LA CERTEZA Y SIMBOLIZACIÓN DE LOS DERECHOS SUBJETIVOS. TOKENS Y CONTRATOS INTELIGENTES

Miguel Ángel Moreno Navarrete
Profesor Titular de Derecho Civil
Universidad de Granada

Fecha de recepción: 15 de abril de 2021
Fecha de aceptación: 15 de mayo de 2021

RESUMEN: Esta investigación trata de realizar una revisión de blockchain, los contratos inteligentes y los tokens desde el punto de vista técnico-jurídico, para evidenciar la importancia que para el Derecho supone, tan solo comparable, en nuestra opinión, con la propia invención de la escritura o el nacimiento y desarrollo del Derecho notarial en la Escuela de Bolonia, que infirieron, en muy diferentes épocas, la seguridad de las relaciones jurídicas. Tratamos de explicar la tecnología blockchain aplicada al Derecho privado. Pero también, es nuestra intención mostrar que los contratos inteligentes y los tokens sustentados en la tecnología blockchain producen dos efectos que nos parecen fundamentales: certeza y simbolización.

ABSTRACTS: This research aims to review blockchain, smart contracts and tokens from a technical-legal point of view, in order to highlight the importance of blockchain for the Law, comparable, in our opinion, only to the invention of writing itself or the birth and development of notarial Law in the Bologna School, which, in very different periods, have made legal relations more secure. Nevertheless, it is also our intention to show that smart contracts and tokens based on blockchain technology produce two effects that we consider fundamental: certainty and tokenisation.

PALABRAS CLAVE: blockchain, contratos inteligentes, fichas o tokens, fungible, no fungible, certeza, simbolización.

KEYWORDS: blockchain, smart contracts, tokens, fungible, non-fungible, certainty, tokenisation.

1. INTRODUCCIÓN

Desde los años 90 del siglo pasado Internet cambió nuestras vidas, se convirtió en la plataforma habitual de libre circulación de información. Desde ese tiempo, en la Red operan personas, datos y modelos de negocio; y su gobierno se basa mas en la confianza que en la propia protección que dispensan las normas jurídicas, muy generalistas, según mi opinión, y contrarias a la globalización y al efecto de control total que la Red produce en el usuario. En definitiva, compartimos información, compramos, etc., por que las empresas nos producen confianza, también, pero en menor medida, por las normas que nos protegen, pero sobre todo, interactuamos por hábitos, negocios o necesidad. Hoy en día, a partir de la criptografía de clave pública y de las tecnologías de registro distribuido, estamos asistiendo a una nueva época, donde el valor y la patrimonialización de Internet es un hecho; pues vamos a pasar de la confianza como motor de la circulación de la información a la seguridad. De esta forma, asistimos al denominado "Internet del valor" (Internet of Value), pues es posible realizar actos y negocios jurídicos de forma segura a partir de técnicas criptográficas y redes descentralizadas.

En este sentido, el Internet del valor se convierte en un instrumento al servicio del mercado, del intercambio de bienes y de prestación de servicios, pero, a diferencia con el comercio electrónico "tradicional", que actuaba como medio ("electrónico") de formalización de las relaciones y negocios jurídicos habituales, este se posiciona en un plano paralelo a la realidad, dónde personas, cosas y conductas son representadas mediante identificaciones electrónicas y tokens o fichas que simbolizan el objeto de las relaciones jurídicas. Y todo ello, a partir de técnicas criptográficas seguras y redes descentralizadas, donde se prefiere el consenso en la Red, o acuerdo de todos, frente a la centralidad y jerarquía normativa propia de los Estados.

El Internet del valor supone, desde el punto de vista jurídico, la seudonimización de las personas y la tokenización de las cosas y servicios. Se trata de un salto cualitativo de lo real a lo simbólico.

El Internet del valor se ha desarrollado a partir de las tecnologías blockchain, denominadas de registro distribuido (DLT), y su posterior evolución, a partir de los criptocontratos, mal denominados "contratos inteligentes". Dichas plataformas blockchain proporcionan seguridad de las transacciones, lo cual supone la clave de su desarrollo y su evolución exponencial. De esta forma, la seguridad es condición para la confianza en las transacciones entre partes distantes entre si, pues blockchain proporciona fiabilidad y prueba de las transacciones, en definitiva, certeza. Mucho más que el comercio electrónico tradicional, fundamentado en la confianza en las empresas, más que en pruebas materiales. Es un gran paso, pues el comercio electrónico se convierte en fiable, y podrá desarrollarse en otros ámbitos del Derecho patrimonial, como los negocios inmobiliarios, en el derecho registral, de sucesiones, etc.

La cuestión es si los sistemas de Derecho, tan arraigados en la Historia, se van a adaptar sobre las bases y fundamentos actuales o, por el contrario, se va a ir adoptando sistemas jurídicos disruptivos. En este sentido, el uso del blockchain debe acompañarse con el establecimiento de un marco jurídico apropiado. Es fundamental que se realice una intervención proporcional en el sector y con criterios claros para identificar las aplicaciones basadas en blockchain de "riesgo elevado", que son aquellas que suponen riesgos significativos, en especial, en materia de derechos de los consumidores.

Pero las bondades de las tecnologías blockchain son contrarrestadas con los riesgos que se pueden producir, pues pueden afectar muy especialmente a la libertad, en este caso, a la libertad de decidir de manera consciente, en definitiva, a la libertad de contratar y contractual, más si cabe, en el ámbito del consumo.

En efecto, frente a lo que supone la digitalización de lo cotidiano, la libertad de contratar que se consagró en la vieja Europa con la implantación de las ideas de la Revolución francesa y que se plasmó en la codificación del Derecho civil, puede desaparecer, para convertir la voluntad humana en inconsciente y predecible. La igualdad de las partes en la contratación puede no existir, ni tan siquiera, con la aplicación de la normativa protectora de los consumidores, pues este "salto tecnológico" menoscaba los derechos y libertades. El Internet del valor y el tratamiento de datos, en cuanto a su aplicación al consumo, pueden afectar fundamentalmente a la libertad individual, pues convierte nuestra conciencia en colectiva. En este sentido, la digitalización de lo cotidiano restringe la libertad y mercantiliza nuestra vida privada. El problema es que el consumidor lo asume como algo habitual y normal, pues, hemos aprendido a convivir con ello.

En la actualidad, las normas jurídicas no nos dan repuestas a este problema, pues un mayor control estatal o una mayor información, control de la publicidad, etc., no es suficiente. Es necesario que el uso de blockchain y los contratos inteligentes esté asociado a un marco normativo específico, ya que los smart contracts van a tener una repercusión jurídica amplia, al permitir la formalización de cualquier tipo de relación jurídica.

Por su parte, respecto a los avances legislativos, en el ámbito de la Unión Europea se ha publicado la Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos (COM(2020) 593 final), de 24.09.2020 (en adelante, MiCA, "Markets in Crypto-Assets"), cuya finalidad principal es la regulación de las finanzas digitales en las plataformas basadas en tecnologías de registro descentralizado.

Esta investigación trata de realizar una revisión de blockchain, los contratos inteligentes y los tokens desde el punto de vista técnico-jurídico, para evidenciar la importancia que para el Derecho supone, tan solo comparable, en nuestra opinión, con la propia invención de la escritura o el nacimiento y desarrollo del Derecho notarial en la Escuela de Bolonia, que infirieron, en muy diferentes épocas, la seguridad y certeza de las relaciones jurídicas.

2. LAS TECNOLOGÍAS DE REGISTRO DISTRIBUIDO (DLT): BLOCKCHAIN Y SMART CONTRACTS

En este tiempo, no puede abordarse un estudio jurídico sobre el tráfico jurídico digital sin acercarnos a las ciencias criptográficas y computacionales, pues, se hace indispensable la comprensión de los sistemas técnicos para su tratamiento jurídico. En general, las técnicas criptográficas tienen como fin que el tráfico de datos cumpla con las reglas de autoría, integridad o autenticidad y no repudio. De tal manera que los datos puedan acreditar, por lo que nos interesa, cualquier tipo de relación o negocio jurídico.

Blockchain es una tecnología que se engloba en la denominada "de registro distribuido" (Distributed Ledger Technology, DLT) con una serie de especificaciones técnicas, muy resumidamente: una base de datos segura copiada y sincronizada en tantos ordenadores como componen la red descentralizada, que es su esencia.

Fue en 2008, uno o varios autores —no se sabe— anónimos, bajo el seudónimo de Satoshi Nakamoto, aseguraron que existía la posibilidad de existencia de una red descentralizada de efectivo electrónico de "igual a igual[1]" (Peer-to-Peer). En general, es una tecnología de estructura

[1] Nakamoto, S. (Seudónimo). "Bitcoin: A Peer-to-Peer Electronic Cash System". Oct. (2008),

de bloques de datos en cadena, donde la unión o eslabón de un bloque con otro se realiza a través de metainformaciones del bloque anterior. Es como un gran libro contable de registro de transacciones, con un "Debe" y un "Haber", donde cada página se representa con un bloque y, además, muestra información de la página anterior. A su vez, el libro contable está almacenado en todos y cada uno de los ordenadores de la red (nodos). Los contables se denominan "mineros" y son los encargados de apuntar en el "Debe" y en el "Haber" del libro y de verificar la realidad del apunte (transacción). Cuando un minero cierra una página, esta ya no puede modificarse sin que entre en conflicto con la página posterior. Por ello, cada una de las páginas de este "libro contable virtual" están encadenadas y son inmutables, es decir, dan prueba cierta del contrato o transacción concreta del que trae causa cada uno de los apuntes (transacciones).

La razón de ser o su utilidad se encuentra en la confiabilidad e integridad de los datos, lo que supone un avance significativo en la seguridad y, por tanto, un instrumento al servicio del Derecho que, históricamente, ha arbitrado sistemas de permanencia de los hechos a través del tiempo o prueba. De esta forma, la blockchain se coloca como una de las técnicas más fiables de constatación de las relaciones en el tráfico jurídico digital. Por tanto, la certeza es una de sus características esenciales.

La inmutabilidad de los datos hace que la utilidad de blockchain en el tráfico jurídico digital sea evidente. Puede utilizarse para innumerables actos y negocios jurídicos, pues es una forma de asegurar, de preconstituir la prueba; ya que la información está en la comunidad (muchos testigos) de forma inmutable y transparente no dependiendo de terceros, además de que casi no es hackeable.

Con esta propuesta técnica, se pasa de un sistema basado en la "confianza", a un sistema mediante el cual se prescinde de prestadores de servicios y terceras partes de confianza a partir de técnicas de seguridad criptográfica. Se pasa de la confianza a la certeza.

En efecto, hoy en día es enorme la cantidad de datos que necesitamos almacenar, algunos con especial relevancia jurídica. Las técnicas informáticas son diversas, desde las más sofisticadas, con la necesaria colaboración de terceros certificadores hasta las más rudimentarias que se podrían resumir en el típico "pantallazo". En cualquier caso, siempre se está bajo amenaza de hackers o de modificaciones no deseadas y, por tanto, de inseguridad. En blockchain esto no casi imposible, la modificación maliciosa de datos se hace casi inviable gracias a su estructura y concepto.

De esta forma, la información contenida en los bloques, la cual puede de muy diferente índole, como partes (sujetos, emisor y receptor), fecha, cuantía, objeto (tokens), transacciones, etc., no es modificable. ¿Por qué? Para contestar a esta cuestión, es necesario abordar más profundamente la cadena de bloques, los nodos y los prestadores de servicios, además de las reglas de actuación.

2.1. LA CADENA DE BLOQUES

¿Cuál es el contenido de un bloque en blockchain?

- A) El "hash". Fundamentalmente, un bloque contiene el denominado "hash" o número de identificación del bloque, el cual es único. Igualmente, el bloque tiene el hash del bloque anterior, lo que constituye el eslabón de la cadena. Y así, sucesivamente, se conectan los bloques. El "hash" es una función matemática mediante algoritmos que cifra y resume alfanuméricamente cualquier contenido, ya sea la identidad de los sujetos como los propios bloques de la cadena. Como hemos expuesto, el número hash de cada bloque es único, además, depende de la información que contiene, de tal forma que, si se modifica la información, cambia el hash. Al cambiar el número único no sería

(https://nakamotoinstitute.org/bitcoin/).

identificado por el bloque posterior, por lo que se rompería la cadena y ésta se invalidaría en el nodo concreto que ha sido modificado maliciosamente, no en todos los nodos, de ahí la seguridad que proporciona.

- B) El encabezado del bloque. En general, el encabezado contiene la data (Time); el nivel de dificultad de averiguación por parte de los mineros de la función hash del bloque (Difficulty Level); datos técnicos (Technical Data); el Merkle Root; el hash del bloque anterior, lo que hace posible la cadena de bloques; y, por último, el "nonce[2]".

La característica principal del nonce, desde el punto de vista jurídico, es que es unidireccional ("de ida"), es decir, con la información contenida en el bloque se puede averiguar su función hash, que es pública, pero no al contrario. No se puede averiguar el contenido del bloque desde el resumen. Y este hash del bloque se modifica si alguien, maliciosamente, modificara o manipulara el bloque (prueba de las transacciones). Como quiera que el bloque siguiente contiene el hash del bloque anterior, ambos hashes no coincidirían. Por ello los bloques son inmutables. Además, para mayor seguridad, el nonce debe ser aceptado por otros mineros mediante consenso.

- C) Las transacciones. Son las que se realizan entre cedente y cesionario. Tienen por objeto la transmisión de criptomoneda (su origen), activos digitales (tokens) o cumplir contratos inteligentes. Cada transacción se basa en una dirección que representa una clave pública (identificación digital) y, para poder realizarla, el cedente deberá conocer su clave privada, que usará para firmarla digitalmente, además deberá tener un activo digital (BTC, Ethereum, etc.). Del mismo modo, el cesionario tiene una dirección que representa su clave pública asociada a su clave privada (identificación digital). Del mismo modo, se pueden generar activos digitales *ex novo* (son la recompensa de los mineros y los programadores en los supuestos de bitcoin o la creación digital en el criptoarte, por ejemplo).

Finalmente, cuando se han realizado (n) transacciones dentro del bloque (generalmente unas 2000), éstas se agrupan en un "Árbol de Merkle[3]" (árbol hash binario, Merkle Tree) que proporciona un método de simplificación y verificación seguro (prueba) de los contenidos de grandes cadenas de datos.

2.2. LOS NODOS

Los nodos, desde el punto de vista jurídico son prestadores de servicios. Desde un punto de vista técnico, resumidamente, son ordenadores sostenidos por los mineros, conectados a una red blockchain con un software que almacena una copia en tiempo real de toda la cadena de bloques. Cuando un bloque se confirma y se cierra por un minero, se comunica a todos los nodos y se almacena copia en los ordenadores (nodos) de cada uno de ellos. Esta es la grandeza del blockchain ya que el libro contable que representa la cadena de bloques se encuentra en todos y cada uno de los nodos, ¿existe mayor prueba de las transacciones? No, pues reiteramos que cada nodo tiene una copia de los datos, no hay una sola base de datos, ya que está replicada en todos (registro distribuido). De tal manera que si un usuario altera los datos, su base de datos no coincidirá con los del resto de nodos, por lo que quedaría, de igual modo, invalidada y la cadena permanece en el

[2] El nonce es una función hash que resume el bloque y debe ser averiguada, en competencias por los incentivos, unos con otros, por los mineros a patir de un problema matemático (Proof-of-Work) que no tiene solución y depende de un nivel de dificultad, el cual se determina por un número que corresponde con el número de ceros iniciales en una cadena alfanumérica (e.g., Dificultad: 19, "0000000000000000000a7f06105cae52513ccffedcb017e9fd5458863b3c79e9"). Al no tener solución se realiza mediante pruebas por los mineros.

[3] Merkle, R. "A Certified Digital Signature". *Advances in cryptology - CRYPTO '89*. Proceedings of a conference held at the University of California, Aug. 20-24 (1989), pp. 218-238
(https://www.researchgate.net/publication/221355342_A_Certified_Digital_Signature).

resto inalterable. Como consecuencia de la anterior, la fiabilidad de los datos la proporcionan los propios nodos no dependiendo de terceros, como prestadores de servicios de certificación, web, de correo, de pago, etc.

2.3. LOS MINEROS

Blockchain es utilizado por dos tipos de sujetos: los usuarios que utilizan el servicio y los denominados "mineros" o aquellos que minan transacciones, cierran o crean nuevos bloques. ¿Qué son los mineros? Son sujetos (prestadores de servicios, empresas) con ordenadores dedicados (nodos) de gran poder computacional conectados a una red blockchain, los cuales verifican la realidad de las transacciones que se ejecutan en la red o "acción de minar" (mining, Proof-of-Work); del mismo modo, confirman que un usuario no realice dos transacciones con el mismo objeto (doble transmisión), es decir, que la cesión del derecho subjetivo es única; además de la falsedad de la transacción. También tienen la función de minar los bloques[4].

En efecto, la razón de éstos últimos es que conforme se realizan transacciones, contratos, etc., la ingente masa de datos debe de ser ubicada en nuevos bloques. Los mineros son los encargados de su creación a partir de técnicas muy complejas. Pero, no basta con su creación, sino que, el nuevo bloque, debe de ser autorizado por el resto de la comunidad (consenso), uniéndose a la cadena.

¿Por qué el interés de los mineros? Los mineros cuando cierran un bloque, dónde se encuentran (n) número de transacciones, obtienen un incentivo o recompensa (en los casos de bitcoins, en esta moneda, por lo que se crean, de esta forma, nuevos bitcoins); además de la comisión por cada una de las transacciones del bloque (transaction fees). Por ello, compiten por conseguir un bloque[5]. Pero, para llegar a esto, es necesario un proceso previo, es el registro de la información, de los datos.

Los mineros, en general, tienen la obligación, en términos informáticos, de ser honestos y se controlan en la propia red por el resto de mineros a través de técnicas criptográficas.

2.4. CONSENSUS Y DESCENTRALIZACIÓN

Los nodos han de seguir las mismas reglas, protocolos, actualizaciones, etc. Los mineros validan las transacciones y los bloques mediante acuerdo entre ellos. Es el denominado "consensus" y se basa en normas propias y en el historial. Las reglas son los parámetros acordados para que una transacción sea válida. El historial es la secuencia de las transacciones del sistema y la actuación de los mineros[6].

Del mismo modo, fruto del consensus es la descentralización, aunque dicha característica no es sinónimo de "sin estructura[7]". La red blockchain no tiene titular, dueño, intermediarios, ni gobiernos que la regule. No está jerarquizada en las típicas relaciones informáticas cliente-servidor,

[4] En ocasiones, dada que su participación depende de la capacidad de computación, se unen con otros mineros creando una cooperativa de minería (pool), para así aunar más capacidad computacional.

[5] Se ha de exponer que el incentivo por cierre de cada bloque se va reduciendo progresivamente con el tiempo, de esta forma, en el caso de bitcoins, el aumento de estos es cada vez menor, fenómeno que se conoce como "halving"; de esta manera, el valor del bitcoin debe aumentar para que sea rentable el minado.

[6] Si no es así, pueden producirse problemas de consenso. Son:

- Bifurcación dura (Hard Fork). Cuando hay un cambio de reglas y no hay consensus, la cadena de bloques se divide.
- Bifurcación blanda Soft fork. Es una falta de consenso de carácter temporal causada por algunos nodos que no siguen las reglas.

[7] *Raina* S. *et al.* "Blockchain Development and Fiduciary Duty". *Stanford Journal of Blockchain Law & Policy*, Vol. 2, Nº. 2 (2019).

sino que la red es distribuida ya que todos los nodos actúan en plano de igualdad y están conectados unos con otros (pares iguales, Peer to Peer).

3. LOS CONTRATOS INTELIGENTES

Fue Szabo, quien en 1995 habló por primera vez del concepto de contrato inteligente y lo definió como: "Un conjunto de promesas, incluyendo protocolos dentro de los cuales las partes cumplen con las otras promesas. Los protocolos suelen ser implementados con programas en una red de computadoras, o en otras formas de electrónica digital, por lo que estos contratos son 'más inteligentes' que sus antecesores en papel. No se implica el uso de inteligencia artificial[8]". En la visión de Szabo, el contrato inteligente se configura como un instrumento técnico de formalizar las relaciones jurídicas a través de redes informáticas, sin que ello implique el uso de la inteligencia artificial. La idea es que muchas de las cláusulas contractuales pueden integrarse en un hardware y software concreto, de tal manera que se facilitan los remedios frente al incumplimiento o, como dice el autor, el incumplimiento del contrato resulte costoso[9].

En nuestra opinión, los conceptos de contratos inteligentes que se han expuesto a lo largo del tiempo describen lo que hace un programa informático o más bien las líneas sucesivas de código, que se basan en acciones y eventos ante estímulos o sucesos, con la particularidad de su almacenamiento. En general, se trata de una denominación común de las cadenas de programación (generalmente, en lenguaje Solidity) que se contienen en diversas plataformas, como Ethereum (la más importante), a las que los programadores le han denominado así. Es más, dichas plataformas, sobre la base del blockchain, realizarán en un futuro muchos más trabajos o acciones que contratos.

En definitiva, con el término «smart contracts» se designan aquellas cadenas de código de programación que ejecutan los propios pactos o prestaciones del contrato de forma automática, sin la intervención de posterior consentimiento o actividad por ninguna de las partes. El contrato legal inteligente se configura como un instrumento técnico de formalizar las relaciones jurídicas a través de redes descentralizadas (DLT). Pero, de todas las ideas innovadoras que aportó Szabo, hemos de detenernos en aquella que nos dice que los contratos inteligentes no usan la inteligencia artificial, aunque son "más inteligentes" que el contrato tradicional. En este sentido, en nuestra opinión, los contratos inteligentes utilizan la programación informática para automatizar la ejecución de un contrato y aportar mecanismos de solución proactivos, pero nada más. Por ello, tendríamos que cuestionarnos el mismo concepto de "smart contracts", más bien, deberíamos hablar de "criptocontratos", por que, como software, utilizan técnicas criptográficas. No obstante, en la actualidad existen proyectos que desarrollan el uso de la inteligencia artificial en las transacciones electrónicas. Por ello, incidimos en la idea que, dado que la aplicación de técnicas criptográficas es su fundamento, sería más conveniente de hablar de criptocontratos, pues la autoejecución no es la propiedad esencial que los distingue.

En este sentido, podemos definir los criptocontratos o contratos legales inteligentes como aquellos contratos que, mediante técnicas criptográficas e interpretados en código informático, determinan las partes, autoejecutan las obligaciones, crean derechos, tokenizan o simbolizan cosas,

[8] Szabo, N. "Smart contracts glossary" (1995). En https://nakamotoinstitute.org/smart-contracts-glossary/ (Consultado el 8 de abril de 2020).

[9] Szabo, N. "Formalizing and Securing Relationships on Public Networks". *First Monday, Peer–reviewed journals on the Internet*, Vol. 2-9, 1997. https://journals.uic.edu/ojs/index.php/fm/article/view/548/469 (Consultado el 12 de enero de 2020).

derechos y obligaciones, tanto de la realidad exterior como digitales, y se registran de forma segura en redes de registro distribuido.

En cuanto a su naturaleza jurídica, se trata de contratos digitales de adhesión destinados a la contratación en masa cuyos pactos o cláusulas generales son impuestas por un tercero, ajeno a la relación contractual entre las partes.

Respecto a las clases de contratos inteligentes, debemos proponer una readaptación de la tradicional teoría del contrato a las teorías de la computación.

En este sentido, en la teoría general de la contratación, los contratos onerosos en función de la determinación de las prestaciones se clasifican en conmutativos y aleatorios. Los contratos conmutativos, son aquellos en que las prestaciones están determinadas, de tal forma, que las obligaciones, en la fase de creación o perfección y cumplimiento o ejecución, coinciden. Por su parte, los contratos aleatorios, la determinación de las prestaciones en la ejecución depende de un hecho posterior —incierto— a la propia creación o perfección del contrato.

La distinción de unos y otros es muy importante para la codificación y programación de los contratos inteligentes y, por tanto, para su propia evolución técnica en el tiempo. Por tanto, en función de la determinación de las prestaciones, los contratos inteligentes pueden clasificarse en deterministas o probabilísticos.

3.1. SMART CONTRACTS DETERMINISTAS

Los contratos conmutativos pueden explicarse a partir del modelo matemático denominado "determinista", aplicado, entre otros, al mundo de la economía de la empresa, según el cual, las mismas entradas o condiciones iniciales producen, sin variación, las mismas salidas y resultados; sin existencia de incertidumbre o azar.

A su vez, el modelo determinista puede ser simple, complejo o hipercomplejo:

- El modelo determinista puede ser simple. Si se aplica a los contratos, nos podemos referir a la prestación periódica del pago de un préstamo (desde el inicio se fijaron y son conocidas las prestaciones dinerarias a plazo).

- El modelo determinista complejo parte del conocimiento del resultado, pero con la interacción de elementos o hechos que, por el conocimiento que se tiene de ellos, pueden determinarse. En este caso, podríamos hablar del contrato de préstamo hipotecario. En el ejemplo, el contrato está determinado en cuanto a sus prestaciones, pero existen toda una serie de hechos que pueden variar las obligaciones, como el índice que modifica el interés variable sometido a la decisión de un órgano externo a la propia relación contractual. Las prestaciones periódicas son conocidas a partir de la experiencia y conocimiento de las fluctuaciones posibles de dicho índice.

- Del mismo modo, existen los modelos deterministas hipercomplejos. Los matemáticos hablan del universo como modelo hipercomplejo. En el ámbito jurídico, nos podríamos referir a un simple contrato de servicios de un abogado para entablar una acción ante los tribunales.

En este caso, la prestación de servicios por parte del abogado está determinada: entrevista, negociación, demanda, juicio oral, recursos, etc. Es verdad que es una obligación de medios y no de resultado, pues el abogado no puede comprometerse a "ganar" el juicio. Pero, en la propia obligación de medios, puede actuarse de muy diferentes maneras: ¿Cuántas entrevistas con el cliente? ¿cuántos folios de demanda? ¿cuántas horas de estudio, o normativa y jurisprudencia a citar? ¿cuánto tiempo de preparación del juicio?, ¿cómo se interpretará el Derecho?, etc. Además, existen otros factores que condicionan la obligación de medios, como son la actuación del procurador, el

sistema judicial, la actuación en juicio, interpretación jurídica y decisiones del juez y, en su caso, el fiscal, la actitud del cliente, etc.

El modelo determinista se predica, desde el punto de vista del código informático, en la red blockchain cuyo objeto es el intercambio de criptomonedas o tokens pues, los nodos por igual, deben de predecir ciertamente el resultado a partir de las funciones que modifican estados. Es por lo que se rechazan, en la propia cadena de bloques (on-chain), los contratos inteligentes aleatorios[10].

Pero ello no obsta para que la incertidumbre se determine en fuentes externas a través de oráculos (off-chain), o terceros, prestadores de servicios, necesarios para el cumplimiento.

3.2. SMART CONTRACTS PROBABILÍSTICOS

Por su parte, los modelos denominados "estocásticos" o probabilísticos, existe algún hecho que no se conoce por lo que no se puede anticipar el resultado.

El modelo probabilístico puede ser simple, complejo o hipercomplejo:

- El modelo probabilístico simple. En este caso, podríamos referirnos a los contratos de juego y apuesta. La prestación se determinará a partir de un hecho futuro pero cierto. Existe incertidumbre temporal, pero en un entorno controlado.

- El modelo probabilístico complejo. Nos podemos referir, por ejemplo, a un contrato de suministro entre empresas, el cual, la determinación de las prestaciones está prefijadas, pero su determinación última dependerán de muchos factores, como el precio de mercado, abastecimiento, transporte, impuestos directos, decisiones gubernamentales, etc. En este caso, el espacio muestral es más amplio, pues existen diferentes resultados posibles.

- Los modelos probabilísticos hipercomplejos se relacionan con el cerebro humano, con la inteligencia. La determinación es muy ardua y concreta a partir del conocimiento previo, experiencia y numerosos estímulos del medio. Se nos ocurre la prestación de servicios que realiza un controlador aéreo. Existen modelos de contratos probabilísticos en la propia blockchain. Así, Chatterjee *et al.*, presentan enfoques aleatorios a partir de la teoría de juegos[11].

4. EL OBJETO DEL CONTRATO INTELIGENTE: LOS TOKENS

El objeto de todo contrato inteligente es el intercambio de bienes y derechos, y los servicios. Como en general, el objeto de todo derecho subjetivo son las cosas y las conductas.

Por "cosa" dice Díez-Picazo, "se suele entender toda realidad del mundo exterior que posee una existencia material"; si bien, también existen "aquellas realidades, que, careciendo de existencia corporal y siendo producto o creación intelectual del espíritu humano, el ordenamiento jurídico valora como posible objeto de derechos subjetivos[12]".

[10] Vogelsteller, F., Buterin V. "Ethereum whitepaper". *Ethereum Foundation*, 2014; Chatterjee, K. *et al.* "Probabilistic smart contracts: Secure randomness on the blockchain". *1st IEEE International Conference on Blockchain and Cryptocurrency*, ICBC 2019, South Korea, 14 May 2019. DOI: 10.1109/BLOC.2019.8751326.

[11] Chatterjee, K. *et al.* "Probabilistic smart contracts: Secure randomness on the blockchain". *Loc. cit.*, DOI: 10.1109/BLOC.2019.8751326.

[12] Díez-Picazo, L. *Fundamentos del Derecho Civil Patrimonial*. Vol. III, 5ª Ed., Editorial Aranzadi, Pamplona, 2008, pp. 184 y 186.

Pero, la tradicional distinción entre bienes muebles e inmuebles, basada fundamentalmente en la movilidad material de la cosa ha de superarse en la realidad actual. Hoy es más preciso centrarse en el concepto de "tangibilidad" de las cosas o posibilidad o no de apropiación. Pues la clasificación de los bienes muebles e inmuebles ha de referirse a las cosas materiales.

En general, la propia existencia de cosas inmateriales que, con el tiempo, han adquirido una importancia vital en la sociedad digital actual y sobre todo en el Internet del valor, hace necesario un replanteamiento de la propia clasificación de las cosas como objeto de las relaciones jurídicas. Las cosas incorporales o derechos son intangibles, inmateriales, y se configuran como susceptibles de apropiación; al igual que las cosas tangibles[13]. De entre las cosas inmateriales, a partir de las tecnologías de la información y de las comunicaciones surgieron los bienes digitales; o aquellos producidos y suministrados en formato digital[14].

Por otra parte, en el ámbito digital, hay que distinguir entre datos[15], código y servicios. Solo aquellos datos y servicios que representan derechos u obligaciones son el verdadero objeto de los derechos subjetivos digitales. Lo "digital" es la expresión de la realidad en valores numéricos discretos, unos y ceros (forma binaria o bits). En este sentido, los datos digitales son bienes intangibles, abstractos; y expresan la realidad a partir del procesamiento o tratamiento automático de información utilizando sistemas computacionales.

En cuanto a los servicios, de acuerdo con el artículo 2.7 de la Directiva (UE) 2019/771, relativa a determinados aspectos de los contratos de compraventa de bienes, es "servicio digital":

- a) Un servicio que permite al consumidor crear, tratar, almacenar o consultar datos en formato digital.

- b) O un servicio que permite compartir datos en formato digital cargados o creados por el consumidor u otros usuarios de ese servicio, o interactuar de cualquier otra forma con dichos datos.

Pero los bienes y servicios digitales no son, en exclusiva, el objeto mediato de los contratos inteligentes, sino que son, en general, toda clase de bienes, incluidos los tangibles, muebles e inmuebles; además de las prestaciones de dar, hacer y no hacer.

Es por lo que, tanto por razones técnicas como jurídicas, se hace necesario la representación de todas las clases de bienes y derechos, así como las obligaciones, en su forma digital. El resultado son los activos digitales y su proceso técnico: la tokenización o simbolización del derecho subjetivo.

[13] El jurisconsulto Gayo distinguió entre cosas corporales o aquellas que por su naturaleza pueden tocarse (*corporales eae sunt quae sui natura tangi possunt*); e incorporales, las cuales consisten en un derecho (*quae tangi non possunt, qualia sunt ea, quae in iure consistunt, sicut hereditas, usus fructus, obligationes quoquo modo contractae*). GAIUS, libro II.1-2, *institutionum*; D. I.8.1.1. GAIUS, libro II.1-2, *institutionum*; D. I.8.1.1.

[14] Artículo 2.6 Directiva (UE) 2019/771, del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de compraventa de bienes, por la que se modifican el Reglamento (CE) Nº 2017/2394 y la Directiva 2009/22/CE y se deroga la Directiva 1999/44/CE. Según el cual: son bienes digitales aquellos datos producidos y suministrados en formato digital. Así se dispone también en la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, Considerando 11.

Así se dispone también en la Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, Considerando 11.

[15] Artículo 2.2.b) DCSD, "(…) datos en formato digital cargados o creados por el consumidor u otros usuarios (…)".

5. LA SIMBOLIZACIÓN DE LOS DERECHOS SUBJETIVOS: LA TOKENIZACIÓN DE LAS COSAS Y LOS SERVICIOS

Como hemos expuesto, sobre la base de los bienes materiales e inmateriales y los servicios se ha de construir, a modo de escalón superior, su representación en el tráfico jurídico digital, en torno a blockchain, como objeto del contrato inteligente.

De ahí, surge un concepto: el token; y la acción o proceso de transformación de las cosas en tokens: tokenización o simbolización (token modelling). Esto produce fundamentalmente el efecto de accesibilidad y la acreditación, en caso de conflicto, de la titularidad jurídica del derecho a partir de la constatación en la cadena de bloques.

Un "token" es una "utilidad", un activo (digital assets). Es la representación digital de los bienes corporales, muebles e inmuebles, o incorporales como los derechos o los créditos y las conductas; y su proceso se denomina "tokenización". Se configuran como la solución técnica digital (criptográfica) de intercambio de bienes y prestación de servicios en las tecnologías de bases de datos distribuidas, pues traen causa de un contrato inteligente. Como hemos expuesto, el proceso de tokenización parte de técnicas criptográficas que dotan al token de las características propias de los bienes materiales o inmateriales, así como los derechos de crédito, objeto del tráfico jurídico, en definitiva, su creación se corresponde con un contrato inteligente.

En general, los tokens se ecuentran en la cadena de bloques de forma nativa (native tokens), como las criptomonedas; o por encima de ésta, a nivel de aplicación (application tokens), en este caso, los tokens operan en la cadena siempre que se asignen primero a un contrato inteligente. Como consecuencia, éstos pueden ser individualizados a través de los balances personales o mediante la identificación única cuando se traten de no fungibles (NFT). En definitiva, "puedo llevar mis tokens (derechos subjetivos) en mi bolsillo" (wallet).

Dicho proceso puede resumirse en esta sentencia referida al criptoarte: "Los tokens son los criptoactivos nativos de una aplicación blockchain. Están impulsados por contratos inteligentes (acuerdos financieros basados en códigos) que están programados en Ethereum. Cuando un artista tokeniza, está convirtiendo su propiedad intelectual en un activo financiero, por lo que la ficha de un artista refleja el valor de su producción creativa[16]".

Pero, ¿qué relación tienen los tokens con las criptomonedas? A diferencia de las criptomonedas, que son una unidad de valor, los tokens representan cualquier bien, derecho u obligación, además de ser también una unidad de valor. En definitiva, solo la obligación pecuniaria se realiza con criptomonedas.

6. BLOCKCHAIN Y LA TRANSMISIÓN DEL DERECHO SUBJETIVO

Para la transmisión del derecho subjetivo, se parte de la transferencia de una "criptomoneda" o token como una cadena de firmas digitales. De tal forma que la criptomoneda (fungible) o token (no fungible) pasa de un propietario a otro mediante el sistema de clave pública y privada, cifrado (hash) y verificación de firmas. Pero este sistema tiene un problema, el propietario de la criptomoneda o token puede haberla transmitido (n) veces, por lo que es necesario la existencia de una autoridad monetaria confiable (MINT) que verifique que la doble (como mínimo) transacción

[16] EEUU. Sentence 9.07.2018, Court: United States District Courts, 9th Circuit, Southern District of California.

no se produzca. En definitiva, dependemos de la centralización que se produce en la entidad de dinero electrónico.

Para solucionar dicho problema, es necesario conocer públicamente todas las transacciones anteriores (historial) para saber si el cedente es el verdadero propietario del token; todo ello, en una agrupación de usuarios y nodos, los cuales acuerden (consenso) que la transacción se hace por el cedente es por una única vez, asegurándose el cesionario que el token se le traspasa desde el verdadero titular. Del mismo modo, es necesario establecer un "sellado de tiempos" (timestamp) que asegure la fecha en que la transacción se efectua por aquello de "*prior tempore, potior in iure*". Dicha marca de tiempo es una función de cifrado segura (hash) que contiene la marca anterior de tiempo y, así, sucesivamente, formando una cadena.

De esta forma, se configura una red que deberá seguir los siguientes pasos (reglas del blockchain):

A) Los bloques, los cuales contienen las transacciones se transmiten a todos los nodos cuando el minero resuelve el nonce.

B) Los nodos aceptan el bloque minado si todas las transacciones son válidas.

C) Los nodos comparan el hash del bloque minado con el hash del anterior bloque.

D) La primera transacción es especial, pues se emite "*ex novo*" por primera vez la criptomoneda o el token.

E) Los usuarios deben registrarse creando así el denominado "monedero" (wallet). Ellos pueden solicitar o enviar dinero o ejecutar un contrato que se contiene en líneas de código.

F) La transacción es iniciada, pero, mientras no es minada, se encuentra en la fase de "unspent output transaction" (UTXO); y se anota en el "mempool", es decir, un espacio de almacenamiento temporal mientras la transacción es procesada por los mineros. Cuantas más transacciones se realicen en la red, mayor será el tiempo de proceso por parte de los mineros.

Respecto de los usuarios, como hemos expuesto, el primer paso es asegurar que la persona cedente es el verdadero titular del activo. Para ello se requiere de una firma digital del usuario a partir de la clave privada asociada a una clave pública[17]. La clave privada solo es conocida por su titular y se utiliza para la firma de la transacción, y el resto de los usuarios puede verificar la identidad y titularidad a partir de la clave pública. Por tanto, cada transacción tiene una firma digital distinta. Todas, excepto la primera que se produce en un bloque (coinbase transaction), tienen entradas (inputs) y salidas (outputs).

¿Qué condiciones debe tener un usuario para realizar una transacción?

A) Lista de inputs necesarios:

- Acceso mediante clave privada.

- La suma en criptomoneda de mis inputs es superior a los de mis outputs. Por tanto, puedo enviar valor. En caso contrario, los nodos no aceptarían la transacción.

- Se ha de referenciar de dónde procede este activo, ya que todas las transacciones son públicas, es decir, el propietario anterior mediante su clave pública.

B) Lista de outputs necesarios:

[17] Ejemplo de clave pública extendida:
"xpub6CCQBjujFFz1Z6uhhu27xs2DVKZvK1sAT2E9TtAbMsV7qzxvbDgMNi9a3cTaZCTe2UXs1FMfEzPQ4msE7D34Lf2AaQWRBTd2yFVYohuJXs4".

- El cesionario debe cumplir con ciertas condiciones para recibir el activo monetario. Por tanto, debe de ser titular de una clave pública conocida por el cedente que, a su vez, está asociada a una privada del cesionario.

- El input tiene que ser mayor que el output y se transfiere por entero; y su diferencia, parte se considera "transaction fees" y es la compensación económica para los mineros, y otra parte, se reenvía a la public key del cedente de nuevo o a otra públic key que este quiera.

Cada transacción (contrato) tiene un nombre (ID), que es un mensaje y se representa mediante un hash (resumen criptográfico, generalmente: SHA256) de dicho mensaje.

La transacción, por último, debe ser verificada y confirmada por los mineros en el menor tiempo posible (de ello depende el incentivo).

Pero, para una descripción más minuciosa del sistema, hemos de referirnos a las clases de tokens, los estándares tokens. Al delimitar las clases de tokens es necesario partir de la tradicional distinción de las cosas en fungibles y no fungibles.

Los tokens fungibles son aquellos que pueden ser sustituidos unos por otros, como las criptomonedas. No fungibles son aquellos que, por su naturaleza, no pueden ser sustituidos, pues representan cosas y derechos únicos, además de obligaciones *intuitu personae*. Pueden ser activos físicos, como toda clase de bienes muebles e inmuebles; activos o bienes digitales; y activos de obligación (derechos de crédito).

Desde el punto de vista técnico, para el correcto funcionamiento del sistema, se hace necesario el acuerdo o consenso de todos sobre qué clase de tokens deben existir. Por ello, surgen los estándares tokens o propuestas consensuadas por la comunidad de usuarios, programadores, empresas, etc., a modo de *traditio* simbólica por consensus.

En general, existen dos tipos de tokens: los "utility tokens" y "security tokens". Los utility tokens son aquellos que, cuya posesión, da derecho a un bien o servicio. Por su parte, los security tokens son aquellos que representan la propiedad de un bien o derecho. Si bien, entre los estándares tokens o protocolos consensuados se encuentran varios asentados y otros que se están desarrollando. Lo importante es que, como forman parte de la programación, se ha de conocer sus funciones en el entorno de los smart contracts.

Desde el punto de vista jurídico, toma bastante importancia la distinción entre tokens fungibles y no fungibles.

6.1. TOKENS FUNGIBLES (ERC-20)

Los tokens fungibles (ERC-20) representan cosas fungibles, es decir, aquellos bienes y derechos que pueden sustituirse unos por otros y se caracterizan por ser divisibles en cuanto a su valor. En general, se crearon para el mercado de las criptomonedas y otros negocios como la financiación de las empresas mediante creación de tokens (ICOS, initial coin offering). La creación (mint) y su extinción (burn) se produce a través de un contrato inteligente, por lo que operan encima de la blockchain, con una serie de especificaciones[18].

[18] Por todo, https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md. En cuanto a sus especificaciones:
- Método Name. Nombre del token [function name() public view returns (string)].
- Método Symbol. Símbolo del token [function symbol() public view returns (string)].
- Método Decimals. Número de decimales, si se utilizan [function decimals() public view returns (uint8)].
- Método TotalSupply. Número total de tokens que existen [function totalSupply() public view returns (uint256)].
- Método BalanceOf. Saldo de la cuenta del propietario, es decir, tokens en propiedad de un sujeto [function balanceOf(address _owner) public view returns (uint256 balance)].

Sobre la base de la cadena de bloques, el sistema se fundamenta básicamente en el almacenamiento de direcciones (sujetos de derecho, titulares de cuenta) y balance de saldos en blockchain. Generalmente, el proceso de transferencia entre cedente y cesionario se realiza de la siguiente forma:

- Consulta de balance actual de tokens (balanceOf), es decir, número de total de tokens disponibles (totalSupply), del cedente.

- Transferencia de tokens (Transfer) a otro titular, cesionario —dirección Ethereum— (transferFrom).

- Aprobación del uso de tokens (Approval).

- El token se guarda en el balance del cesionario (wallet).

Este es el estándar actual, si bien, ya existen mejoras sobre el mismo, como el token ERC-223 o ERC-777. O el ERC-948 para los servicios de suscripción.

6.2. TOKENS NO FUNGIBLES (NFTs, Non Fungible Tokens, ERC-721, ERC-1155)

Pueden ser objeto mediato de los contratos inteligentes bienes no fungibles, ya sean muebles o inmuebles, así como los derechos subjetivos; y las obligaciones ("Negative value" assets). Su tokenización se produce mediante el token estándar ERC-721 y más modernamente el ERC-1155. También existe, el ERC-989, el cual permite que un token pueda ser titular a su vez de otro token a modo de "child tokens" o "parent tokens" respectivamente; o el ERC-994 diseñado para el registro de bienes inmuebles.

Hoy en día, se está generalizando el uso del token ERC-1155. Este se nos presenta, en nuestra opinión, como fundamental desde el punto de vista jurídico, pues es capaz de aglutinar la utilidad de un token fungible y no fungible a la vez, es decir, es capaz de simbolizar varios derechos u obligaciones de diferente naturaleza. Su importancia se verá en un futuro próximo, pero sin duda, es el germen del desarrollo efectivo de los contratos inteligentes a toda clase de contratos tradicionales y de desarrollo digital de la libertad contractual.

Nos interesa desarrollar el funcionamiento de un contrato inteligente referido a un token no fungible (ERC-721), para comprender la transmisión de los derechos subjetivos[19].

La mayoría de las operaciones se relacionan con la verificación de la realidad del token y de la titularidad mediante la comprobación de la dirección (ownerOf) u otra dirección autorizada (takeOwnership).

A) Operaciones relativas a la verificación del titular y del token:

- Método Transfer. Transferencia del token al cesionario [function transfer(address _to, uint256 _value) public returns (bool success)].

- Método TransferFrom. Transferencia del token desde el cedente [function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)].

- Método Approve. Se permite la transferencia al cesionario [function approve(address _spender, uint256 _value) public returns (bool success)].

- Método Allowance. Nos informa sobre la cantidad de tokens que pueden transferirse [function allowance(address _owner, address _spender) public view returns (uint256 remaining)].

- Evento Transfer. Se activa cuando se transfieren los tokens [event Transfer(address indexed _from, address indexed _to, uint256 _value)].

- Evento Approval. Aprobación de la transferencia [event Approval(address indexed _owner, address indexed _spender, uint256 _value)].

[19] Todo el código de programación en el lenguaje solidity, es tomado del repositorio https://github.com/.

- Cada token no fungible se identifica con un ID único no modificable (uint256) (e.g., 0x150b7a02[20]).

- Asignación del token a un titular, es decir, a una dirección de Ethereum[21].

- Verificación de la titularidad del token (dirección aprobada[22]).

- Verificación del ID único del token a la titularidad asignada[23].

- Verificación de la aprobación del operador[24].

B) Operaciones relativas al contrato:

- Comprobación de saldo del titular cedente[25].

- Y retorno del identificador único del token y de la dirección (titularidad del propietario[26]).

- Aprobación de la dirección del cesionario para transferencia del ID único del token[27].

- El sistema devuelve la dirección aprobada (titularidad del cesionario) para un token único[28].

- Aprobación o no de la transacción por el operador, el cual transfiere el token[29].

- Aprobación del operador por el propietario[30].

B) Operaciones relativas al cumplimiento del contrato.

El cumplimiento del contrato se realiza mediante la transferencia del token con ID único, esta puede realizarse a otro titular o a un contrato inteligente, el cual formará su objeto.

- Transferencia del token. Partes (address from, address to) y objeto (uint256 tokenId[31]).

- Si bien, la transferencia habrá de realizarse de forma segura, tanto a un nuevo titular como a otro contrato inteligente[32].

---

[20] 'bytes4 private constant _ERC721_RECEIVED = 0x150b7a02;

[21] 'mapping (uint256 => address) private _tokenOwner

[22] 'mapping (uint256 => address) private _tokenApprovals

[23] 'mapping (address => Counters.Counter) private _ownedTokensCount

[24] 'mapping (address => mapping (address => bool)) private _operatorApprovals

[25] 'function balanceOf(address owner) public view returns (uint256)
    require(owner != address(0), "ERC721: balance query for the zero address")
    return _ownedTokensCount[owner].current

[26] 'function ownerOf(uint256 tokenId) public view returns (address)
    address owner = _tokenOwner[tokenId]
    require(owner != address(0), "ERC721: owner query for nonexistent token"
    return owner

[27] 'function approve(address to, uint256 tokenId) public
    address owner = ownerOf(tokenId)
    require(to != owner, "ERC721: approval to current owner"
    require(_msgSender() == owner || isApprovedForAll(owner, _msgSender,
      "ERC721: approve caller is not owner nor approved for all")
    _tokenApprovals[tokenId] = to
    emit Approval(owner, to, tokenId)

[28] 'function getApproved(uint256 tokenId) public view returns (address)
    require(_exists(tokenId), "ERC721: approved query for nonexistent token")
    return _tokenApprovals[tokenId]

[29] 'function setApprovalForAll(address to, bool approved) public
    require(to != _msgSender(), "ERC721: approve to caller")
    _operatorApprovals[_msgSender()][to] = approved
    emit ApprovalForAll(_msgSender(), to, approved)

[30] 'function isApprovedForAll(address owner, address operator) public view returns (bool)
    return _operatorApprovals[owner][operator]

[31] 'function transferFrom(address from, address to, uint256 tokenId) public
    //solhint-disable-next-line max-line-length
    require(_isApprovedOrOwner(_msgSender(), tokenId), "ERC721: transfer caller is not owner nor approved")
    _transferFrom(from, to, tokenId)

[32] 'function safeTransferFrom(address from, address to, uint256 tokenId) public

- Verificación de la realidad y existencia del token[33].

- Verificación de que el titular puede transferir el token[34].

C) Proceso de transferencia con creación de un nuevo token:

Se crea un nuevo token y se verifica que no exista con anterioridad. El destino puede ser otra dirección (sujeto) o un contrato inteligente[35].

7. CERTEZA Y SIMBOLIZACIÓN

A lo largo de esta investigación hemos tratado de describir la tecnología blockchain aplicada al Derecho privado. Si bien, es nuestra intención mostrar que, más allá de lo anecdótico que puede suponer la auto-ejecución de las prestaciones en la Red, desde el punto de vista jurídico, supone un avance que puede desembocar en disrupción jurídica, como ya se habla, respecto de las técnicas computacionales, de disrupción tecnológica.

Las técnicas criptográficas dan certeza a las transacciones y producen el efecto que, en la Historia, desde la Baja Edad Media ha supuesto la institución notarial y el sistema de registros públicos, además de la documentación privada de las relaciones jurídicas. Blockchain es una tecnología que manifiesta, si no más, la certeza y, por tanto, la confianza y seguridad.

Pero, en nuestra opinión, lo más importante es que es una tecnología que puede simbolizar las relaciones jurídicas, desarrollar una realidad digital paralela a la realidad, al tráfico jurídico tradicional; pues sujetos de derecho, bienes, derechos y obligaciones son representados. Esta es la verdadera esencia para el Derecho.

Si a ello se le une la inteligencia artificial, la neurociencia teórica, la realidad virtual, la computación en la nube, etc., tenemos los ingredientes esenciales para el nacimiento de proyectos como "metaverso". Aún es pronto para ver los resultados de la aplicación de esta realidad paralela digital, pero no se tardará mucho en que se hable de un cambio de paradigma jurídico.

---

safeTransferFrom(from, to, tokenId, "")
function safeTransferFrom(address from, address to, uint256 tokenId, bytes memory _data) public
require(_isApprovedOrOwner(_msgSender(), tokenId), "ERC721: transfer caller is not owner nor approved")
_safeTransferFrom(from, to, tokenId, _data);
function _safeTransferFrom(address from, address to, uint256 tokenId, bytes memory _data) internal
_transferFrom(from, to, tokenId);
require(_checkOnERC721Received(from, to, tokenId, _data), "ERC721: transfer to non ERC721Receiver implementer")

[33] 'function _exists(uint256 tokenId) internal view returns (bool)
address owner = _tokenOwner[tokenId]
return owner != address(0)

[34] 'function _isApprovedOrOwner(address spender, uint256 tokenId) internal view returns (bool)
require(_exists(tokenId), "ERC721: operator query for nonexistent token")
address owner = ownerOf(tokenId)
return (spender == owner || getApproved(tokenId) == spender || isApprovedForAll(owner, spender)

[35] 'function _safeMint(address to, uint256 tokenId, bytes memory _data) internal
_mint(to, tokenId)
require(_checkOnERC721Received(address(0), to, tokenId, _data), "ERC721: transfer to non ERC721Receiver implementer")
function _mint(address to, uint256 tokenId) internal
require(to != address(0), "ERC721: mint to the zero address")
require(!_exists(tokenId), "ERC721: token already minted")
_tokenOwner[tokenId] = to;
_ownedTokensCount[to].increment
emit Transfer(address(0), to, tokenId)