permanece en la cadena de bloques por formar, esta, parte de la rama larga— vuelva a ser seleccionada por un minero para integrarla en un nuevo bloque y sea verificada por este, se dará cuenta que utiliza las mismas monedas que otra transacción que ya forma parte de la cadena y, por tanto, será rechazada.

De esta forma, la regla utilizada para establecer qué transacción es la preferente es la denominada *fork choice*, conforme a la cual, en el caso de una bifurcación, los mineros deben optar siempre por la rama más larga, es decir, la que tenga mayor número de bloques confirmados, medidos en términos de capacidad computacional requerida para validarlos. La transacción incluida en esta rama será la que prevalezca, aun cuando fuera posterior[193]. Ello implica que las transacciones incluidas en bloques que integran las ramas más cortas y que estaban ya confirmadas, dejan de estarlo.

Se afirma que con esta regla se preserva el consenso a través de la red porque lo que acuerda una mayoría se presume válido porque se presume que quienes controlan la mayoría de capacidad computacional en la red actúan de acuerdo con el protocolo[194]. De acuerdo con la *lex criptographica,* por tanto, gana aquel cuya transacción haya quedado incluida en el bloque más largo.

Es más, se presume que aquellos que tienen mayor capacidad de poder computacional en la red actúan de acuerdo con las reglas del protocolo[195]. Es lo que se denomina la «versión consenso de la verdad —*consensus versión*

of the truth—[196]» y es una consecuencia inevitable del carácter estrictamente descentralizado de la cadena de bloques y la ausencia —teórica— de cualquier tipo de autoridad central. Así como en el mundo previo a la cadena de bloques, existían servidores centrales que controlaban y validaban la información, en el ecosistema de la cadena de bloques, esa labor —a menudo de alcance global— la realizan nodos descentralizados, que alcanzan un consenso mediante la aplicación de un protocolo, sin intervención de ningún tercero.

7.3.3. La regla fork choice *no significa consenso sino indefensión.*

Es necesario llamar la atención sobre el hecho de que, tanto en la versión tradicional del protocolo, la que se usa para *bitcoin* por ejemplo, como en versiones posteriores, como, por ejemplo *Ethereum*, el dueño de unas determinadas *bitcoins* o de un determinado bien no tiene mecanismos, dentro de los propios protocolos, para oponerse si alguien las utiliza por él indebidamente. Este hecho, junto con el anonimato que caracteriza los protocolos y la irreversibilidad de las transacciones, una vez comprobadas e incorporadas a la cadena de bloques, le deja totalmente indefenso.

Repele, por ello, denominar *regla de consenso* a una regla en la que A adquiere de B, titular según el protocolo, ve confirmada su adquisición por el mismo y, sin embargo, posteriormente, pierde lo adquirido porque B volvió a disponer a favor de C y esta disposición se transmitió más rápidamente por la red, sin intervenir negligencia alguna por su parte y sin poder hacer nada para evitarlo, salvo una cosa: pagar más a un minero para que dé preferencia a resolver el problema matemático que permita validar el bloque en el que se incluye su transacción y, de ese modo, aumentar las probabilidades de ganar prioridad.

El protocolo de los bloques encadenados, por lo tanto, sí provoca la existencia de terceros indefensos, es decir, de dueños que dejan de serlo sin causa alguna que lo justifique, según nuestra concepción, y sin que puedan hacer nada para evitarlo. Este problema se agrava si consideramos las soluciones dadas a los incidentes DAO de 2016 y *Bitcoin Cash* de 2017, en donde los gobernantes reales de estas redes adoptaron soluciones conforme a sus intereses rompiendo las reglas del protocolo. Ello exige la existencia de una tecnología institucional que lo evite mediante la intervención de un tercero imparcial —Estado— que, en el caso que nos ocupa, es exactamente el papel que desempeña el Registro de la Propiedad.

Estos incidentes evidencian que la cadena de bloques puede fallar y que, cuando falla, no hay prevista ninguna tecnología institucional para resolver estos fallos, lo que no es aceptable. Como afirma ROUBINI:

«La verdad es que los desarrolladores —developers— tienen un poder absoluto para actuar como jueces y como jurado. Cuando algo va mal (….) ellos simplemente cambian el code y «fork» una moneda fallida por otra arbitrariamente, revelando la absoluta falta de confiabilidad de una empresa que no era de fiar desde el principio»[197].

Paras resolver este tipo de problemas se necesita una regla diferente, así como la intervención de una tercera parte imparcial de naturaleza pública con facultades jurisdiccionales, lo cual forma parte de las funciones habituales de registradores y jueces.

7.4. La cuestión de si la *tokenización* conlleva un cambio en la ley de circulación de los bienes inmuebles

GONZÁLEZ-MENESES, M.[198] sostiene que la *tokenización* de los activos con existencia física supone la sustitución de la ley de circulación tradicional de los derechos reales sobre bienes inmuebles y su sustitución por una nueva ley circulatoria caracterizada por la legitimación exclusivamente criptográfica.

En nuestra opinión, como resulta de lo hasta aquí expuesto, *la tokenización* de un activo inmobiliario no conlleva dicha sustitución. Nada impide que los agentes económicos se transmitan inmuebles mediante *tokens*, pero dichas transmisiones, como veremos, solo podrían transmitir titularidades negociales —y, por tanto, protegidas solo por una regla de responsabilidad—, pero no titularidades *in rem*, protegidas, por tanto, por una regla de propiedad, a diferencia de lo que sucede cuando se transmiten bienes inmuebles siguiendo la ley de circulación registral de los mismos. Los párrafos que siguen están destinados a justificar dicha afirmación.

Del mismo modo que la letra de cambio es una tecnología jurídica que resolvió los problemas que planteaba el mecanismo civil de la cesión de créditos para la circulación del crédito y cuya construcción conceptual —añadimos nosotros— permitió el desarrollo de los títulos valores, los cuales, posteriormente, han experimentado un proceso de desincorporación mediante su electronificación[199], la *tokenización* de inmuebles, según el mismo autor, consistiría en la incorporación del derecho de propiedad sobre un concreto inmueble —identificado mediante un identificador unívoco— a un determinado *token,* de manera que la circulación de este determinase la transmisión a todos los efectos de la propiedad del mismo.

Así, este inmueble *tokenizado* pertenecería a una determinada dirección de usuario, es decir, a una clave pública de encriptación, y para su transmisión irreversible a otra dirección de usuario, sería suficiente la aplicación de una clave privada —que podría realizarse desde un teléfono móvil y, por

tanto, sin necesidad de escritura pública ni de inscripción en el Registro de la Propiedad previa calificación—. Cualquier titularidad registral, una vez *tokenizada*, podría transmitirse de ese modo, es decir, extrarregistralmente, del mismo modo que sucede hoy con la titularidad sobre una hipoteca cambiaria o sobre un título del mercado hipotecario —v.gr. cédulas o bonos hipotecarios[200]—.

Prescindiremos de la exposición y análisis de las modificaciones legales e institucionales que serían necesarias para un cambio de ley de circulación de este alcance, para centrarnos en el análisis de su posibilidad y, en su caso, conveniencia[201].

La inscripción en un registro de derechos es, con las debidas matizaciones, el equivalente a una letra de cambio inmobiliaria[202], con su régimen civil de circulación específico. Al igual que la letra de cambio sustituye el régimen de circulación de la cesión de créditos por el cambiario, la incorporación de los derechos de propiedad sobre bienes inmuebles al folio registral implica una modificación sustancial del régimen de circulación de la propiedad inscrita en relación a la no inscrita, sustituyendo el régimen de circulación civil —artículo 609 del Código civil— por el de circulación registral —artículo 609 del Código civil y artículo 34 de la Ley Hipotecaria—.

Como consecuencia de dicho cambio, en las respectivas leyes de circulación, en ambos casos se producen efectos similares:

1. En la transmisión por endoso, al tenedor no le afectan las excepciones que deriven del negocio causal o subyacente, siempre que se trate de un poseedor regular —con buena fe— del documento cambiario —artículo 1170 del Código civil y artículos 19 y 20 de la Ley 19/1985, de 16 de julio, Cambiaria y del Cheque, en adelante LCCh— y sea una persona distinta de la otra parte del contrato subyacente, pues la denominada *abstracción cambiaria* solo opera *inter tertios*, no *inter partes* —como todo el Derecho de la seguridad del tráfico en nuestro sistema jurídico—.

2. Similarmente, en la transmisión registral mediante un acto de mercado —es decir, a título oneroso y de buena fe—, el cumplimiento de todos sus requisitos —*ex* artículos 609 del Código civil y 34 de la Ley Hipotecaria— conlleva que al adquirente no le afectan las excepciones causales que deriven de actos o negocios jurídicos anteriores al suyo referentes al mismo bien inmueble, ni se le antepongan cargas que no figuren inscritas. Al igual que en el caso anterior, la abstracción formal o procesal de los actos o negocios jurídicos anteriores —equivalentes al negocio jurídico subyacente en relación a la letra— solo opera *inter tertios*, como consecuencia de lo dispuesto por el artículo 33 de la Ley Hipotecaria —*deferred indefeseability*— no *inter partes* —*inmediate indefeseability*— a diferencia de lo que sucede en algunos sistemas Torrens.

Al igual que la inoponibilidad de excepciones *inter tertios* derivadas del negocio jurídico subyacente recibe la denominación, en el ámbito cambiario, de abstracción cambiaria, a la inoponibilidad de excepciones *ex iure tertii*, es decir, derivadas de actos o negocios jurídicos anteriores referentes al mismo bien, en el ámbito registral, se la debe denominar *abstracción registral*[203].

Entre la transmisión cambiaria y la registral existen, sin embargo, algunas diferencias importantes a los efectos que nos ocupan:

1. En el endoso, la letra pasa de mano en mano y se transmite el derecho de crédito mediante la transmisión de la letra que lo incorpora —Confer.: artículo 17 LCCh—. En la transmisión registral no se transmite físicamente el folio registral —custodiado por el registrador—, sino que requiere el procedimiento civil de transmisión de los derechos reales —artículo 609 del Código civil— formalizado en escritura pública —por exigencia del artículo 3 de la Ley Hipotecaria—, actuando como transferente el titular registral con poder de disposición y exigiendo al adquirente la inscripción de su adquisición negocial —artículo 34 de la Ley Hipotecaria—.

2. La letra de cambio incorpora un derecho de crédito consistente en exigir del aceptante el pago de una cantidad de dinero en una fecha determinada en los términos que resulta del tenor literal de la letra. Se trata de un derecho de crédito simple. El folio registral, diversamente, incorpora titularidades sobre derechos reales inmobiliarios de contenido variable y complejo, así como causas de ineficacia de los actos y negocios jurídicos de los que derivan dichas titularidades y que pueden frustrar la adquisición por el adquirente del titular registral, pero sin que ello pueda sorprenderle, salvo en los casos en que opere una excepción a la fe pública registral, en cuyo caso, la sorpresa será solo relativa, porque tales excepciones deben ser establecidas por ley.

3. Debido a esas diferencias, la letra de cambio es un título valor de literalidad completa porque la descripción del derecho incorporado es suficiente para delimitarlo en relación a los adquirentes mediante actos de tráfico[204]. La inscripción registral, sin embargo, es un título valor de literalidad incompleta porque la descripción del derecho incorporado al asiento registral no es suficiente para delimitarlo en relación a los adquirentes mediante actos de tráfico, pese a lo dispuesto por el artículo 38 de la Ley Hipotecaria, ni en cuanto a la delimitación física — v.gr.: artículo 9 de la Ley Hipotecaria tras ser modificado por la Ley 13/2015 de Reforma de la Ley Hipotecaria aprobada por Decreto de 8 de febrero de 1946 y del texto refundido de la Ley de Catastro Inmobiliario, aprobado por Real Decreto Legislativo 1/2004, de 5 de marzo, lo que ordinariamente exige recurrir al Catastro — ni en cuanto a la delimitación jurídica —debido v.gr.: a las excepciones a la fe pública registral—.

4. La transmisión de la letra es un acto enteramente privado. La transmisión registral también, pero con intervención pública porque el acto o negocio de finalidad traslativa requiere documentación publica —artículo 3 de la Ley Hipotecaria— e inscripción registral —artículo 34 de la Ley Hipotecaria— y esta requiere superar la calificación registral, esto es, el test de legalidad a cargo del registrador —artículo 18 de la Ley Hipotecaria—.

Es precisamente esta última característica de la ley de circulación registral, especialmente la necesidad de solicitar y obtener del Estado, a través del Registro de la Propiedad, el reconocimiento de la titularidad negocial para, una vez reconocida, atribuir al adquirente negocial una titularidad *in rem* a través de la inscripción, la que presenta mayores inconvenientes para que la *tokenización* de activos inmobiliarios pueda imponer una nueva ley de circulación de bienes inmuebles basada exclusivamente en la legitimación criptográfica, en sustitución de la ley de circulación registral. Dicha ley de circulación criptográfica podría existir, pero solo podría atribuir titularidades negociales, como toda adquisición inmobiliaria realizada *ex* artículo 609 del Código civil, prescindiendo del Registro de la Propiedad.

Para entenderlo, es preciso entender el fundamento de que la ley de circulación registral de bienes inmuebles condensada en el artículo 34 de la Ley Hipotecaria —complementado esencialmente por los artículos 32, 33 y 38 de la Ley Hipotecaria y 608, 609 y 1537 del Código civil— exige la intervención pública concretada en la necesidad de adquirir de un titular registral con poder de disposición, y obtener la inscripción registral del derecho adquirido negocialmente.

Tal fundamento hay que buscarlo en el significado de la inscripción en un registro de derechos o de tráfico como el nuestro.

La inscripción es una declaración del poder público sobre la identidad del propietario o titular del derecho real y sobre la extensión de su derecho, una declaración que no es definitiva, pero que puede ser impugnada, si bien con nulas posibilidades de éxito si el titular según la inscripción reúne los requisitos legalmente exigidos —artículo 34 de la Ley Hipotecaria— para ser protegido[205]. Suministra al mercado el titular del *ius disponendi* así como el derecho del que puede disponer, por lo que la inscripción deviene en un insumo prácticamente incuestionable para el juez y, por lo tanto, para el mercado. No puede afectarlo, por tanto, ninguna causa de ineficacia de actos o contratos anteriores referentes al mismo inmueble, si no constan inscritas o, constando, no tienen alcance real por no estar protegidas por una *actio in rem*. Ello explica por qué la ley de circulación registral exige que se adquiera de un titular registral —es decir, de un titular reconocido por el Estado como tal—, con *ius disponendi*.

Pero mientras un adquirente negocial no obtenga la inscripción registral de su adquisición, esto es, una declaración por parte del Estado que lo re-

conozca como titular *in rem*, no es propiamente tal sino un titular negocial. Mientras no inscriba su adquisición, su transmitente —esto es, el titular registral— sigue siendo el titular reconocido por el Estado *erga omnes*, con todos los riesgos que ello implica para el adquirente.

Para acceder a la inscripción, el Estado, a través del Registro de la Propiedad, examina la legalidad formal y sustantiva del proceso adquisitivo[206]. No solo la examina desde la perspectiva del Derecho Privado, sino también desde la del Derecho Público involucrado en la transacción —fiscal, agrario o urbanístico, medioambiental, anti blanqueo, etc.—, pues una de las características de la propiedad sobre la tierra y, en general, de los derechos reales inmobiliarios, es el alto grado de intervención pública que existe en relación a los mismos. Los humanos estamos destinados a compartir la superficie terrestre entre un número creciente de habitantes, lo que implica escasez creciente y, por tanto, mayor intervención pública. Como sostiene DE SOTO[207], la propiedad requiere un consenso acerca de cómo los recursos deben ser poseídos, utilizados e intercambiados, consenso que forma parte de la esencia del Derecho de propiedad. Si el Estado respaldara a quienes se apropian de activos inmobiliarios sin respetar los cauces y requisitos legales necesarios para su adquisición existe el riesgo de que quiebre tal consenso.

La circulación digital de un *token* inmobiliario sería, en ese escenario, idéntica a la de una criptomoneda, pero, a diferencia de la criptomoneda, un activo inmobiliario *tokenizado* no es una unidad digitalizada del valor económico de las cosas, sin existencia extradigital, sino todo lo contrario: un activo con existencia extradigital representado por un *token* digital, lo que plantea los problemas de interacción *on-chain- off-chain* a los que nos hemos referido. No es tampoco un *token* representativo de un derecho de crédito simple incorporado al *token* sino de la titularidad obligacional incorporada a un *token*, pero sobre un derecho real inmobiliario.

Se correría el riesgo de que el activo inmobiliario representado por el *token* no existiese, o se hubiese *tokenizado* más veces en diferentes plataformas *blockchain.* Para solventar este segundo problema habría que proceder a la *tokenización* del activo inmobiliario inscrito, —o no inscrito, pero a través de un procedimiento inmatriculador en este caso— hacerlo en forma auténtica e incorporarlo a una plataforma *blockchain* que debería ser única en cada jurisdicción.

A partir de ese momento, se iniciaría un tráfico anónimo del inmueble, que circularía mediante el simple conocimiento de una clave, eludiendo la normativa de Derecho Privado aplicable a los actos y contratos de finalidad traslativa y, además, el Derecho Público aplicable —fiscal, medioambiental, urbanístico, etc.—. Como subraya GONZÁLEZ MENESES[208], y, en el mismo sentido SIEIRA GIL, J. y CAMPUZANO GÓMEZ-ACEBO, J.[209], ello

tendría una consecuencia de extraordinaria relevancia jurídica. En la medida en la que de un *token* solo puede disponer un sujeto que conoce la clave privada vinculada a la clave pública que ha recibido una transacción anterior del mismo *token,* no es posible que una autoridad pública de cualquier tipo, ordene una transferencia del *token* a un destino determinado sin contar con la voluntad del titular en cuestión, por lo que, técnicamente, la *tokenización* de un activo lo sustrae del ámbito de la responsabilidad patrimonial de su titular y lo hace incoercible.

Por ello, un mero acto privado de creación, transmisión, modificación o extinción de titularidades inmobiliarias, incorporadas o no a *tokens* solo puede tener, en su caso, efectos estrictamente obligacionales *inter privatos.*

VIII. LA PREFERENCIA POR LA CONFIANZA EN TERCEROS PARA PROTEGER LA INTEGRIDAD JURÍDICA DE NUESTROS DERECHOS

A todo ello hay que añadir que la libertad individual exige un precio en términos de responsabilidad personal que no todos están dispuestos a pagar. En este sentido, afirma ARRUÑADA que los individuos:

«…conociendo sus propias debilidades, a menudo confían más y prefieren confiar en soluciones centralizadas, basadas en agentes de custodia privados y públicos.

Esta preferencia por confiar en terceros más que en sí mismos impone una restricción particularmente grave a las aplicaciones en el ámbito de la propiedad porque la naturaleza universal de la propiedad requiere que se apliquen las mismas reglas a todos los titulares de los derechos sobre cada bien. En un hipotético sistema de propiedad plenamente descentralizado, todas las personas deberíamos estar otorgando o negando nuestro consentimiento a todo tipo de transacciones que puedan afectar a nuestros derechos de propiedad. En consecuencia, nos convertiríamos en los únicos custodios no solo de nuestras claves criptográficas (para obtener el aviso y otorgar el consentimiento) sino también para proteger la integridad legal de nuestros derechos»[210].

No todo el mundo está dispuesto a asumir esa responsabilidad porque no siempre es sencillo defender la integridad jurídica de nuestros derechos y, además, porque las partes, cuando contratan, pueden confabularse no solo para perjudicar derechos concretos de personas individualmente identificables sino bienes públicos —y, por tanto, derechos de terceros difusos— definidos y protegidos por normas imperativas y prohibitivas no conocidas en muchas ocasiones por los ciudadanos no expertos en Derecho. Adicio-

nalmente, ello requeriría una atención permanente a cada transacción que se hiciera en la red, lo que exigiría dedicar un tiempo del que normalmente el ciudadano común carece.

De hecho, la solución que propone la cadena de bloques equivale a decir, en el ámbito de los Registros de la Propiedad: (1) Los Registros de la Propiedad son públicos. En consecuencia, toda transacción registrada sin oposición de ninguno de los titulares inscritos es válida y efectiva; (2) En caso de doble venta, no prevalece el adquirente que inscribe en primer lugar su adquisición, aunque sea el segundo adquirente contractual si es de buena fe e inscribe con anterioridad. Prevalece el adquirente que obtiene la mayoría de votos de los propietarios inscritos, incluso contra el consentimiento del propietario inscrito que ha sido privado de su titularidad.

No parece que una solución de este tipo pueda ser legalmente aceptable porque resulta de circunstancias que escapan totalmente del control del dueño, así como de los adquirentes.

Por último, hay que tener en cuenta que, en un mundo crecientemente especializado, la supervisión legal también necesita estar crecientemente especializada.

IX. CONTRATOS AUTOMATIZADOS, CADENA DE BLOQUES Y REGISTROS DE DOCUMENTOS

Para tratar del alcance de la cadena de bloques en relación a los registros de documentos, es preciso hacer referencia a algunas de las características esenciales de los mismos.

Lo primero que conviene destacar es que este tipo de registros no realiza pronunciamientos sobre titularidades sino que se limita a ordenar los documentos que contienen actos y contratos de finalidad traslativa por el orden de su recepción en el Registro, fijando como fecha del documento frente a terceros no la que figura en el propio documento sino la de su recepción por el Registro de la Propiedad, vedando que los documentos no publicados, aunque sean de fecha anterior, sean oponibles frente a los publicados, aunque sean de fecha posterior. Hasta hace poco, en Francia, la *inoponibilidad* operaba aun cuando un segundo adquirente contractual conociese la existencia de una transacción anterior no publicada.

Hay que tener en cuenta, por último, que todo registro de derechos es también, parcialmente, un registro de documentos, en la medida en que una de sus funciones consiste en asignar prioridades, haciendo inoponibles los documentos no publicados frente a los publicados en los mismos términos que lo hace un registro de documentos —v.gr.: documento presentado en

el Libro Diario, con asiento de presentación en vigor, antes de inscribirse el derecho real de que se trate—.

En una primera aproximación, parece que el alcance de la cadena de bloques en relación a este tipo de registros será mayor que en relación a un registro de documentos. Así, por ejemplo, ARRUÑADA sostiene que[211] es concebible que un registro de escrituras pueda ser reemplazado por un sistema automático para datar los contratos privados y preservar sus contenidos, si las partes en dichos contratos privados no pueden manipular ambas funciones una vez que hayan firmado.

Precisa que, obviamente, esta misma conclusión se aplicaría a la parte de registro de documentos que tienen todos los registros de derechos.

Ciertamente, es concebible, pero, hoy por hoy, no parece realizable. Al menos teóricamente, no sería manipulable el contenido de los contratos formados digitalmente dentro de una red de bloques encadenados, pero, en el caso de que el transmitente dispusiera simultánea o inmediatamente después a favor de un tercero, se plantearía un grave problema. La solución legal a esta situación es que se publica el documento que primeramente acceda al Registro. Sin embargo[212], si se aplicase a los registros el protocolo seguido en las cadenas de bloques, ante una presentación sucesiva con relación a una misma finca, los presentantes no podrían conocer con qué rango o prioridad se van a inscribir sus derechos, pudiendo ocurrir que el derecho constituido y presentado en último lugar se inscriba con preferencia al presentado en primer lugar, dado que por una mera cuestión aleatoria —el minado de bloques— o monetaria —el último presentante pagó una comisión superior a los demás— se minó antes el bloque en el que se incluyó la última transacción y todavía podría ser peor, si un derecho inicialmente inscrito, posteriormente se «desinscribe» por encontrarse en una rama corta[213].

Ello implica que el principio de seguridad jurídica no sería posible en el protocolo de la cadena de bloques. No parece que una solución de este tipo fuera legalmente admisible, por ser, además, ajena a la diligencia desplegada por los adquirentes, al ser consecuencia de circunstancias que escapan a su control.

Es más, en este punto, no hay que olvidar que la estructura de incentivos de los mineros estimula la producción de comportamientos perversos, lo que demuestra, que, pese a las pretensiones, los incentivos de los diferentes intervinientes en la cadena no están alineados. En efecto, estos no solo cobran en términos de *bitcoins* por la solución de problemas matemáticos, sino que, además, cobran comisiones de las partes. Aunque, hoy por hoy, no son obligatorias para confirmar las transacciones, sí lo son para ganar prioridad para ello[214], lo que podría ser utilizado por un segundo adquirente para conseguir un tratamiento prioritario.

No obstante, al ser ambas transacciones públicas, podrían evitarse las consecuencias de las segundas disposiciones haciendo que un oráculo pudiera decidir que se admite solo la primera transacción anulando las que integren la cadena que derive de la realizada en segundo lugar. Y parece que quien estaría en mejor disposición para desempeñar esta función oracular sería el registrador, debido a su posición de neutralidad.

Una solución de este tipo, sin embargo, sería la demostración de que la tecnología de los bloques encadenados no podría sustituir a un registro de documentos para la asignación de prioridades. Tampoco, por lo tanto, a un registro de derechos en esa parte de su función.

X. CONCLUSIONES

Bitcoin y *Blockchain* emergieron en el entorno libertario como instrumentos para liberarse de las políticas de los bancos centrales durante la pasada crisis financiera y de los Estados, permitiendo que los individuos pudieran operar con sus propias monedas. Posteriormente, la tecnología de la cadena de bloques, junto con los contratos automatizados, pretenden emerger como tecnologías que se bastan a sí mismas para garantizar unas transacciones y unas titularidades seguras, sin necesidad de intervención alguna por parte del Estado.

Sin embargo, la cadena de bloques no es un sistema transaccional persona a persona porque necesita la intervención de terceros, como los mineros, y, si opera con los contratos autoejecutables, necesita recurrir a oráculos en un amplio número de escenarios. Ciertamente, desde un punto de vista libertario, si esos terceros son individuos privados, en lugar del Estado, entonces no son propiamente terceros, lo cual es una peligrosa fantasía si de lo que se trata es de proteger las titularidades y facilitar las transacciones simultáneamente.

Tanto si opera en el protocolo *Bitcoin* como en el protocolo *Ethereum,* la cadena de bloques no puede evitar recurrir a intermediarios. De hecho, puede afirmarse que la cadena de bloques no prescinde de intermediarios, sino que sustituye unos operadores por otros. Más concretamente, aspira a sustituir al Estado por intermediarios privados bajo el argumento de ser una tecnología honesta e infalible. Como hemos visto, esta no deja de ser una afirmación pretenciosa.

La cadena de bloques no es un servicio gratuito, sino que su uso tiene un coste.

En el caso del *Bitcoin*, suele afirmarse que las comisiones son menores que las bancarias. Esto es cierto actualmente porque los mineros obtienen sus ingresos hallando el *hash* del bloque, pero, en el futuro, su fuente de

ingresos serán las comisiones, por lo que estas muy probablemente se encarecerán, tal y como preveía M. HEARN[215].

En el caso del protocolo *Ethereum*, el cual desempeña su función junto con los contratos autoejecutables, necesita recurrir a oráculos, en un amplio número de escenarios, como hemos visto. Los servicios de estos oráculos no son gratuitos y no hay razones para suponer que impliquen costes menores que los de los sistemas institucionales.

La cadena de bloques no es un sistema autónomo, descentralizado e inmodificable, tal y como han demostrado los incidentes *DAO* y *Bitcoin Cash* y otros. Como expusimos anteriormente, esos hechos demostraron la existencia de poderes centrales a los que nadie había elegido, sin ninguna autoridad legal, pero con un innegable capacidad de imposición que usaron en su propio beneficio. Estos poderes centrales demostraron tener capacidad de imposición suficiente para borrar y cambiar el, supuestamente, inmodificable contenido de los bloques.

Esos poderes son privados y sus decisiones no afectan al Estado. Prefieren el principio según el cual *code is law* en lugar de la sujeción de la *lex cripotographica* a la Ley.

Sin embargo, si admitimos que la tecnología de la cadena de bloques no es necesariamente una tecnología libertaria y autosuficiente y admitimos que puede ser una tecnología organizada y gestionada por terceros, especialmente por el Estado, en este caso, la cadena de bloques puede desempeñar una importante función de apoyo a los sistemas transaccionales inmobiliarios, por ejemplo, contribuyendo al almacén de documentos, conservación de archivos o realización de notificaciones.

Al mismo tiempo, el progreso de la inteligencia artificial permitirá el desarrollo de contratos autoejecutables más complejos y la utilidad de estas tecnologías tendrá un mayor alcance, sin que hoy podamos predecir cuál puede llegar a ser.

En todo caso, la cadena de bloques es una tecnología y, como tal, abre nuevas posibilidades, permite hacer cosas nuevas, pero no debemos olvidar que no nos dice qué cosas deberíamos hacer. En otras palabras, las tecnologías son instrumentos de poder y, en consecuencia, obedecen a la lógica del poder, esto es, a su utilización en beneficio de quien ostenta dicho poder.

Por ello, las tecnologías deben ser utilizadas dentro de un marco institucional que garantice adecuadamente el equilibrio de los diferentes intereses en juego.

BIBLIOGRAFÍA

Autores

ARRUÑADA, B., *Blockchains Struggle to Deliver Impersonal Exchange,* Minn. J.L. SCI & Tech., Vol. 19.1, 1918, 78.

BEDNAREK, A., https://www.securityevaluators.com/casestudies/ethercombing,

BOGOST, I., *Cryptocurrency Might Be a Path to Authoritarianism*, ATLANTIC (30 de mayo de 2017), https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543 [https://perma.cc/UU6F-7MFW].

BRENNAN, G. *The Impact of e-Conveyancing on Title Registration. A Risk Assessment*., Ed. Springer, 2015.

CALABRESI, G. y MELAMED, D. A., Property Rules, Liability Rules and Inaliena bility: One View of The Cathedral, published in 1972 by *Harvard Law Review*

CHAUM, D., https/www.chaum.com/publications/Security_Wthout_Identification.html.

CIPHERTRACE, *Fourth Quarter Cryptocurrency Anti-Money Laundering Report 2018 Q4*, Enero de 2019. Puede obtenerse en: https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf, visitado el 1 de mayo de 2019.

COHEN, P.J., *Set Theory and the Continuum Hypothesis*, 1966, W.A. Bejamin, Nueva York.

COOK COUNTY RECORDER OF DEEDS, *Blockchain Pilot Program Final Report* 32-34 (2017), http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot- Program-for-web.pdf-

DANS, E. En el prólogo a la traducción española de TAPSCOTT, D. y *TAPSCOTT, A. La Revolución Blockchain, Ed. Deusto.*

DE OTTO, I., *Estudios sobre el poder judicial,* Ed.: Ministerio de Justicia, 1989. DEUSTO, 2017, 15.

DE FILIPPI, P. y WRIGHT, A., *Blockchain and the Law*. *The Rule of Code,* Harvard University Press, 2018.

DENNETT, D. C., *Brainchildren: essays on designing minds*, 1998, Harmondsworth, Penguin Books.

DE SOTO, H., *El misterio del capital*, Ed.: Península, 2001.

DÍEZ-PICAZO Í PONCE DE LEÓN, L., *Fundamentos de Derecho Civil Patrimonial*, T.III, Ed.: Thomson-Civitas, Cizur Menor, 2008.

DOUCEUR, J.R., *The Sybil Attack*, *in Peer-to-peer-systems*.

EIZAGUIRRE, J.M., *Revista de Derecho Bancario y Bursátil*, núm. 57, 1995.

EYAL, I.& GÜN SIRER, E., *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, *en* Financial Cryptography & Data Security (2014).

FELIÚ REY, J., *Smart Contract:* Concepto, ecosistema y principales cuestiones de Derecho privado, *La Ley Mercantil,* núm. 47, 2018.

FRANZÉN, T., *Gödel's Theorem. An Incomplete Guide to its Use and Abuse*, 2005, A.K. Peters, Wellesley, Mass.

GALLEGO FERNÁNDEZ, L.A., *Cadenas de bloques y Registros de derechos, Revista Crítica de Derecho Inmobiliario*, núm. 765.

GARTNER.COM,: Hype Cycle for Emerging Technologies, https://blogs.gartner.

GONZÁLEZ J., *Principios Hipotecarios*, Asociación de Registradores de la Propiedad, Madrid, 1931.

GONZÁLEZ-MENESES, M., *La «tokenización» de inmuebles ¿economía colaborativa o mercantilización extrema?,* en *La protección del consumidor en la vivienda colaborativa*, Muñiz Espada E., Ed.: La Ley, Wolters Kluwer, Madrid, 2019.

GÓMEZ GÁLLIGO, J., *El Registro de la Propiedad y los nuevos retos de blockchain,* en Muñiz Espada E., (dir.) Ed.: Wolters Kluwer, 2019

HOFSTADTER, D., *Gödel, Escher, Bach: An Eternal Golden Braid*, 2006, Basic Books, New York, Holden, C., Science vol. 311.

ILLESCAS ORTIZ, R.(Dir.), *Electronificación de los títulos valores*, Ed.: Civitas, Thomson Reuters., 2018.

KAY, J., *El dinero de los demás*, Barcelona, RBA Ed. 2017.

GÖDEL, K., *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik, December 1931.

KAAL y CALCATERRA, *Crypto transaction dispute resolution*, The Business Laywer, Spring 2018.

KOSBA, A. MILLER, A., SHI E WEN, Z. y PAPAMANTHOU Ch.'Hawk: - *Preserving Smart Contracts, The Blockchain Model of Criptography and Privacy-,* en IEEE Sympsium on Securiry and Privacy (SP), 2016,, ed. : Locasto M., Shmatikov, V. Y Erlingsson U., Puscataway, NJ:IEEE,2016, 839-858.

LANDO, O. *Principios de Derecho Europeo de los contratos. Partes I y II revisadas*, preparadas por la Comisión de Derecho Europeo de los Contratos Presidente: Profesor Ole Lando. http://campus.usal.es/~derinfo/Material/LegOblContr/PECL%20I+II.pdf

LEGERÉN-MOLINA, A. Retos jurídicos que plantea la cadena de bloques, en *Revista de Derecho Civil*, vol. VI, núm. 1 (enero-marzo de 2019).

Leyes Hipotecarias de España: Fuentes y Evolución, T. I., Vol. II, Ed.: Castalia, 1989.

LUCAS, J. R., *Minds, machines and Gödel*, Philosophy 36, April-July 1961, 112-127. Reimpreso en: Kenneth, Malcolm y Frederick, James, *The Modelling of Mind*, Computers and Intelligence, 1963, Notre Dame Press.

MAY Th., *Crypto Anarchy and Virtual Communities* (1994), http//groups.csail.mit.edu/mac/clases/6.805/articles/crypto/cypherpunks/may-virtual-comm.html.

— *Crypto Anarchist Manifesto*, https://www.activism.net/cypherpunk/crypto-anarchy.html.

MÉNDEZ GONZÁLEZ, F. P., La inscripción como título valor o el valor de la inscripción como título, en *RCDI*, núm. 703, septiembre-octubre de 2007,

— *De la publicidad contractual a la titulación registral. El largo proceso hacia el Registro de la Propiedad*, Thomson, Civitas, 2008.

— Estado, Propiedad, Mercado, en *Revista Crítica de Derecho Inmobiliario*, núm. 708, 2008.

— *Fundamentación económica del derecho de propiedad privada e ingeniería jurídica del intercambio impersonal*. Ed.: Thomson Reuters, 2011.

— Derechos reales y titularidades reales, en *RCDI*, núm. 736.

— *La función de la fe pública registral en la transmisión de bienes inmuebles. Un estudio del sistema español con referencia al sistema alemán*., Ed.: Tirant Lo Blanch, 2017, 45-49.

MMC Ventures, *The State of AI: Divergence*, 2019. Puede verse en: https://www.mmcventures.com/wp-content/uploads/2019/02/The-State-of-AI-2019-Divergence.pdf, visitado el 1 de mayo de 2019.

NAKAMOTO SATOSHI, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (octubre de 2008). http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

NORTH. D.C, *Instituciones, cambio institucional y desempeño económico*. Ed. Fondo de Cultura Económica, Mexico D.F., 1995.

MERRILL, T.W. y SMITH, H.E, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle, The Yale Law Journal*, octubre, 4, 2000, Vol. 110-1.

MOLINA BALAGUER, F., *Informe correspondiente a la Segunda Conferencia Anual de Ibrea -International Blockchain Real Estate Association-* Nueva York, 10 de octubre de 2017. *Paper* citado con autorización del autor.

MORAVEC, H.P. *Mind Children: The Future of Robot and Human Intelligence*, Harvard University Press, 1990.

NAGEL, E. and NEWMAN, J., *Gödel's Proof.*, 1959, reeditado en 2001, New York University Press, New York.

NARAYANA, B. y otros, *Bitcoin and Cryptocurrency* Technologies 2 (2016) *(«Optimists claim that Bitcoin will fundamentally alter payments, economics, and even politics around the world*»).

O'NEIL, Cathy, *Weapons of Math Destruction*, 2017, Penguin Books. Traducción española: *Armas de Destrucción Matemática*, 2018, Capitán Swing Libros S.L.

PAU PEDRÓN A., *Panorama del sistema inmobiliario alemán,* en *La publicidad registral*, Ed.: Colegio de Registradores de la Propiedad y Mercantiles de España, Madrid, 2001.

PENROSE R., *The Emperor's New Mind. Concerning Computers, Minds, and The Laws of Physics*, 1989, Oxford University Press.

— *Shadows of the Mind: A Search for the Missing Science of Consciousness*, 1994, Oxford University Press.

— *The Large, the Small and the Human Mind*, 1997, Cambridge University Press.

ROJO M.ª. Isabel, *Blockchain: Fundamentos de la cadena de bloques*. Ed.: Ra-Ma, 2018.

ROSENFELD, M., *Analysis of hashrate- based double-spending*, 2014. https://arxiv.org/pdf/1402.2009v1, visitado el 1 de mayo de 2019.

ROTHSTEIN, A., *The End of Money. The story of bitcoin, cryptocurrencies and the blockchain revolution,* New Scientist, 2017.

ROUBINI, N. https://www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10, visited November 16, 2018.

SAVAUX, E. *El nuevo Derecho francés de obligaciones y contratos*.https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-C-2016-30071500741

SCHNEIDER, V., et al., *Blockchain: Putting Theory into Practice*, Goldman Sachs Equity Res. 4 (May 24, 2016), https://www.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1 [https://perma.cc/93FJ-EEDW]

SEARLE, John. R., *Minds, Brains, and Programs.* Behavioral and Brain Sciences 3, 1980.

SHOHAM YOAV, RAYMOND PERRAULT, ERIK BRYNJOLFSSON, JACK CLARK, JAMES MANYIKA, JUAN CARLOS NIEBLES, TERAH LYONS, JOHN ETCHEMENDY, BARBARA GROSZ and ZOE BAUER, *The AI Index 2018 Annual Report*, AI Index Steering Committee, Human-Centered AI Initiative, Stanford University, Stanford, CA, December 2018. Puede verse en: http://cdn.aiindex.org/2018/AI%20Index%202018%20Annual%20Report.pdf

SPARKES, M, *The Coming Digital Anarchy*, Telegraph (9 de junio de 2014), http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html [https://perma.cc/T4LT-BXRK].

SURDEN, H. *Computable Contracts*, *U. C. Davis L. Rev.*, vol. 46, 2012

SZABO, N., *Smart Contract: Building Blocks for Digital Markets,* 1996, Literature/LOTwinterschool2006 /szabo.best.vwh.net/smart_contracts_2.html

— *Formalizing and Securing Relationships on Public Networks,* /firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First

TAPSCOTT, D. and TAPSCOTT, A.,*Blockchain Revolution*, Penguin, N.Y, 2016.

TELIA COMPANY, ChromaWay and Kairos Future, *The Land Registry in the blockchain. A development project with Lantmäteriet (The Swedish Mapping, cadastre and land registration authority)*, July 2016.

THE ECONOMIST, *Not-So-Clever Contracts*, 28 de julio de 2016, http://www.economist.com/news/business/21702758-time-being-least-human-judgment- still-better-bet-cold-hearted [hereinafter *Not-So-Clever Contracts*] («[T]rusted parties, known as oracles, could supply the data to a blockchain[…]»

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27 de septiembre de 2019. https://media.consensys.net/report-the-legal-and-regulatory-framework-of-blockchains-and-smart-contracts-8f397eaf0b1f

THOMAS R., *The New Zealand Experience: The risks and implications of automation*, Ponencia presentada por el autor a la Conferencia que tuvo lugar en Auckland, New Zealand, 29-31 de agosto de 2018.

TUR FAÚNDEZ, C., *Smart Contracts. Análisis jurídico*, Ed.: Reus, Madrid, 2018.

TURING A. *Computing Machinery and Intelligence*, (Mind, New Series, Vol. 59, núm. 236, ocutbre de 1950, Oxford University Press on behalf of the Mind Association)

Visa at a Glance, Visa Inc., junio de 2015.

VILARROIG MOYA, R. y PASTOR SEMPERE, C. (Dir), *Blockchain: Aspectos tecnológicos, empresariales y legales.* Ed.: Thomson Reuters Aranzadi, 2018.

WERBACH, K., *Trust, but Verify: Why the Blockchain Needs the Law*, Berkeley Technology Law, Journal, Vol. 33:487, 489, 2018.

WESTERMAN, H.P., EICKMAN, D., DINGER, W., *Sachenrecht,* 6.ª ed., C.F Müller Juristischer Verlag, Heidelberg, 1988, 100 ss. Wolff-Raiser, en el *Tratado de Derecho Civil*, Enneccerus, Kipp y Wolff, T. III,1.º. Traducción española con anotaciones de Pérez González y Alguer, Barcelona, 1971.

WILLIAMSON, O.E, *The Economic Institutions of Capitalism: Firms, Markets and Relational Contracting,* 1985.

WOLPERT, D.H., Macready, W.G., *No Free Lunch Theorems for Optimization*, 1997, IEEE Transactions on Evolutionary Computation Vol. 1, núm. 1.

Páginas web

https://www.forbes.com/sites/oliversmith/2019/01/31/blockchain-startups-showed-no-signs-of-life-in-2018/#4169b5f3463e
https://www.axios.com/corporate-america-blockchain-bitcoin-fervor-over-fb13b-c5c-81fd-4c12-8a7b-07ad107817ca.html
https://www.bloomberg.com/news/articles/2019-02-03/crypto-is-over-paris-fintech-summit-returns-to-disrupting-banks
https://www.forbes.com/sites/jpreissler/2019/03/20/cboe-pulls-out-of-the-bitcoin-futures-market
https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html
https://www.businessinsider.com/ico-south-korea-bans-icos-2017-9?IR
https://www.elmundo.es/tecnologia/2019/04/09/5caca98cfdddff7d5b8b46f2.html
https://blogs.gartner.com/smarterwithgartner/files/2018/08/PR_490866_5_Trends_in_the_Emerging_Tech_Hype_Cycle_2018_Hype_Cycle.png
https://arxiv.org/abs/1904.08653
https://www.theverge.com/2017/11/2/16597276/google-ai-image-attacks-adversarial-turtle-rifle-3d-printed
https://www.labsix.org/physical-objects-that-fool-neural-nets
https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf,
https://towardsdatascience.com/is-artificial-intelligence-racist-and-other-concerns-817fa60d75e9, o
https://www.elmundo.es/motor/2019/03/26/5c99277421efa07c438b4632.html
https://www.nature.com/articles/d41586-018-05707-8
https://tech.co/news/sexist-ai-doomed-reflect-worst-2018-10
https://smoda.elpais.com/feminismo/algoritmos-machistas
http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212
https://www.bloomberg.com/news/articles/2019-09-08/how-the-algorithms-running-your-life-are-biased-quicktake
https://civio.es/tu-derecho-a-saber/2019/05/16/la-aplicacion-del-bono-social-del-gobierno-niega-la-ayuda-a-personas-que-tienen-derecho-a-ella
https://civio.es/novedades/2019/07/02/que-se-nos-regule-mediante-codigo-fuente-o-algoritmos-secretos-es-algo-que-jamas-debe-permitirse-en-un-estado-social-democratico-y-de-derecho
https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor
https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25152&LangID=E
https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing,
https://www.technologyreview.es/s/11138/por-que-necesitamos-expertos-que-estudien-como-se-comporta-la-ia

https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016R0679
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2901-1-1.
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2576-1-1
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143325
https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system
https://www.bloomberg.com/news/articles/2019-04-26/major-tech-firms-come-out-against-police-use-of-ai-algorithms
https://venturebeat.com/2019/04/26/partnership-on-ai-algorithms-arent-ready-to-automate-pretrial-bail-hearings
https://steemit.com/ethereum/@chris4210/an-open-letter-to-the-dao-and-the-ethereum-community
https://www.greaterzuricharea.com/en/news/chainsecurity-saves-ethereum-security-breach
https://arxiv.org/pdf/1802.06038.pdf
https://blog.comae.io/the-280m-ethereums-bug-f28e5de43513
https://mashable.com/2017/07/20/ethereum-hackers-theft-32-million/?europe=true
www.bloomberg.com/news/articles/2019-01-08/ethereum-classic-movements-halted-by-coinbase-on-signs-of-attack
https://www.securityevaluators.com/casestudies/ethercombing
https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&iframe=true
https://www.blockchain.com/es/pools
https://www.blockchain.com/charts/avg-block-size?timespan=all
https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.ewfepr21j
https://www.blockchain.com/charts/transaction-fees?timespan=all
https://transactionfee.info/charts/payments/segwit
https://www.blockchain.com/charts/avg-block-size?timespan=all
https://tradeblock.com/blog/the-51-attack-what-bitcoin-can-learn-from-alt-coin-experiments
https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions
https://www.ccn.com/1-1-million-malicious-miner-exploits-verge-network-for-seven-figure-payday,
https://www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again,
https://blog.theabacus.io/the-verge-hack-explained-7942f63a3017
https://blog.theabacus.io/lets-do-the-time-warp-again-the-verge-hack-part-deux-c6396ab36ecb
https://toshitimes.com/zencash-falls-victim-to-a-51-attack-with-550000-worth-of-tokens-stolen
https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack
https://breakermag.com/51-attack-vertcoins-strength-fatal-flaw

https://www.bloomberg.com/news/articles/2019-01-08/ethereum-classic-movements-halted-by-coinbase-on-signs-of-attack
https://coinmarketcap.com
https://blog.sia.tech/fundamentals-of-proof-of-work-beaa68093d2b
https://www.bloombergquint.com/business/bitcoin-is-worth-less-than-the-cost-to-mine-it-jpmorgan-says#gs.FhYdn8AW
https://bitcoin.es/noticias/jp-morgan-bitcoin-btc-no-es-rentable
https://www.crypto51.app
https://coinmarketcap.com/all/views/all
https://blockstream.com/technology/#sidechains
https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem
https://www.coindesk.com/quadrigacx-officially-enters-bankruptcy-with-millions-still-missing
https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.ewfepr21j

NOTAS

[1] https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-blockchain-and-distributed-ledger-technologies. Sobre aspectos generales de la tecnología blockchain, puede verse, Vilarroig Moya R. Y Pastor Sempere C. (Dir), *Blockchain: Aspectos Tecnológicos, Empresariales y Legales*, Ed.: Thomson Reuters Aranzadi, 2018, especialmente, 36-40.

[2] Tecnologías del Libro Distribuido, DLT, por sus siglas en inglés, derivadas de *Distributed Ledger Technologies*.

[3] TAPSCOTT D. and TAPSCOTT A. *Blockchain Revolution*, Penguin, N.Y, 2016, 16.

[4] ROUBINI, N. https://www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10.

[5] SPARKES, M. *The Coming Digital Anarchy*, TELEGRAPH (9 de junio de 2014), http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html, [https://perma.cc/T4LT-BXRK].

[6] BOGOST I, *Cryptocurrency Might Be a Path to Authoritarianism*, ATLANTIC (30 de mayo de 2017), https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/ [https://perma.cc/UU6F-7MFW].

[7] MAY Th. escribió en 1988 su *Crypto Anarchist Manifesto* en el que ya anunciaba que la aparición de Internet y los avances en la criptografía de clave pública y privada posibilitaría que los individuos y los grupos se comunicaran e interactuaran de una manera más anónima, pudiendo negociar contratos electrónicos de modo que no se pudiera conocer el verdadero nombre o identidad legal del otro. Ver https://www.activism.net/cypherpunk/crypto-anarchy.html.

[8] CHAUM, D., ya advirtió que las nuevas tecnologías de computación podrían privar a los individuos de controlar su propia información, la cual podría ser utilizada por gobiernos y corporaciones para inferir modos de vida y hábitos. La manera de contrarrestar este peligro era la de desarrollar técnicas criptográficas susceptibles de uso masivo que permitieran enviar mensajes con seguridad. Ver: https://www.chaum.com/publications/Security_Wthout_Identification.html.

[9] Véase: https://www.forbes.com/sites/oliversmith/2019/01/31/blockchain-startups-showed-no-signs-of-life-in-2018/#4169b5f3463e.

[10] Véase: https://www.axios.com/corporate-america-blockchain-bitcoin-fervor-over-fb13bc5c-81fd-4c12-8a7b-07ad107817ca.html.

[11] Véase: https://www.bloomberg.com/news/articles/2019-02-03/crypto-is-over-paris-fintech-summit-returns-to-disrupting-banks.

[12] Véase: https://www.forbes.com/sites/jpreissler/2019/03/20/cboe-pulls-out-of-the-bitcoin-futures-market.

[13] Véase: https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html.

[14] Véase: https://www.businessinsider.com/ico-south-korea-bans-icos-2017-9?IR=T.

[15] Vease: https://www.elmundo.es/tecnologia/2019/04/09/5caca98cfdddff7d5b8b46f2.html.

[16] Este gráfico forma parte del informe de Gartner: «Hype Cycle for Emerging Technologies», y puede obtenerse en la dirección: https://blogs.gartner.com/smarterwithgartner/files/2018/08/PR_490866_5_Trends_in_the_Emerging_Tech_Hype_Cycle_2018_Hype_Cycle.png.

[17] WERBACH, K., *Trust, but Verify: Why the Blockchain Needs the Law*, Berkeley Technology Law, Journal, Vol. 33:487, 489, 2018.

[18] Véase el Informe de *The European Union Blockchain Observatory and Forum,* denominado *Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27 de septiembre de 2019, 9. https://media.consensys.net/report-the-legal-and-regulatory-framework-of-blockchains-and-smart-contracts-8f397eaf0b1f.

[19] DANS, E. En el prólogo a la traducción española de TAPSCOTT D. y TAPSCOTT A.: *La Revolución Blockchain*, Ed. Deusto, 2017, 15.

[20] Una exposición de la aparición progresiva de las diferentes tecnologías que, comenzando en 1950, acaban configurando *blockchain* puede verse en DE FILIPPI P. y WRIGHT A, *Blockchain and the Law*. *The Rule of Code*, Harvard University Press, 2018, especialmente 13-32.

[21] Ver MAY, T., *Crypto Anarchy and Virtual Communities* (1994), http//groups.csail.mit.edu/mac/clases/6.805/articles/crypto/cypherpunks/may-virtual-comm.html.

[22] Sobre bitcoin y criptodivisas alternativas hay una ingente bibliografía. Puede consultarse VILARROIG MOYA R. y PASTOR SEMPERE C. (Dir), *Blockchain: Aspectos Tecnológicos, Empresariales y Legales*, Ed.: Thomson Reuters Aranzadi, 2018, especialmente, 40 a 176. También ROJO M.ª. Isabel, *Blockchain, Fundamentos de la cadena de bloques*, Ed.: Ra-Ma, 2018, especialmente, 71-95.

[23] SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (octubre de 2008). http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

[24] Por ello, en este caso, el negocio jurídico no sería de intercambio de cosa por dinero, sino de cosa por cosa, es decir, una permuta. En este sentido también GÓMEZ GÁLLIGO, J. *El Registro de la Propiedad y los nuevos desafíos del blockchain*, en *La protección del consumidor en la vivienda colaborativa*, MUÑIZ ESPADA, E., Ed.: La Ley, Wolters Kluwer, Madrid, 2019, 574.

[25] DE FILIPPI, P. y WRIGHT, A., *Blockchain and the Law. The Rule of Code*, Harvard University Press, 2018, especialmente 27 a 29. Vease también VILARROIG MOYA, R. y PASTOR SEMPERE, C. (Dir.), *Blockchain: Aspectos Tecnológicos, Empresariales y Legales*, Ed.: Thomson Reuters Aranzadi, 2018, especialmente, 66 a 71. También ROJO M.ª. Isabel, *Blockchain, Fundamentos de la cadena de bloques*, Ed.: Ra-Ma, 2018, especialmente, 97-159.

[26] Véase KAY, J. *El dinero de los demás*, Barcelona, RBA Ed. 2017, 181-185.

[27] Así, por ejemplo, DE FILIPPI y WRIGHT, A. se refieren a que *blockchain* sirve de apoyo a registros resilientes, transparentes, no repudiables y resistentes a las trampas, destacando que las cadenas de bloques están almacenando documentos —*records*— de un modo secuencial, ordenados temporalmente, por partes conocidas y autenticadas, los cuales son accesibles —y auditables— por cualquiera con conexión a Internet. Dichos

documentos incluyen títulos inmobiliarios —*title to land*—. *Op. cit.* 46. En realidad, se refieren a archivos, pero no a sistemas registrales en un sentido técnico. En cuanto a que se trata de documentos con partes conocidas y autenticadas, es una afirmación que puede considerarse correcta si se trata de documentos autenticados mediante firma electrónica o mediante intervención humana —notario—, pero no si se trata de transacciones realizadas mediante *blockchain*, ya que en esta tecnología contratan dos direcciones electrónicas, sin que pueda acreditar la identidad de las personas que se hallan tras ellas. Goldman Sachs estima que la aplicación de las tecnologías del libro o inventario —*ledger*— distribuido —DLT, por sus siglas en inglés— a los sistemas de *Title Insurance* en los Estados Unidos podría ahorrar entre dos y cuatro billones de dólares anuales. *Ver* SCHNEIDER V. *et al., Blockchain: Putting Theory into Practice*, Goldman Sachs Equity Res. 4 (May 24, 2016), https://www.scribd.com/doc/313839001/Profiles-in -Innovation-May-24-2016-1 [https://perma.cc/93FJ-EEDW]. Hay que recordar, sin embargo, como hace SCHNEIDER, que el seguro de título es necesario en los Estados Unidos porque tiene un sistema de «*registration by title*» en lugar de «*title by registration*», lo que impide que la registración confiera un título inatacable. TAPSCOTT, D. y TAPSCOTT, A.—*op. cit.*, 42— se refiere a *blockchain* como instrumento que dé seguridad, protección y garantía del derecho a la tierra y a otros bienes que se posean legalmente. Esta afirmación puede interpretarse en el sentido de que *blockchain* actuaría como *enforcer* del sistema legal en lugar de como sustituto del mismo.

[28] WESTERMAN, H.P., EICKMAN, D., DINGER, W., *Sachenrecht,* 6.ª ed., C.F Müller Juristischer Verlag, Heidelberg, 1988, 100 y sigs. WOLFF-RAISER utiliza la expresión *acto estatal*, en Derecho de cosas, en el *Tratado de Derecho Civil*, Enneccerus, Kipp y Wolff, T. III, 1.º. Traducción española con anotaciones de PÉREZ GONZÁLEZ y ALGUER, Barcelona, 1971, 226.

[29] DE OTTO, I. *Estudios sobre el poder judicial,* Ed.: Ministerio de Justicia, 1989. Ciertamente, se trata de una declaración que no es definitiva porque puede ser impugnada, si bien con nulas posibilidades de éxito si el titular según la inscripción reúne los requisitos para ser protegido. Esto es lo que significan los principales efectos o propiedades normativas atribuidas a la inscripción, especialmente la fe pública registral.

[30] THOMAS, R.: A land registration system, especially one which offers indefeasibility, is not a straightforward data-processing system, based on *nemo dat* principles. The Registrar is the gatekeeper granting definitive legal rights, *The New Zealand Experience: The risks and implications of automation*, Ponencia presentada por el autor a la Conferencia que tuvo lugar en Auckland, New Zealand, 29-31 de agosto de 2018.

[31] MÉNDEZ GONZÁLEZ, F. P., *Fundamentación económica del derecho de propiedad privada e ingeniería jurídica del intercambio impersonal*. Ed.: Thomson Reuters, 2011.

[32] *Cook County Recorder of Deeds, Blockchain Pilot Program Final Report,* (2017) 32-34, http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf.

[33] Telia Company, ChromaWay and Kairos Future, *The Land Registry in the blockchain. A development project with Lantmäteriet (The Swedish Mapping, cadastre and land registration authority)*, July 2016.

[34] En concreto el algoritmo utilizado para el cálculo de las huellas de los documentos es el SHA-256 (que también es el más utilizado en el protocolo *Blockchain*). Una descripción de este algoritmo puede encontrarse en: http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf.

[35] Artículos 106 y siguientes de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social: https://boe.es/buscar/doc.php?id=BOE-A-2001-24965.

[36] En este sentido, el Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles de España es prestador de confianza de servicios de certificación para firmas electrónicas y sellados temporales electrónicos cualificados, conforme al Regla-

mento EU núm. 910/2014, de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior: https://webgate.ec.europa.eu/tl-browser/#/tl/ES/11.

[37] Artículo 28.1 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (https://www.boe.es/buscar/act.php?id=BOE-A-2011-11605) y artículos 27.2 y 27.3.a de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565).

[38] Artículo 28.5 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (https://www.boe.es/buscar/act.php?id=BOE-A-2011-11605, visitado el 1 de mayo de 2019) y artículo 27.3.c de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565.

[39] Dado que cualquier carácter diferente —mayúsculas/minúsculas, comas/puntos, etc.— o formato distinto o simplemente un espacio en blanco más o menos entre uno y otro documento, daría lugar a hashes totalmente diferentes, aunque el contenido jurídico de ambos documentos fuese idéntico.

[40] MOLINA BALAGUER, F., *Informe correspondiente a la Segunda Conferencia Anual de Ibrea —International Blockchain Real Estate Association—* Nueva York, 10 de octubre de 2017. *Paper* citado con autorización del autor.

[41] Esta es una cuestión de capital importancia —y que, por ello, trataremos de forma más extensa a lo largo de este artículo—, sobre todo en sistemas registrales de derechos construidos en torno al principio de seguridad jurídica preventiva, como ocurre en el caso español. En este sentido, los diferentes modelos registrales se pueden diferenciar, fundamentalmente, en cuanto al modo y el momento en que se depuran las posibles contradicciones con los derechos de terceros y la legalidad y, desde este punto de vista, los dos principales diseños organizativos que históricamente se han propuesto han sido los registros de depósito de documentos y los registros de derechos.

Los primeros se limitan a datar y conservar pruebas de las escrituras o contratos en las que eventualmente se basarán los tribunales para decidir sobre los derechos en litigio mientras que los registros de derechos van más allá de la mera publicidad de los documentos potencialmente acreditativos de los contratos, ya que garantizan el reconocimiento por el Estado de las titularidades sobre los derechos y los propios derechos. En estos sistemas, los contratos no son traslativos, sino que son contratos con finalidad traslativa y para que esta se produzca efectivamente, es decir, con carácter *erga omnes*, se requiere la inscripción. Para conseguirlo, los documentos han de ser calificados por el registrador, con el fin de detectar posibles ilegalidades, así como cualquier conflicto que pueda perjudicar otros derechos reales. Como consecuencia de todo ello, la información del registro está siempre depurada y es capaz de proporcionar titularidades definitivas e irrevocables, en el sentido de que el tercero de buena fe, que adquiera sobre la base de la información suministrada por el registro, adquiere un derecho real, inatacable.

La superioridad de los registros de derechos, por tanto, es clara en cuanto a la calidad de sus productos ya que, no solo aseguran perfectamente la propiedad del titular, sino que también reducen de forma drástica el coste de las transacciones futuras, proporcionan mejores incentivos para la inversión, abaratan el crédito hipotecario, etc. (Véase, por ejemplo: United Nations Economic Commission for Europe, Study on Key Aspects of Land Registration and Cadastral Legislation, HMLR, Londres, 2000).

Pero para que todos estos beneficios se produzcan no basta, sin embargo, con que las partes se limiten a suscribir un contrato. Al contrario, es necesario verificar que no concurren ninguno de los supuestos que puedan determinar su nulidad o ineficacia y, así, entre otros extremos, habrá de determinarse, no solo que se ha prestado el consentimiento, que quienes lo han prestado son quienes dicen ser, que lo han hecho libre e informadamente, que no se encuentran incapacitados ni tienen sus facultades de dispo-

sición limitadas, que en el momento de dicha prestación los otorgantes estaban en pleno uso de sus facultades (arts. 1261 y sigs. CC) y, en caso de que se actúe por medio de un representante, que este cuente realmente con dicho poder de representación, que no esté revocado y que las facultades que se le han delegado son suficientes para llevar a cabo el negocio jurídico a que se refiere el contrato suscrito (art. 1259 CC), que exista una causa y que esta no sea ilícita o falsa (arts. 1261, 1275 y 1276 CC), que tengan un objeto cierto (art. 1261 CC) etc., sino también que las diferentes circunstancias que conforman dicho negocio jurídico se ajustan a la legalidad y no afectan a los derechos preexistentes de terceros, etc. Ninguna de estas cuestiones se resuelve mediante las cadenas de bloques.

[42] Sobre los intentos de construir una identidad digital basada en *blockchain* dentro de la Administración pública, véase VILARROIG MOYA, R. y PASTOR SEMPERE, C. (Dir.), *Blockchain: Aspectos Tecnológicos, Empresariales y Legales*, Ed.: Thomson Reuters Aranzadi, 2018, especialmente 321 a 336.

[43] Cualquier usuario de la cadena puede tener varios identificadores y usar uno diferente para cada transacción. Igualmente, el sellado de tiempo tampoco identifica quién sea el sujeto concreto que efectúa el registro —quién cierra el bloque— sino la dirección desde la que se realiza. De todas maneras, como sostiene LEGERÉN-MOLINA, debe tenerse presente que, por medio de mecanismos indirectos, existe cierta caracterización de los números identificativos, tanto del emisor como del receptor de cualquier transacción: el seguimiento de las IP o de las cuentas, en su caso, asociadas a las operaciones —por ejemplo, un proveedor, por razones de eficiencia, mantendrá una o pocas direcciones *bitcoin* para cobrar a sus clientes sin cambiarlas de manera habitual—, análisis de tráfico, etc. Ello permite a LEGERÉN-MOLINA afirmar que la cadena de bloques no es «anónima» sino «pseudónima». Véase LEGERÉN-MOLINA, A. Retos jurídicos que plantea la cadena de bloques, en *Revista de Derecho Civil*, vol. VI, núm. 1 (enero-marzo, de 2019), Estudios, 206 y 207.

[44] Véase el Informe de *The European Union Blockchain Observatory and Forum,* denominado *Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27 de septiembre de 2019, 14. https://media.consensys.net/report-the-legal-and-regulatory-framework-of-blockchains-and-smart-contracts-8f397eaf0b1f.

[45] *Ibidem*.

[46] *Ibidem*.

[47] *Ibidem*, 12: «The situation is more complex when it comes to eSignatures and eSeals (signatures of a legal entity as opposed to a natural person)».

[48] El informe *Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27 de septiembre de 2019, anteriormente citado, reconoce la necesidad, en estos casos, de acudir a las «bases de datos de las sociedades o a algún otro oráculo confiable, los cuales necesitan algún tipo de reconocimiento legal» —24—. En el caso de las sociedades mercantiles esa función la cumplen con ventaja los registros mercantiles.

[49] Para apreciar la capacidad de obrar, en nuestro sistema jurídico, también procede la consulta al Registro de la Propiedad, dado lo dispuesto por los artículos 2 de la Ley Hipotecaria y 7 del Reglamento Hipotecario.

[50] No entramos a analizar aquí la cuestión de la denominada forma digital, especialmente en el ámbito de los *smarts contracts,* en donde, como afirma FELIÚ REY, desempeña una función dinámica. Como afirma este autor: «En realidad, un *Smart Contract* sin lenguaje máquina y sin forma de código autoejecutable no ofrece ninguno de los efectos esperados, ni puede integrar información para determinar las prestaciones (p.ej. un precio de cotización o un dato GPS de localización), ni puede ejecutar las prestaciones (p.ej. una transferencia de dinero o una publicación de una información), ni puede automáticamente tampoco aplicar las medidas autoejecutables previstas en caso de incumplimiento (p.ej. transmitir la orden a un dispositivo conectado para que no pueda ponerse en marcha el vehículo, la desactivación de una clave de acceso, o la eliminación de archivos o datos).

En el caso de los *smart contracts*, la falta de forma determinada implicaría que no estuviéramos ante tal figura, no produciendo los efectos que le son propios. Hay un contrato válido, pero no se producen los efectos propios consustanciales a la forma y el lenguaje, independientemente que se puedan obtener por las vías tradicionales». FELIÚ REY, J. «*Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado*», *La Ley Mercantil, núm.* 47, 2018, 11.

[51] The European Union Blockchain Observatory and Forum*, Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27 de septiembre de 2019, 33. https://media.consensys.net/report-the-legal-and-regulatory-framework-of-blockchains-and-smart-contracts-8f397eaf0b1f

[52] Véase MENDEZ GONZÁLEZ, F. P., *Derechos reales y titularidades reales,* en *RCDI*, núm. 736, 797, nota 51.

[53] MERRILL, T.W. y SMITH, H.E, Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, The Yale Law Journal*, 4 de octubre de 2000, Vol. 110-1, 38-42.

[54] MERRILL, T.W y SMITH, H.E, *op. cit.*, 39-40.

[55] Podría objetarse que, en Alemania, por ejemplo, el sistema registral es de encasillado, y, sin embargo, por la vía de las cargas reales, admite una amplia variedad de derechos reales. Según PAU PEDRÓN, la figura de la carga real convierte en ilusorio el sistema de *numerus clausus* en el sistema alemán. Según este autor, la carga real admite los más variados contenidos imaginables. Esta multiplicidad de contenidos de la carga real ha sido característica típica del Derecho medieval: las más variadas figuras —*Dienste, Zehnen, Grundzinsen, Fronden* y otras muchas— se engloban en el concepto de carga real, limitándose el BGB a decir en el parágrafo 1105 que una finca puede ser gravada con prestaciones. PAU PEDRÓN A., *Panorama del sistema inmobiliario alemán,* en *La publicidad registral*, 57. Ed.: Colegio de Registradores de la Propiedad y Mercantiles de España, Madrid, 2001. A las cargas reales se refiere también nuestro Código civil, entre otros, en los artículos 336, 788 o 1086, pero, a nuestro juicio, no son derechos reales de goce, sino mecanismos de garantía para hacer efectivas determinadas obligaciones, normalmente de prestación periódica. Véase DÍEZ-PICAZO Y PONCE DE LEÓN, L. *Fundamentos de Derecho Civil Patrimonial*, T. III, Ed.: Thomson-Civitas, Cizur Menor, 2008, 96-98. Hay que tener en cuenta, además, que en el sistema alemán, el Registro no solo practica inscripciones bajo el sistema de encasillado sino que archiva el documento y que, además, el sistema transmisivo es, al menos relativamente, abstracto, por lo que la transmisión del derecho real carece de conexión con el negocio causal.

[56] GONZÁLEZ-MENESES, M., *La «tokenización» de inmuebles ¿economía colaborativa o mercantilización extrema?,* en *La protección del consumidor en la vivienda colaborativa*, Muñiz Espada E., Ed.: La Ley, Wolters Kluwer, Madrid, 2019, 552.

[57] GONZÁLEZ-MENESES, M., *op. cit.,* 555.

[58] GONZÁLEZ-MENESES, M., *op. cit.* 557.

[59] No obstante, conviene subrayar que, en nuestro país no hay ninguna criptodivisa que tenga la consideración de dinero de curso legal en el sentido del artículo 1170 del Código civil por lo que su utilización para «pagar» la adquisición de un bien inmueble debería tener la consideración de permuta. Sobre los aspectos legales y tributarios de las criptodivisas en nuestro país, véase VILARROIG MOYA, R. y PASTOR SEMPERE C. (Dir.), *Blockchain: Aspectos Tecnológicos, Empresariales y Legales*, Ed.: Thomson Reuters Aranzadi, 2018, especialmente, 191-240.

[60] SZABO, Nick, *Smart Contract: Building Blocks for Digital Markets,* 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006 /szabo.best.vwh.net/smart_contracts_2.html (last acces, November, 26, 2018). Véase también TUR FAÚNDEZ, C., *Smart Contracts. Análisis jurídico*, Ed.: Reus, Madrid, 2018.

[61] SZABO, N. *Formalizing and Securing Relationships on Public Networks,* /firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First.

[62] En este sentido se pronuncia el Informe *Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27 de septiembre de 2019, anteriormente citado, 22.

[63] The Economist, *Not-So-Clever Contracts*, 28 de julio de 2016, http://www.economist.com/news/business/21702758-time-being-least-human-judgment- still-better-bet-cold-hearted [hereinafter *Not-So-Clever Contracts*] («[T]rusted parties, known as oracles, could supply the data to a blockchain[.]».

[64] DE FILIPPI P. y WRIGHT A. *op. cit.,* 83.

[65] Sobre el significado del término consenso en el ecosistema *blockchain* nos extenderemos posteriormente, pues es un término cuyo uso puede inducir a confusión, como veremos.

[66] En nuestro ordenamiento jurídico, el artículo 3.4 de la Ley 59/2003 de 19 de diciembre de Firma Electrónica dispone que «*La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel*». Respecto de la firma electrónica avanzada —de rango menor— el artículo 3.2 solo dice que genera un «*alto nivel de confianza*» pero sin atribuirle un valor probatorio específico. El problema está en que, como señalamos anteriormente, para que la firma electrónica pueda ser calificada como reconocida es necesario que identifique a los firmantes, algo que repele a la filosofía de la tecnología de los bloques encadenados.

[67] MÉNDEZ GONZÁLEZ, F.P., *La función de la fe pública registral en la transmisión de bienes inmuebles. Un estudio del sistema español con referencia al sistema alemán*., Ed.: Tirant Lo Blanch, 2017, 45-49.

[68] Vease SAVAUX, E. *El nuevo Derecho francés de obligaciones y contratos*.https://www.boe.es/publicaciones/anuarios_derecho/abrir_pdf.php?id=ANU-C-2016-30071500741. También *Principios de Derecho Europeo de los contratos. Partes I y II revisadas*, preparadas por la Comisión de Derecho europeo de los contratos. Presidente: Profesor Ole Lando. http://campus.usal.es/~derinfo/Material/LegOblContr/PECL%20I+II.pdf.

[69] FELIÚ REY, J. *Smart Contract:* Concepto, ecosistema y principales cuestiones de Derecho privado*, La Ley Mercantil, núm.* 47, 2018, 18.

[70] Véase LEGERÉN-MOLINA, A. *Retos jurídicos que plantea la cadena de bloques*, en Revista de Derecho Civil, vol. VI, núm. 1 (enero-marzo de 2019), Estudios, 226.

[71] FILIPPI, P. y WRIGHT, A. *Blockchain and the Law*, Harvard University Press, 2018, 77. Véase en el mismo sentido FELIÚ REY, J. *Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado, La Ley Mercantil, núm.* 47, 2018, 8 y sigs. Como afirma este autor, 9: «…debemos advertir que, en el estado actual de la tecnología, el dispositivo, en realidad, no entiende conceptos, sino que ejecuta instrucciones tal y como están programadas. Es decir, cuando presionamos la tecla de impresión, para imprimir un documento, el dispositivo no entiende el concepto de impresión ni la orden, ejecuta sencillamente un protocolo que consigue la finalidad querida, es decir, la obtención en soporte papel de un contenido que estaba en soporte digital. Otro ejemplo algo más sofisticado, en el que ya comenzamos a incorporar nociones de tecnología más avanzada con soluciones de inteligencia artificial, sería el caso de un coche autónomo ante el que se cruza una pelota. Con seguridad, el vehículo se detendrá o aminorará la marcha ante la identificación de un obstáculo, porque así se ha programado antes, pero difícilmente, en el estado actual de la técnica, será capaz, por sí solo, de intuir que, tras la pelota, pueda aparecer corriendo un niño intentando recuperarla». En esta misma línea, SURDEN, H. *Computable Contracts*, *U. C. Davis L. Rev.*, vol. 46, 2012, 633 y sigs., quien afirma que: «(…) *contemporary computer algorithms cannot read or understand even basic written language texts anywhere near the sophistication exhibited by a person of ordinary literacy».*

[72] Véase el Informe de *The European Union Blockchain Observatory and Forum,* denominado *Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27

de septiembre de 2019, 14. https://media.consensys.net/report-the-legal-and-regulatory-framework-of-blockchains-and-smart-contracts-8f397eaf0b1f.

[73] Se refiere a la obra: *Principia Mathematica*, de Alfred North WHITEHEAD y Bertrand RUSSELL, compuesta por tres volúmenes publicados por primera vez, respectivamente, en 1910, 1912 y 1913.

[74] GÖDEL, Kurt, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik, December 1931, vol. 38, 173-198.

[75] Entre los muchos textos de carácter divulgativo acerca de los teoremas de Gödel, su demostración, significado y relación con otras ramas del conocimiento, se pueden citar los siguientes:

– FRANZÉN, T., *Gödel's Theorem. An Incomplete Guide to its Use and Abuse*, 2005, A.K. Peters, Wellesley, Mass.

– HOFSTADTER, D., *Gödel, Escher, Bach: An Eternal Golden Braid*, 2006, Basic Books, New York, Holden, C., Science vol. 311, 317.

– NAGEL, E., and NEWMAN, J., *Gödel's Proof*, 1959, reeditado en 2001, New York University Press, New York.

[76] Los enunciados de estos teoremas establecen: 1.- Cualquier formalización consistente S en la que se puedan efectuar operaciones aritméticas elementales, es incompleta respecto de los enunciados de la aritmética elemental; esto es, hay enunciados cuya verdad o falsedad no se puede demostrar dentro de S. y 2.- Para cualquier formalización consistente S en la que se puedan efectuar operaciones aritméticas elementales, no es posible probar la consistencia de S dentro de S.

El propio Gödel en la introducción de su artículo señalaba que: «*Como es sabido, el progreso de la matemática hacia una exactitud cada vez mayor ha llevado a la formalización de amplias partes de ella, de tal modo que las deducciones pueden llevarse a cabo según unas pocas reglas mecánicas. Los sistemas formales más amplios construidos hasta ahora son el sistema de* Principia Mathematica *(PM) y la teoría de conjuntos de Zermelo-Fraenkel (desarrollada aún más por J. von Neumann).*

Estos dos sistemas son tan amplios que todos los métodos usados hoy día en la matemática pueden ser formalizados en ellos, es decir, pueden ser reducidos a unos pocos axiomas y reglas de inferencia. Resulta por tanto natural la conjetura de que estos axiomas y reglas basten para decidir todas las cuestiones matemáticas que puedan *ser formuladas en dichos sistemas. En lo que sigue se muestra que esto no es así, sino que, por el contrario, en ambos sistemas hay problemas relativamente simples de la teoría de los números naturales que no pueden ser decididos con sus axiomas (y reglas)*».

[77] O en palabras del propio GÖDEL: «*Todos ustedes conocen las famosas palabras de Hilbert sobre que todo matemático está convencido de que para cada pregunta matemática precisamente formulada es posible encontrar una única respuesta y que es exactamente esta convicción el estímulo fundamental del trabajo de investigación matemático. Hilbert mismo estaba tan convencido de esto que aún pensaba que era posible que se diera una demostración matemática de esto, al menos en el dominio de la teoría de los números.*

¿Cómo podemos imaginar que una tal demostración pueda ser obtenida? Para buscarla primero tenemos que analizar el significado del teorema a ser demostrado. Para cada hombre desprejuiciado esto solo puede significar lo siguiente: dada una proposición matemática cualquiera A, existe una demostración para A o para no-A, donde por «demostración» se entiende algo que parta de axiomas evidentes y proceda por inferencias evidentes. Ahora, formulado de esta manera, el problema no es susceptible de tratamiento matemático pues involucra las nociones no-matemáticas de evidencia. Luego lo primero que hay que hacer es explicitar esta noción a través del análisis de las demostraciones matemáticas reales. Si eso se hace —y ha sido hecho por la lógica matemática y por la Teoría de la Demostración de Hilbert— entonces nuestro problema puede ser tratado matemáticamente y la respuesta resulta ser negativa aún en el dominio de la teoría de los números.

Pero es claro que esta respuesta negativa tiene dos significados diferentes: (1) puede significar que el problema en su formulación original tiene una respuesta negativa, o (2) puede significar que algo se perdió en el proceso de transición de la evidencia al formalismo. Es fácil ver que realmente ocurrió lo segundo, puesto que las preguntas de la teoría de los números que son indecidibles en un formalismo dado son siempre decidibles por inferencias evidentes que no son expresables en el formalismo dado. Respecto de la evidencia de estas nuevas inferencias, ellas resultan ser tan evidentes como las del formalismo dado. Luego el resultado es más bien que no es posible formalizar la evidencia matemática aún en el dominio de la teoría de los números, pero la convicción acerca de la cual Hilbert hablaba permanece enteramente inalterada».

[78] COHEN, P.J., *Set Theory and the Continuum Hypothesis*, 1966, W.A. Benjamin, Nueva York.

[79] Esta hipótesis afirma que no hay ningún conjunto cuya cardinalidad —número de elementos o tamaño del conjunto— se halle estrictamente entre la de los números enteros y la de los números reales.

[80] El *Entscheidungsproblem* indaga sobre si, dada una teoría matemática no trivial, es posible diseñar un algoritmo que, dada una proposición cualquiera de esa teoría, nos indique si la misma es verdadera o falsa.

[81] El décimo problema de Hilbert plantea la siguiente pregunta: ¿es posible diseñar un algoritmo que, dada una ecuación diofántica (es decir, una ecuación polinómica de una o varias variables con coeficientes enteros y respecto de la cual se buscan exclusivamente soluciones enteras) indique si admite o no alguna solución?

[82] CHURCH, Alonzo, *An unsolvable problem of elementary number theory*, American Journal of Mathematics, Vol. 58, núm. 2. (April, 1936), 345-363.

[83] TURING, A., *On Computable Numbers with an Application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society, Volume s2-42, Issue 1, 1937, 230-265.

[84] Precisamente, en enero de 2019 se publicó en la revista *Nature*, un artículo en el que también se demuestra que existen problemas que una Inteligencia Artificial, incluso empleando técnicas de *learning,* nunca podrá resolver. Puede verse en la dirección: https://www.nature.com/articles/s42256-018-0002-3. El caso concreto estudiado en este artículo es un problema similar a la hipótesis del continuo de *Cantor*.

[85] Por ejemplo, GÖDEL, tras conocer los resultados de TURING, señaló que: «*No es posible mecanizar el razonamiento matemático, esto es, nunca será posible reemplazar los matemáticos por una máquina, aún si nos confinamos a los problemas de la teoría de números. Hay por supuesto, porciones de las matemáticas que pueden ser completamente mecanizadas y automatizadas; por ejemplo, la geometría elemental es una de ellas, pero la teoría de los números enteros ya no lo es*».

[86] Más adelante se dará una definición más técnica de los oráculos, por ahora basta decir que son servicios de terceros que proporcionan al contrato inteligente información sobre si determinado suceso o evento, contemplado por aquel, se ha producido, o no, para que dicho contrato pueda ejecutar la acción correspondiente.

Imaginemos un contrato inteligente que gestiona una apuesta deportiva, en concreto, el resultado de un concreto partido de la liga de fútbol profesional. En este escenario, por un lado, estarían los sistemas en los que reside y se ejecuta el contrato inteligente y, por otro, aquellos de los que el contrato obtiene el resultado del partido respecto del que se ha realizado la apuesta, por ejemplo, los servicios telemáticos que para ello pueda proporcionar la propia Liga de Fútbol Profesional; estos servicios serían un oráculo del contrato inteligente que gestiona la apuesta.

[87] Ver NARAYANA, B. y otros, *Bitcoin and Cryptocurrency Technologies 2* (2016) (2016) *(«Optimists claim that Bitcoin will fundamentally alter payments, economics, and even politics around the world.»*).

[88] Los títulos denominados «derivados» se denominan así porque su valor *deriva* del de otros títulos. Si los títulos son derechos sobre activos, los derivados son derechos

sobre otros títulos, y su valor depende del precio de esos títulos subyacentes. Una vez creados los derivados, se pueden crear otras capas de derivados y así sucesivamente. El valor de los activos subyacentes a estos contratos derivados es tres veces el valor de todos los activos físicos del mundo. Se trata de títulos comercializables con los que suele practicarse «*trading* de alta frecuencia», a través de ordenadores que constantemente compran y venden valores. Véase KAY, J. *El dinero de los demás*, Barcelona, RBA Ed., 2017, 16.

[89] ARRUÑADA, B., *Blockchains Struggle to Deliver Impersonal Exchange,* Minn. J.L. SCI & Tech., Vol.19.1, 1918, 78.

[90] El concepto de contratos relacionales fue acuñado por Williamson, para referirse a aquellos contratos que son completados por las partes *ex post,* a veces incluso después de haberse perfeccionado el contrato, bien por ser ineficiente hacerlo *ex ante*, o, sencillamente, imposible. Ver WILLIAMSON, O. E, *The Economic Institutions of Capitalism: Firms, Markets and Relational Contracting,* 1985. Como se ha afirmado, muchos contratos —los relacionales— operan más como matrimonios a largo plazo que como relaciones ocasionales breves —Ver KOSBA, A., MILLER, A., SHI, E., WEN, Z., y PAPAMANTHOU, Ch., Hawk: *Preserving Smart Contracts, The Blockchain Model of Ceiptography and Privacy,* en IEEE Sympsium on Securiry and Privacy (SP), 2016,, ed. : Locasto M., Shmatikov, V. y Erlingsson U., Puscataway, NJ:IEEE,2016, 839-858. Pero, incluso, en estos casos, *blockchain* aporta el valor de posibilitar la verificabilidad del contenido de los documentos, como expusimos anteriormente.

[91] YOAV SHOHAM, RAYMOND PERRAULT, ERIK BRYNJOLFSSON, JACK CLARK, JAMES MANYIKA, JUAN CARLOS NIEBLES, TERAH LYONS, JOHN ETCHEMENDY, BARBARA GROSZ and ZOE BAUER, *The AI Index 2018 Annual Report*, AI Index Steering Committee, Human-Centered AI Initiative, Stanford University, Stanford, CA, December 2018. Puede verse en: http://cdn.aiindex.org/2018/AI%20Index%202018%20Annual%20Report.pdf.

[92] MMC Ventures, *The State of AI: Divergence*, 2019. Puede verse en: https://www.mmcventures.com/wp-content/uploads/2019/02/The-State-of-AI-2019-Divergence.pdf.

[93] Así, por ejemplo, las técnicas matemáticas, principalmente de carácter estadístico y de análisis numérico, en las que se fundamentan los algoritmos de aprendizaje y aprendizaje profundo actuales son: el método de mínimos cuadrados (1805), el teorema de Bayes (1812) o las cadenas de Markov (1913).

Posteriormente, en 1950, Alan TURING publica su artículo: *Computing Machinery and Intelligence*, (Mind, New Series, Vol. 59, núm. 236 —octubre de 1950—, 433-460, Oxford University Press on behalf of the Mind Association) en el que se pregunta si las máquinas pueden pensar y propone su: *imitation game, también conocido como* test de Turing, que es un test para determinar si un ordenador es inteligente y que se basa en verificar si una persona comunicándose con él, a través de mensajes tecleados, puede confundirlo o no con otro ser humano (hoy en día, no obstante, existen tests más fuertes como el de Winograd que tiene en cuenta el *sentido común*). Más tarde, en 1951, Marvin Minsky diseña y construye SNARC (Stochastic Neural Analog Reinforcement Computer), la primera red neuronal.

[94] SEARLE, John. R, *Minds, Brains, and Programs*. *Behavioral and Brain Sciences* 3, 1980, 417-457. Existen otras categorizaciones más actuales como la debida a Arend Hintze, que atiende al nivel de competencia, y distingue entre máquinas reactivas, de memoria limitada, conformes con la teoría de la mente y autoconscientes, pero, no obstante, se ha optado por la clasificación de Searle por su carácter más didáctico.

[95] Véase, por ejemplo: Hans P. MORAVEC, *Mind Children: The Future of Robot and Human Intelligence*, Harvard University Press, 1990.

[96] En la siguiente dirección: https://arxiv.org/abs/1904.08653 puede encontrarse un informe que explica como engañar a un sistema de vigilancia con cámaras e IA, mediante la utilización de un simple parche de colores.

[97] Véase, por ejemplo: https://www.theverge.com/2017/11/2/16597276/google-ai-image-attacks-adversarial-turtle-rifle-3d-printed o también: https://www.labsix.org/physical-objects-that-fool-neural-nets.

[98] En la siguiente dirección: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf, puede encontrarse un informe en el que se explica cómo engañar a un sistema de conducción autónoma simplemente colocando tres pegatinas transparentes —no visibles para el ser humano— en el asfalto haciendo que se desvíe, cambie de carril o, incluso, que se dé la vuelta.

[99] PENROSE, R., *The Emperor's New Mind. Concerning Computers, Minds, and The Laws of Physics*, 1989, Oxford University Press.

— PENROSE R., *Shadows of the Mind: A Search for the Missing Science of Consciousness*, 1994, Oxford University Press.

— PENROSE R., *The Large, the Small and the Human Mind*, 1997, Cambridge University Press.

[100] LUCAS, John R., *Minds, machines and Gödel*, Philosophy 36, April-July 1961, págs: 112-127. Reimpreso en: Kenneth, Malcolm y Frederick, James, *The Modelling of Mind*, Computers and Intelligence, 1963, Notre Dame Press, 255.

[101] HOFSTADTER, D., *GÖDEL, Escher, Bach: An Eternal Golden Braid*, 2006, Basic Books, New York, Holden, C., Science vol. 311, 317.

[102] DENNETT, Daniel Clement, *Brainchildren: essays on designing minds*, 1998, Harmondsworth, Penguin Books.

[103] Los números complejos o imaginarios son números que se construyen a partir de las raíces cuadradas de números negativos. Estas raíces, sin embargo, no tienen solución ya que no existe ningún número que, al multiplicarlo por sí mismo, dé, como resultado, un número negativo. El lector interesado puede intentar calcular una raíz cuadrada de este tipo en cualquier calculadora, ordenador, hoja de cálculo, programa, etc., y lo que obtendrá será un mensaje de error. Sin embargo, a pesar de lo anterior, un acto de intuición y creatividad permitió su concepción y desarrollo posterior, constituyendo, hoy en día, una herramienta poderosísima en el ámbito científico.

[104] Ver nota núm. 47.

[105] El experimento de la habitación china trata de poner de manifiesto que el pensamiento no consiste simplemente en la ejecución de un algoritmo, la ausencia de comprensión en estos algoritmos, así como el carácter limitado del test de Turing. El experimento consiste en imaginar a una persona, que no entiende ni habla chino, encerrada en una habitación en la que solo existen dos rendijas. Fuera de la habitación hay un interlocutor que solo habla chino y que no sabe que hay dentro de la habitación cerrada. Por la primera de las rendijas el interlocutor introduce tarjetas con símbolos en chino. El individuo del interior debe entregar, a través de la segunda rendija, respuestas, también en chino, a las tarjetas de entrada que ha recibido, para lo cual cuenta con un manual que le indica qué respuestas puede dar a cada conjunto de caracteres chinos que reciba. Por tanto, la persona encerrada buscando y siguiendo las secuencias del manual, y sin saber chino, podrá proporcionar respuestas correctas.

Ante este escenario cabe preguntarse si el individuo en el interior de la habitación sabe chino o si lo *entiende* el manual o si se puede considerar que el conjunto formado por la habitación, la persona encerrada y el manual, es un sistema que entiende chino. El interlocutor, desde luego, pensará que la habitación es capaz de responderle y, desde este punto de vista, esta superaría el test de Turing con lo que, de acuerdo con este test, estaríamos ante un sistema inteligente. Sin embargo, es claro que ninguno de los elementos que integran dicho sistema, con el que se relaciona el interlocutor, comprende el chino, y, por tanto, aunque el conjunto de aquellos supere el test de Turing, este no confirma que el individuo encerrado efectivamente entienda el chino, por lo que una ejecución correcta de un algoritmo realizada por un autómata u ordenador no constituye un acto de conocimiento ni de comprensión.

[106] WOLPERT, D.H., MACREADY, W.G., *No Free Lunch Theorems for Optimization*, 1997, IEEE Transactions on Evolutionary Computation Vol. 1, núm. 1, 67-82.

[107] Véase, por ejemplo: https://towardsdatascience.com/is-artificial-intelligence-racist-and-other-concerns-817fa60d75e9, o también: https://www.elmundo.es/motor/2019/03/26/5c99277421efa07c438b4632.html.

[108] Véase, por ejemplo: https://www.nature.com/articles/d41586-018-05707-8, o también: https://tech.co/news/sexist-ai-doomed-reflect-worst-2018-10, también: https://smoda.elpais.com/feminismo/algoritmos-machistas o http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 o https://www.bloomberg.com/news/articles/2019-09-08/how-the-algorithms-running-your-life-are-biased-quicktake.

[109] Véase, por ejemplo: https://civio.es/tu-derecho-a-saber/2019/05/16/la-aplicacion-del-bono-social-del-gobierno-niega-la-ayuda-a-personas-que-tienen-derecho-a-ella, o también: https://civio.es/novedades/2019/07/02/que-se-nos-regule-mediante-codigo-fuente-o-algoritmos-secretos-es-algo-que-jamas-debe-permitirse-en-un-estado-social-democratico-y-de-derecho.

[110] Véase, por ejemplo: https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor o también: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25152&LangID=E.

[111] O'NEIL, Cathy, *Weapons of Math Destruction*, 2017, Penguin Books. Traducción española: *Armas de Destrucción Matemática*, 2018, Capitán Swing Libros S.L.

[112] Véase, por ejemplo, el estudio de este sistema elaborado por la asociación periodística ProPublica: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[113] Véase, por ejemplo: https://www.technologyreview.es/s/11138/por-que-necesitamos-expertos-que-estudien-como-se-comporta-la-ia.

[114] Véase: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016R0679.

[115] Véase: https://eur-lex.europa.eu/legal- content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2901-1-1.

[116] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2576-1-1.

[117] Véase, por ejemplo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143325.

[118] Véase: https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system, visitado el 1 de mayo de 2019.

[119] Véase, por ejemplo: https://www.bloomberg.com/news/articles/2019-04-26/major-tech-firms-come-out-against-police-use-of-ai-algorithms, o bien: https://venturebeat.com/2019/04/26/partnership-on-ai-algorithms-arent-ready-to-automate-pretrial-bail-hearings, visitados el 1 de mayo de 2019.

[120] ARRUÑADA, B., *Blockchains Struggle to Deliver Impersonal Exchange,* Minn. J.L. SCI & Tech., Vol. 19.1, 1918, 78.

[121] ARRUÑADA, B., *Blockchains Struggle to Deliver Impersonal Exchange,* Minn. J.L. SCI & Tech., Vol. 19.1, 1918, 92.

[122] ARRUÑADA, B., *Blockchains Struggle to Deliver Impersonal Exchange,* Minn. J.L. SCI & Tech., Vol. 19.1, 1918, 73.

[123] Puede verse en la dirección: https://steemit.com/ethereum/@chris4210/an-open-letter-to-the-dao-and-the-ethereum-community.

[124] Véase: https://www.greaterzuricharea.com/en/news/chainsecurity-saves-ethereum-security-breach.

[125] Véase: https://arxiv.org/pdf/1802.06038.pdf.

[126] Véase, por ejemplo: https://blog.comae.io/the-280m-ethereums-bug-f28e5de43513.

[127] Véase, por ejemplo: https://mashable.com/2017/07/20/ethereum-hackers-theft-32-million/?europe=true.

[128] Véase, por ejemplo: https://www.bloomberg.com/news/articles/2019-01-08/ethereum-classic-movements-halted-by-coinbase-on-signs-of-attack.

[129] Véase: https://www.securityevaluators.com/casestudies/ethercombing.

[130] La clave privada debe mantenerse secreta, y puede considerarse como nuestra firma personal, permite firmar electrónicamente los mensajes, y es el único medio que permite gestionar y disponer de las monedas virtuales asociadas a la pareja de claves de que se trate. Por tanto, su pérdida supone la pérdida definitiva de estas monedas y, del mismo modo, si un tercero hace uso de nuestra clave privada podrá disponer de nuestras monedas como quiera. La clave pública, por el contrario, puede darse a conocer libremente, no permite firmar mensajes, pero si descifrar los mensajes encriptados o firmados con la clave privada asociada a ella. Además, será el identificador del usuario, de modo semejante a una dirección de correo electrónico, nombre de usuario, etc. Para cada clave privada solo habrá una clave pública que permite realizar las anteriores funciones.

[131] Por ejemplo, las que todos sus caracteres son: '1' o '2' o 'a', etc. o bien todos los caracteres son el '0' salvo el último que es un '1', etc.

[132] BEDNAREK, A., incluso creó una cuenta con claves de este tipo, en la que ingresó un dólar, y pudo comprobar cómo le fue robado a los pocos segundos de ingresarlo, pero, además, examinando las transacciones pendientes de confirmación de *Ethereum* pudo verificar que, con milisegundos de diferencia a la sustracción, hubo otros intentos de robar el mismo dólar, lo que demuestra que existen muchos atacantes dedicados a buscar y monitorizar activa y sistemáticamente este tipo de cuentas para luego vaciarlas.

[133] GALLEGO FERNÁNDEZ, L.A, *Cadenas de bloques y Registros de derechos, Revista Crítica de Derecho Inmobiliario*, núm. 765, 115.

[134] GALLEGO FERNÁNDEZ, L.A, *Ibidem*, 118.

[135] Véase LEGERÉN-MOLINA, A. *Retos jurídicos que plantea la cadena de bloques,* en *Revista de Derecho Civil*, vol. VI, núm. 1 (enero-marzo de 2019), Estudios, 226.

[136] Puede consultarse en: https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&iframe=true.

[137] Vease North. D.C, *Instituciones, cambio institucional y desempeño económico*. Ed. Fondo de Cultura Económica, Mexico D.F., 1995, 13.

[138] Véase: Satoshi NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, (octubre de 2008), http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

[139] Las estadísticas sobre esta materia, correspondientes a las últimas 24 y 48 horas, así como a los últimos 4 días, pueden verse en la dirección: https://www.blockchain.com/es/pools.

[140] Transacciones en las que se transfiere el importe mínimo, o cercano a él, entre cuentas del propio atacante o atacantes.

[141] Véase: https://www.blockchain.com/charts/avg-block-size?timespan=all.

[142] Véase, por ejemplo: *Visa Fact Sheet,* Visa Inc. https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf.

[143] GALLEGO FERNÁNDEZ, L.A, Cadenas de bloques y Registros de derechos, *Revista Crítica de Derecho Inmobiliario*, núm. 765, 115.

[144] Véase: https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.ewfepr21j.

[145] Véase: https://www.blockchain.com/charts/transaction-fees?timespan=all, visitado el 1 de mayo de 2019.

[146] Véase: https://transactionfee.info/charts/payments/segwit.

[147] Véase: https://www.blockchain.com/charts/avg-block-size?timespan=all.

[148] MENI ROSENFELD, *Analysis of hashrate-based double-spending*, 2014. https://arxiv.org/pdf/1402.2009v1.

[149] Véase: https://tradeblock.com/blog/the-51-attack-what-bitcoin-can-learn-from-alt-coin-experiments.

[150] Véase: https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions.

[151] Véase: https://www.ccn.com/1-1-million-malicious-miner-exploits-verge-network-for-seven-figure-payday, https://www.ccn.com/privacy-coin-verge-succumbs-to-51-attack-again, https://blog.theabacus.io/the-verge-hack-explained-7942f63a3017 o https://blog.theabacus.io/lets-do-the-time-warp-again-the-verge-hack-part-deux-c6396ab36ecb.

[152] Véase: https://toshitimes.com/zencash-falls-victim-to-a-51-attack-with-550000-worth-of-tokens-stolen.

[153] Véase: https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack.

[154] Véase: https://breakermag.com/51-attack-vertcoins-strength-fatal-flaw.

[155] Véase, por ejemplo: https://www.bloomberg.com/news/articles/2019-01-08/ethereum-classic-movements-halted-by-coinbase-on-signs-of-attack.

[156] Véase: https://coinmarketcap.com.

[157] Véase: https://blog.sia.tech/fundamentals-of-proof-of-work-beaa68093d2b.

[158] *Ibidem.*

[159] Véase: https://www.bloombergquint.com/business/bitcoin-is-worth-less-than-the-cost-to-mine-it-jpmorgan-says#gs.FhYdn8AW o https://bitcoin.es/noticias/jp-morgan-bitcoin-btc-no-es-rentable.

[160] En la página: https://www.crypto51.app, pueden obtenerse estimaciones del coste en dólares que supondría alquilar una hora de la capacidad de computo necesaria para llevar a cabo ataques del 51% respecto de diversas monedas.

[161] Véase: https://coinmarketcap.com/all/views/all.

[162] LEGERÉN MOLINA, A. *op. cit.*, 199-200. Por ello, de manera coherente con el referido carácter de las cadenas de bloques, se ha propuesto la creación de una plataforma en código abierto con un sistema para la resolución de conflictos sobre *smart contracts* y transacciones con criptomonedas que resulte descentralizado, al igual que las cadenas de bloques. Sobre esta materia, *vid.*, por todos, Kaal y Calcaterra, «*Crypto transaction dispute resolution*», The Business Laywer, Spring 2018. Cita tomada de Legerén Molina A.

[163] GÓMEZ GÁLLIGO J. *El Registro de la Propiedad y los nuevos retos de blockchain,* en Muñiz Espada E., (dir.) Ed.: Wolters Kluwer, 2019. 579.

[164] LEGERÉN MOLINA, A. *op. cit.* 200.

[165] BRENNAN, G. *The Impact of e-Conveyancing on Title Registration. A Risk Assessment*., Ed. Springer, 2015, 29.

[166] GALLEGO FERNÁNDEZ, L.A, *Cadenas de Bloques y Registros de Derechos,* in *Revista Crítica de Derecho Inmobiliario*, núm. 765, 120.

[167] Véase: https://blockstream.com/technology/#sidechains.

[168] DE FILIPPI, P. and WRIGHT, A. *Blockchain and the Law*, Harvard University Press, 2018, 29.

[169] DE FILIPPI, P. and WRIGHT, A. *Blockchain and the Law*, Harvard University Press, 2018, 30.

[170] Véase, por ejemplo: https://www.bloomberg.com/news/articles/2019-02-04/crypto-exchange-founder-dies-leaves-behind-200-million-problem.

[171] CipherTrace, *Fourth Quarter Cryptocurrency Anti-Money Laundering Report 2018 Q4*, Enero de 2019. Puede obtenerse en: https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf.

[172] CipherTrace, *Fourth Quarter Cryptocurrency Anti-Money Laundering Report 2019 Q1*, Abril de 2019. Puede obtenerse en: https://ciphertrace.com/wp-content/uploads/2019/05/ciphertrace-q1-2019-cryptocurrency-anti-money-laundering-report.pdf.

[173] Véase, por ejemplo: https://www.coindesk.com/quadrigacx-officially-enters-bankruptcy-with-millions-still-missing.

[174] Así, por ejemplo, en España véase: Ley 5/2018, de 11 de junio, de modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en relación a la ocupación ilegal de viviendas, (https://www.boe.es/boe/dias/2018/06/12/pdfs/BOE-A-2018-7833.pdf).

[175] CALABRESI, G. y MELAMED, D.A., *Property Rules, Liability Rules and Inalienability: One View of The Cathedral,* 1972, by Harvard Law Review. Ver también MÉNDEZ GONZÁLEZ, F.P., *Derechos reales y titularidades reales*, *Revista Crítica de Derecho Inmobiliario*, núm. 736. *Grosso modo*, tal distinción, desde una perspectiva de análisis económico del Derecho, es equivalente a la distinción formulada por el Derecho Romano entre *actio in rem* y *actio in personam.* Si un derecho está protegido por una regla de propiedad, no puede ser alterado sin el consentimiento de su titular. Si está protegido por una regla de responsabilidad sí puede ser alterado, pero satisfaciendo al propietario la indemnización correspondiente.

[176] MÉNDEZ GONZÁLEZ, F.P., *La función de la fe pública registral en la transmisión de bienes inmuebles. Un estudio del sistema español con referencia al alemán*., Ed.: Tirant Lo Blanch, Valencia, 2017, especialmente 76 a 81.

[177] Sobre el significado de la *publificación* del sistema transmisivo inmobiliario por el Registro de la Propiedad, véase MÉNDEZ GONZÁLEZ F.P., *Fundamentación Económica del Derecho de propiedad privada e ingeniería jurídica del intercambio impersonal*, Ed. Thomson Reuters, 2011, 116 a 136.

[178] Sobre el concepto de oráculo, véase FELIÚ REY, J. Define este autor los oráculos como fuentes de información exterior que suministran datos a un *smart contract* con el fin de o bien concretar las prestaciones o bien proceder a su cumplimiento. FELIU REY, J. *Smart Contract: concepto, ecosistema y principales cuestiones de Derecho privado, La Ley Mercantil,* núm. 47, 2018. En cuanto a quienes pueden ser los oráculos que suministren esa información, pueden ser desde el Registro Civil, la policía que emite los documentos de identidad personal junto con los notarios, *solicitors* o *conveyancers.*

[179] THOMAS R., *The New Zealand Experience: The risks and implications of automation*, Ponencia presentada por el autor a la Conferencia que tuvo lugar en Auckland, Ne Zealand, 29-31 de agosto de 2018, 23.

[180] MÉNDEZ GONZÁLEZ, F.P., *Estado, Propiedad, Mercado,* en *Revista Crítica de Derecho Inmobiliario*, núm. 708, 2008. Thomas R., *The New Zealand Experience: The risks and implications of automation*. Ponencia presentada por el autor a la Conferencia que tuvo lugar en Auckland, New Zealand, 29-31 de agosto de 2018, especialmente, páginas 23, 24 y sigs

[181] GONZÁLEZ JERÓNIMO, *Principios Hipotecarios*, Asociación de Registradores de la Propiedad, Madrid, 1931, 274.

[182] WERBACH K., Trust, but Verify: Why the Blockchain Needs the Law, *Berkeley Technology Law, Journal*, Vol.: 33:487, 2018, 501.

[183] ROTHSTEIN, A., *The End of Money. The story of bitcoin, cryptocurrencies and the blockchain revolution, New Scientist*, 2017, 36.

[184] Esta posibilidad es conocida como The Sybil Attack. Ver John R. DOUCEUR, The Sybil Attack, *in Peer-to-peer-systems* 251, 2002.

[185] ROTHSTEIN, A., *The End of Money. The story of bitcoin, cryptocurrencies and the blockchain revolution, New Scientist*, 2017, 40-43.

[186] WERBACH, K. *op. cit.* 501.

[187] La mayoría, sin embargo, no es suficiente, como han demostrado expertos en seguridad: basta con que un grupo de mineros controle más de un tercio de la capacidad computacional para que puedan realizar un ataque con éxito. EYAL, I.& GÜN SIRER, E., Majority Is Not Enough: Bitcoin Mining Is Vulnerable, en *Financial Cryptography & Data Security,* 436, 438 (2014).

[188] Esta técnica se conoce con el nombre de *proof of work*. No todos los sistemas *blockchain,* sin embargo, utilizan esta técnica criptográfica. Otros sistemas de consenso usan la *proof of stake*, conforme a la cual los validadores arriesgan perder las criptomo-

nedas que les pertenezcan si engañan, a otros. Vease WERBACK, K. *op. cit.*, 502, así como Narayanan et altri, en *op. cit.*, 61.

[189] Cada *Bitcoin,* además, solo puede ser creado como mecanismo de recompensa al minero que resuelve el *hash,* a un ritmo predeterminado y decreciente, con un límite, lo cual resuelve, además, el problema de la determinación de la oferta monetaria sin la existencia de un banco central.

[190] Podría alegarse que quien usa *blockchain* está aceptando todas sus posibles consecuencias. Sin embargo, esta alegación no es admisible por las siguientes razones:1.— Cuando alguien usa *blockchain* cree que no fallará, porque se predica como una tecnología confiable. Es más, sus partidarios afirman que uno de los principales valores añadidos de esta tecnología es, precisamente, evitar este tipo de fraudes. 2.— Si, para sustituir los sistemas vigentes de transmisión, *blockchain* se erige en el único sistema de transferencia, los agentes no podrán elegir.

Puede afirmarse también que en los sistemas tradicionales tampoco se obtienen los consentimientos de todos los posibles afectados. Un contrato tiene lugar entre dos partes y el transferente puede no ser el propietario, pero hacerse pasar por el mismo. El contratante puede, incluso, no ser quien dice ser, porque puede fallar el sistema o sistemas de identificación. En el caso de los registros de documentos, estos solo producen efecto de inoponibilidad de lo no inscrito frente a lo inscrito, sin necesidad de buena fe —Italia— o requiriendo su concurrencia para producir tal efecto —Francia—. En los registros de derechos, sin embargo, las inscripciones implican asignaciones de propiedad, —v.gr.: sistema español de organización arancelaria y responsabilidad personal del registrador—. Asimismo, se rodea al procedimiento registral de garantías suficientes para evitar decisiones erróneas que contravengan el sistema legal, tanto privado —identidad, capacidad de las partes, etc.— como público —cumplimiento con las leyes fiscales, urbanísticas, medioambientales, etc.—. La cuestión es si estos sistemas de identificación, control legal, autenticación del contenido, etc. pueden ser sustituidos con ventaja por *blockchain* o no al menos frente a terceros. Para que el sistema sea fiable se imponen ciertos principios —prioridad, tracto sucesivo, cierre, calificación, independencia del registrador, etc.— e, incluso, algunos sistemas se organizan para desincentivar la posible corrupción.

[191] Este problema se planteará siempre que la contratación se refiera a activos con existencia fuera de la red, no solo inmuebles. Su identificación se realizará por mecanismos al margen. Como siempre que se trata de *blockchain*, esta tecnología nos permitirá verificar no la exactitud de la identificación sino el contenido de la verificación suministrada por un agente externo. La fiabilidad de *blockchain* se refiere a dicha verificabilidad y la verificación como tal será más o menos fiable en función de la garantía que ofrezca el procedimiento de verificación. Paralelamente a lo que sucede, por ejemplo, con la fe pública notarial cuando incorpora el plano de una finca, que no garantiza ni la existencia de la finca ni la correspondencia de sus linderos con los del plano, pero si la existencia del plano aportado —aunque, en este caso, la fiabilidad viene impuesta por disposición legal no por fiabilidad tecnológica, como en el caso de *blockchain*—.

[192] GALLEGO FERNÁNDEZ, L.A., *Cadenas de Bloques y Registros de Derechos,* en *Revista Crítica de Derecho Inmobiliario*, núm. 765, 110.

[193] FILIPPI, P y WRIGHT, A. *Blockchain and the Law*, Harvard University Press, 2018, 24.

[194] *Ibidem*.

[195] *Ibidem*.

[196] The European Union Blockchain Observatory and Forum*, Legal and Regulatory Framework of Blockchains and Smart Contracts*, de 27 de septiembre de 2019, pág.11. https://media.consensys.net/report-the-legal-and-regulatory-framework-of-blockchains-and-smart-contracts-8f397eaf0b1f

[197] ROUBINI, N. https://www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10.

[198] GONZÁLEZ-MENESES, M., *op. cit,* 552-553.

[199] Véase ILLESCAS ORTIZ, R. (Dir.), *Electronificación de los títulos valores*, Ed.: Civitas, Thomson Reuters., 2018, 36 y sigs.

[200] Los artículos 12 y 13 de la Ley 2/1981 reguladora del mercado hipotecario secundario, en la redacción dada por la Ley 41/2007 de 7 de diciembre no exigen inscripción registral para las cédulas y bonos hipotecarios respectivamente, aunque sí un registro contable de las entidades emisoras.

[201] Para una exposición de cómo debería circular el *token* de un inmueble inscrito conforme a la legislación hoy vigente en España, véase SIEIRA GIL, J. y CAMPUZANO GÓMEZ-ACEBO, J., *Blockchain, tokenización de activos inmobiliarios y su protección registral,* en *RCDI*, núm. 775, septiembre-octubre de 2019, especialmente 2302 a 2314.

[202] Merece ser destacada la intervención del Sr. Arrazola durante la discusión en el Senado del Proyecto de Ley Hipotecaria de 1861: «…eso es lo que había de hacer la nueva Ley Hipotecaria: dar ensanche a la propiedad, convertirla en moneda territorial que pueda pasar de mano en mano como pasa un pagaré o una letra…». *En Leyes Hipotecarias de España: Fuentes y Evolución,*T. I. Vol. II, Ed,: Castalia, 1989, 80.

Para un desarrollo de esta idea, véase MÉNDEZ GONZÁLEZ, F. P., *La inscripción como título valor o el valor de la inscripción como título,* en *RCDI*, núm. 703, septiembre-octubre de 2007, 2059-2164.

[203] Para un desarrollo de la abstracción registral, véase MÉNDEZ GONZÁLEZ, F.P*, La función de la fe pública registral en la transmisión de bienes inmuebles. Un estudio del sistema español con referencia al alemán.* Ed. Tirant Lo Blanch, 2017, 40-45. También MÉNDEZ GONZÁLEZ, F.P*, La inscripción como título valor o el valor de la inscripción como título,* RCDI, núm. 703, 2130-2142.

[204] EIZAGUIRRE, J.M distingue entre títulos de literalidad completa y títulos de literalidad incompleta. En el primer caso sitúa a la letra de cambio y en el segundo a las acciones de una S.A, ya que para conocer con exactitud la extensión del derecho que incorporan, es necesario consultar los correspondientes estatutos sociales. EIZAGUIRRE, J.M*, Revista de Derecho Bancario y Bursatil*, núm. 57, 1995, 21.

[205] Para un mayor desarrollo de esta afirmación, véase MÉNDEZ GONZÁLEZ, F.P. *Fundamentación económica… op. cit.,* 136 y sigs.

[206] Sobre el procedimiento registral, véase MÉNDEZ GONZÁLEZ, F.P, *De la publicidad contractual a la titulación registral. El largo proceso hacia el Registro de la Propiedad*, Thomson, Civitas, 2007, 199-203.

[207] DE SOTO H., *El misterio del capital*, Ed.: Península, 2001, 184.

[208] GONZÁLEZ-MENESES, M., *op. cit.* 563-566.

[209] SIEIRA GIL, J. y CAMPUZANO GÓMEZ-ACEBO, J., *op. cit.*, 2301.

[210] ARRUÑADA, B., *Blockchains Struggle to Deliver Impersonal Exchange,* Minn. J.L. SCI & Tech., Vol. 19.1, 1918, 92.

[211] ARRUÑADA, B., *Blockchains Struggle to Deliver Impersonal Exchange,* Minn. J.L. SCI & Tech., Vol. 19.1, 1918, 16.

[212] GALLEGO FERNÁNDEZ, L.A, *Cadenas de bloques y Registros de derechos, Revista Crítica de Derecho Inmobiliario*, núm. 765, 130.

[213] GALLEGO FERNÁNDEZ, L.A., *Cadenas de bloques y Registros de derechos, Revista Crítica de Derecho Inmobiliario*, núm. 765, 130. Continúa afirmando este autor que: «*Es evidente que esto crea, no seguridad, sino inseguridad jurídica y dificulta el tráfico ya que los operadores económicos, en el momento de suscribir los contratos inscribibles, no podrán tener la completa seguridad de que en dicho instante la situación de los derechos inscritos que figuran en el registro es la definitiva, ni de la prioridad que su derecho, una vez presentado en el registro, tendrá frente a otros que se presenten coetáneamente con él, de tal forma que será posible, por ejemplo, que la ejecución de un derecho constituido y presentado posteriormente a otro, pero inscrito con un rango*

anterior a este por la aleatoriedad del funcionamiento de la cadena de bloques, provoque la cancelación de este último».

[214] GALLEGO FERNÁNDEZ, L.A., *Cadenas de bloques y Registros de derechos, Revista Crítica de Derecho Inmobiliario*, núm. 765, 109.

[215] https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.ewfepr21j.

(Trabajo recibido el 25-11-2019 y aceptado para su publicación el 9-3-2020)