Artículo doctrinal

BLOCKCHAIN, SMART CONTRACTS Y ADMINISTRACIÓN DE JUSTICIA

YOLANDA RÍOS LÓPEZ

MAGISTRADA-JUEZ DEL JUZGADO DE LO MERCANTIL Nº 1 DE BARCELONA.
ESPECIALISTA EN ASUNTOS MERCANTILES POR EL CGPJ.

enero de 2021

BLOCKCHAIN INTELLIGENCE
www.blockchainintelligence.es

ÍNDICE:

1. NUEVAS TECNOLOGÍAS Y PROCESO CIVIL

En la denominada "*Era de la Cuarta Revolución Industrial*", en la que emergen nuevas tecnologías disruptivas, la "*blockchain*", también llamada cadena de bloques, los "*smart contracts*", erróneamente traducidos como "*contratos inteligentes*", y la inteligencia artificial, ocupan un lugar privilegiado en los centros de investigación y desarrollo de empresas privadas y entidades públicas. El reto no es pequeño; garantizar la seguridad de las transacciones, en un mercado enormemente globalizado, en el que los recursos electrónicos han desplazado a los tradicionales medios de contratación y pago.

Una de las cuestiones que no ha merecido excesiva atención pese a su creciente relevancia atañe a cuál deber ser el valor probatorio que la información registrada en la cadena de bloques puede ostentar en un proceso civil.

Asimismo, se ha planteado la duda relativa al alcance del "*smart contract*" como fuente de relaciones jurídicas, y cómo deben operar los mecanismos probatorios para que el juez pueda resolver un litigio basado en "*contratación inteligente*" conforme a Derecho.

No existe un marco legal que regule las tecnologías disruptivas, pese a los esfuerzos de la Unión Europea por crear marcos homogénos de gobernanza. Ello alcanza no solo a los criptoactivos, sino también a sistemas más complejos, como los "*smart contracts*", los dispositivos "*internet of things*", o los "*software*" de inteligencia artificial, que permiten la creación en tiempo real de millones de datos, codificados mediante complejas claves criptógraficas, y almacenados masivamente en registros que no siempre son compatibles.

El estudio de los aspectos procesales relevantes para resolver aquellos litigios en los que la configuración de la cadena de bloques como sistema de almacenamiento de datos pueda ser decisiva, exigen un análisis sosegado de las normas de Derecho Probatorio, ante la inexistencia de legislación aplicable a la "*blockchain*". Se impone, así, la necesidad de fijar una definición previa de los estándares tecnológicos más relevantes.

A su vez, la incipiente problemática derivada del uso de los "*smart contracts*", como códigos informáticos de ejecución automática, exige analizar su desarrollo tecnológico, para efectuar una traslación ordenada, desde lo informático hasta lo jurídico, introduciendo mecanimos de gobernanza y de "*enforcement*" útiles.

2. LA "BLOCKCHAIN", ¿UNA AUTÉNTICA BASE DE DATOS?

Numerosas definiciones sobre la tecnología "*blockchain*" han sido formuladas[1]. El presente estudio no pretende abordar con exhaustividad todas ellas, limitándose a destacar aquellos rasgos técnicos de la "*blockchain*" que, por su especial relevancia, permitirán enjuiciar la fiabilidad y autenticidad del sistema.

La cadena de bloques constituye una base de datos descentralizada, basada en tecnología DLT (*distributed ledger technology*), en la que múltiples nodos o usuarios, a través del sistema "*peer-to-peer*", validan la información registrada en cada uno de los bloques a partir de una fórmula de consenso, en la que basta que los acuerdos se adopten por mayoría para que la información se considere fiable y auténtica.

El principal rasgo del referido sistema de confianza es que prescinde de la intervención de cualquier autoridad externa, pues el sistema se rige por las decisiones que adoptan los propios nodos participantes, en régimen de autogobernanza[2].

La cuestión es si cabe afirmar que la integridad e inmutabilidad de los datos registrados constituye una cualidad inherente, implícita a dicha tecnología, o si, por el contrario, es posible una manipulación que ponga en tela de juicio el uso de dicha tecnología.

En caso de afirmar que existe una inmediata correlación entre la información que accede a dicha base de datos, y la autenticidad de su contenido, por el mero hecho de hallarse registrada en una cadena de bloques, resultaría una revolución en el sistema probatorio.

---

[1] En cuanto al origen de la tecnología "blockchain", a finales de 2008, bajo el seudónimo de "Satoshi Nakamoto", una persona o grupo de personas publicó un artículo que presentaba una nueva forma de ejecutar una plataforma digital, descentralizada y de usuario-a-usuario, llamada "chain of blocks", caracterizada por la forma en la que la plataforma descentralizada se ejecutaba partiendo de una estructura de base de datos distribuida, siendo la primera aplicación de la tecnología "blockchain" la famosa criptomoneda "bitcoin".Posteriormente, en el año 2013 el programador Vitalik Buterin publicó un artículo describiendo un nuevo tipo de plataforma basada en "blockchain" llamada "Ethereum" (véase https://ethereum.org/), que permite la creación de programas que funcionan de forma descentralizada dentro de la blockchain a modo de "cajas" criptográficas que contienen valor, el cual sólo puede ser desbloqueado si ciertas condiciones se cumplen; se trata del "Smart Contract" .

[2] Una "blockchain" es una base de datos distribuida entre diferentes usuarios, protegida por medio de la criptografía y, organizada en diferentes bloques de transacciones que se relacionan entre sí a través de algoritmos matemáticos (véase ALEXANDER PREUKSCHAT, "Blockchain: la revolución industrial de Internet", Barcelona, Gestión 2000, 2017). Sus principales elementos son: a) Un nodo: un ordenador personal o un superordenador, dependiendo de la complejidad de la red. Todos los nodos deben tener el mismo software o protocolo para comunicarse entre ellos, independientemente de la capacidad de cómputo; b) Un software o protocolo estándar: se trata de un software informático que ofrece un estándar común para que los nodos puedan comunicarse entre sí; c) Una red entre pares o de usuario-a-usuario o P2P (Peer-to-Peer), de forma que los nodos de la red se conectan directamente a una misma red; d) Un sistema descentralizado, pues no existe una parte intermediaria que ejerza el control en la red, de modo, que todos los ordenadores conectados a la red son los que la controlan, ya que no existe una jerarquía entre los nodos, son todos iguales entre sí.

3. "BLOCKCHAIN" Y PRUEBA EN EL PROCESO CIVIL

3.1. La "*blockchain*" como fuente de prueba.

En el ámbito del Derecho Procesal, es clásica la distinción de CARNELUTTI[3] entre fuentes y medios de prueba.

Las fuentes de prueba son los instrumentos que contienen información o datos relevantes[4] al margen de la realidad procesal. Cuando se habla de preconstituir prueba, se alude a la creación de un registro o soporte apto para contener información con vistas a su posterior aportación en un proceso judicial.

Los medios de prueba son los instrumentos que la legislación procesal reconoce como mecanismos aptos para introducir las fuentes de prueba en el proceso civil.

De ordinario, los artículos 299 y siguientes de la Ley de Enjuciamiento Civil 1/2000, de 7 de enero, enumera con carácter *numerus apertus* como medios de prueba los documentos, el interrogatorio de parte, la prueba testifical, el dictamen pericial y el reconocimiento judicial, además de los medios de reproducción de la palabra, el sonido o la imagen.

En este contexto, analizar el valor probatorio que en un eventual procedimiento judicial pudiera otorgarse a la cadena de bloques exige deslindar en qué medida dicho libro-registro puede ser fuente de prueba, y por qué vía los datos registrados pueden ser introducidos en el proceso como medio de prueba.

3.2. Hechos registrados en la cadena de bloques.

Por su propia configuración técnica, resulta que la cadena de bloques permite certificar información sobre tres extremos relevantes; a saber, el hecho, acto o estado de cosas sobre el que se constituye el registro en la misma, la identidad del otorgante (si está previamente definida), y el sellado de tiempo, o momento temporal en el que cada transacción queda sellada de forma auténtica e inmutable en el tiempo en el bloque.

[3] CARNELUTTI, F., La prueba civil, Buenos Aires, Ed. Arayu, 1955.

[4] Desarrollando dichos conceptos, resulta que la fuente es un concepto extrajurídico, que se corresponde con una realidad anterior y extraña al proceso, mientras que el medio de prueba es un concepto jurídico, concretamente procesal, que designa el instrumento o actividad que permite la introducción de las fuentes en el proceso; la fuente existe con independencia de que llegue a realizarso o no un proceso, mientas que el medio cobra sentido en relación con un proceso y producirá efectos en un proceso concreto; las partes antes de iniciar un proceso buscan las fuentes de prueba y, una vez obtenidas, efectúan la proposición de los medios de prueba para introducir las fuentes en el proceso; las fuentes preexisten al proceso, mientras que en éste solo se practican los medios, pues sin proceso no existen medios. Por contra, las fuentes son independientes en su existencia, perviven ajenas al proceso; la fuente es lo sustantivo y material, el medio es la actividad.

Desde el prisma del Derecho Probatorio, la cadena de bloques plantea dos grandes retos.

El primero de ellos enfrenta el inconveniente derivado del anonimato de los usuarios, pues, por definición, cualquier sujeto que registra transacciones a través de la "*blockchain*" pública, opera mediante un sistema de claves criptográficas públicas y privadas que garantiza la privacidad del usuario. Ello impide establecer una correlación entre la persona física que está actuando y el usuario que accede a la red virtual, es decir, entre la identidad física y la identidad virtual.

El segundo obstáculo emana de la integridad del contenido de la cadena de bloques. Si no accede al registro el documento completo, sino el denominado "*hash*", es decir, como la huella digital del mismo, la autenticidad parece ceñida a dicha clave alfanumérica, procedente de la criptografía. Se requerirá, pues, de un "*traductor*" que descodifique el contenido del mensaje de manera fiable. Y este elemento también pudiera ser objeto de prueba en el proceso civil.

3.3. La "blockchain" como soporte electrónico.

Uno de los aspectos esenciales en el estudio de la cadena de bloques como base de datos auténtica atañe a la naturaleza electrónica de la misma, pues todos los ordenadores o nodos que la conforman están interconectados entre sí en un plano de igualdad.

Como regla general, los hechos relevantes de los que queda constancia en la cadena de bloques, tales como la realidad de la transacción, el sujeto titular de la misma, y el sellado de tiempo, pueden ser introducidos en un procedimiento judicial incorporando el soporte electrónico en el que se hallan registrados, así como la copia impresa del *hash*, de la transacción, y de los bloques afectados, junto a las claves criptográficas que permiten su descodificación[5].

[5] Ilustramos un ejemplo de transacción susceptible de ser implementada en una cadena de bloques, y toda la información relevante que pudiera acceder al proceso civil en caso de incumplimiento o frustración del negocio jurídico, a partir del símil que recoge FELIU REY, J., Smart Contract: Concepto, ecosistema y principales cuestiones de Derecho privado, en "Revista la Ley Mercantil", nº 47, mayo 2018, Ed. Wolkers Kluwer. pág. 11 y 12: "Imaginemos una mesa de reuniones alrededor de la cual se sienta un número significativo de personas. Cada una de estas personas (ordenadores o nodos conectados) tiene un libro de registro en blanco donde realiza anotaciones (sistema descentralizado). La primera anotación, sigamos con el ejemplo, es que A tiene 50 acciones y se las quiere transmitir a B. Primero se verifica que A tiene 50 acciones que puede transmitir (bloque con información), y se comprueba que todos lo miembros de la mesa están de acuerdo con esta anotación inicial (sistema de verificación por consenso descentralizado). Luego se transmite a B. Como todos tienen en su libro que A es el titular y las puede transmitir, proceden a anotar la transmisión a B. Si A quiere volver a transmitir esas acciones, no podría porque ya no consta en el registro como titular y los miembros de la mesa al verificar tal información rechazarían la anotación, por lo que no permitirían esa transacción. Sólo B podría transmitir las acciones ulteriormente. Intentar una alteración de los registros, aunque no es imposible, exigiría un consenso de todos los miembros de la mesa y una modificación en todos los nodos de cadenas de bloques que recogen un tracto sucesivo, lo que resultaría, sin duda, altamente improbable."

4. LA "BLOCKCHAIN" COMO MEDIO DE PRUEBA

En el proceso civil, solo deben ser objeto de prueba los hechos controvertidos, es decir, aquéllos sobre los que las partes se hallen disconformes, y hayan sido previamente traidos a colación en el relato fáctico que sustenta la demanda y la contestación. Cualquier dato sellado en la cadena de bloques debe acceder al proceso a través de los medios de prueba legalmente previstos.

4.1. La "Blockchain" como documento privado.

La prueba documental constituye un soporte apto para incorporar al proceso las fuentes de prueba electrónicas, pues toda información registrada en el bloque no deja de conformar un documento, con la singularidad de que aparece plasmado en un soporte informático.

El artículo 3.5 de la Ley de Firma Electrónica 59/2003, de 19 de diciembre, dispone que constituye documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado, pudiendo ser soporte de documentos públicos y privados.

Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, ostentará el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

En el supuesto de la cadena de bloques, procede aportar al proceso como prueba documental privada la impresión del "*hash*", es decir, la clave alfanumérica aspociada a un determinado contenido, así como su "*traducción al lenguaje humano*" como si se tratara de un documento escrito tradicional en soporte papel.

Esta eficacia probatoria se aprecia con mayor intensidad en el ámbito de la contratación, ya que los artículos 23 y 24 de la Ley 34/2002, de 11 de Julio, de Servicios de la Información y del Comercio Electrónico, enfatizan una clara equivalencia entre el soporte electrónico y el soporte papel como fuente de prueba que puede acceder a cualquier proceso.

En concreto, el artículo 23.3 LSSICE establece que la forma electrónica equivale a la forma escrita, por lo que es claro que la base de datos que configura la cadena de bloques constituye un documentos a los efectos probatorios.

Añade el artículo 24.2 LSSICE que el soporte electrónico en el que se halle registrado un contrato electrónico será admisible en juicio como prueba documental.

En torno a su valor probatorio, el artículo 326.1 de la Ley de Enjuiciamiento Civil dispone que los documentos privados harán prueba plena en el proceso siempre que su autenticidad no sea impugnada por la parte perjudicada. Por tanto, la regla es que, en caso de que no resulte impugnada la autenticidad, el registro en *blockchain* impreso en un documento privado despliega la fuerza probatoria plena.

Solo la impugnación de la autenticidad de dicho soporte provocará que el aportante deba pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente con el fin de acreditar su autenticidad.

Cuando no se pudiere deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

En el concreto ámbito de la firma electrónica, el soporte en que se hallen los datos firmados electrónicamente es admisible como prueba documental, por lo que el artículo 326.3 LEC dispone que si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.

Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

Una cuestión problemática es que, en el actual sistema procesal, parece necesario que el documento privado aportado al proceso se acompañe de un dictamen pericial elaborado por un técnico experto en "*blockchain*" que certifique la autenticidad de los datos insertos en la cadena de bloques, en particular los aspectos criptográficos, así como la equivalencia entre la huella digital y el dato que pervive en el mundo exterior.

Ahora bien, la conveniencia de aportar dicho dictamen no excluye la posibilidad del juez de valorar el medio de prueba documental por sí mismo,

al albur del artículo 326.2 LEC, sin necesidad de acompañarlo de exámenes adicionales.

4.2. La "*blockchain*" como documento público.

Uno de los retos principales que plantea el uso de la cadena de bloques es la posibilidad de otorgar a la misma el valor probatorio que la legislación procesal asigna exclusivamente al documento público[6].

Quienes defienden las bondades de la cadena de bloques como mecanismo de almacenamiento de información fiable e inmutable, señalan que el registro y de los datos en el bloque constituye una prueba inequívoca, cuanto menos, de la realidad del hecho, acto o transacción registrada, así como del sellado de tiempo.

De lege lata, el listado de documentos públicos que con carácter *numerus clausus* recoge el artículo 317 LEC se refiere a aquellos documentos expedidos por autoridades, ya sean judiciales, notariales o registradores, legitimadas para certificar, en el ámbito de sus competencias, la autenticidad de dichos contenidos.[7]

La primera conclusión es que la información que resulta de la cadena de bloques no consta certificada por fedatario alguno, lo que de entrada impide afirmar que la *blockchain* puede ser equiparada a un documento público, por no hallar expreso encaje en la legislación procesal.[8]

---

[6] De conformidad con el artículo 1216 del Código Civil, son documentos públicos los autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la ley, añadiendo el artículo 1218 del mismo Cuerpo Legal que los documentos públicos hacen prueba, aun contra tercero, del hecho que motiva su otorgamiento y de la fecha de éste. También harán prueba contra los contratantes y sus causahabientes, en cuanto a las declaraciones que en ellos hubiesen hecho los primeros.

[7] Dispone el citado precepto que: Son, por tanto, documentos públicos con arreglo a la normativa procesal los contemplados en el artículo 317 LEC, a cuyo tenor, a efectos de prueba en el proceso, se consideran documentos públicos:

1.º Las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Letrados de la Administración de Justicia.

2.º Los autorizados por notario con arreglo a derecho.

3.º Los intervenidos por Corredores de Comercio Colegiados y las certificaciones de las operaciones en que hubiesen intervenido, expedidas por ellos con referencia al Libro Registro que deben llevar conforme a derecho.

4.º Las certificaciones que expidan los Registradores de la Propiedad y Mercantiles de los asientos registrales.

5.º Los expedidos por funcionarios públicos legalmente facultados para dar fe en lo que se refiere al ejercicio de sus funciones.

6.º Los que, con referencia a archivos y registros de órganos del Estado, de las Administraciones públicas o de otras entidades de Derecho público, sean expedidos por funcionarios facultados para dar fe de disposiciones y actuaciones de aquellos órganos, Administraciones o entidades.

[8] Cuestión distinta es que la parte interesada en introducir un determinado hecho en el proceso interese la participación de un fedatario público, como el notario, a los efectos de configurar un documento público. Ahora bien, el valor probatorio del mismo será limitado. Cabe solicitar una cta de protocolización

Sería en todo caso necesaria una reforma *de lege ferenda* en la que el legislador equiparara expresamente las certificaciones extraídas de la cadena de bloques con los documentos validados por fedatario público[9].

Cuestión distinta es si, con base en sus rasgos tecnológicos, la cadena de bloques permite la emisión de certificados que podamos considerar a efectos procesales como "*auténticos*". A la vista de las características enumeradas *ut supra*, parece que solo la realidad de la transacción registrada y el momento temporal del sellado son elementos verdaderamente fiables.

En cuanto al modo de aportación de los documentos públicos al proceso, el artículo 318.1 LEC dispone que los documentos públicos deberán aportarse al proceso en original o por copia o certificación fehaciente, bien en soporte papel o mediante documento electrónico, o si, habiendo sido aportado por copia simple, en soporte papel o imagen digitalizada, conforme a lo previsto en el artículo 267, no se hubiere impugnado su autenticidad.

Por tanto, de atribuir al registro en la cadena de bloques valor probatorio pleno, bastaría la aportación al proceso de la copia digitalizada del mismo, siendo necesaria la aportación del original en el supuesto en que el contrario impugnara aquélla.

Sin duda, la necesidad de la aportación de un dictamen pericial sigue diendo el caballo de batalla. Su utilidad en orden a garantizar al juez la correspondencia entre el código encriptado y el lenguaje humano es indudable.

---

o de presencial notarial para dar fe del contenido de la informaicón sellada en un bloque. El acta de protocolización tiene lugar cuando un particular o un tercero eefctúa una impresión previa de la informaicón relevante y solicita notarialmente la protocolización. En este caso, el notario extiende una cta de ptrotoclización haciendo constar los datos de identidad del compareciente, el hecho de la entrega de un documento previamente impreso,a sí como la fecha de tal entrega, sin que la fe pública notarial alcance la existencia de la inscripción de la informaicón en el bloque, sino a aquello que el notario ve o percibe por los sentidos.El acta de presencia tendré lugar cuando un particuolar solicite del notario que naviegue a través de ls red, personándose el notario a un lugar virtualm, extendiendo acta de las operaciones realizadas, recogiendo sus impresiones. La fe pública notarial se extiende a ñpos contenidos percibidos por el notario.

[9] En el ámbito del Derecho Comparado, en Italia existe una regulación expresa de la "blockchain"introducida mediante la enmienda del artículo 8 de la Ley de Conversión del Decreto-ley de simplificación nº 135/2018, que acoge una definición sobre la tecnología de registros distribuidos, y sobre los "smart contracts", siendo de especial valor la regulación en el artículo 41 sobre el valor probatorio de un documento estampado en "blockchain". Sin embargo, aun cuando no existe impedimento legal para que la información registrada en la cadena de bloques pueda admitirse como medio de prueba, su valor probatorio permenece en la órbita de la valoración judicial. No existe jurisprudencia unánime que garantice que el hash generado constituye prueba de información certera. Un antecedente jurisprudencial que reconoce a la tecnoloigía "blockchain" como medio de prueba es la declaración del comisario de cuentas del Tribunal de Casación francés, realizada en febrero de 2019, afirmando que permite probar la existencia de una creación proporcionando un certificado digital.

5. EL "*SMART CONTRACT*" COMO NEGOCIO JURÍDICO

5.1 Concepto.

Un "*smart contract*" puede ser definido en términos generales como un protocolo de códigos informáticos, escrito por tanto en un lenguaje codificado, que permite que un dispositivo tecnológico ejecute de forma automatizada las secuencias previamente programadas, prescindiendo de cualquier así intervención humana[10].

Se dice, por tanto, que en el "*smart contract*" el "*código es la ley*", pues cada una de las cláusulas negociales redactada según el paradigma "*if X, then Y*" ejecutará inexorablemente programada, lo que incrementará la seguridad jurídica y permitirá prescindir de cualquier tercero intermediario.

5.2 Los "*smart contracts*" como "*negocios jurídicos*".

Partiendo de la regulación que los artículos 1089, 1091, 1261 y 1278 del Código Civil español efectúan de los contratos, será posible categorizar al "*smart contract*" como negocio jurídico fruto de una libre autonomía de la voluntad de las partes siempre que exista un previo consentimiento por parte de aquéllas acerca de las prestaciones que constituyan su objeto, y la causa del mismo sea válida.[11]

[10] Son muy diversas las definiciones que se han realizado sobre los "smart contracts", en función de la perspectiva civil-mercantil, matemática o informática que se tome en consideración. Tratamos de sistematizar las siguientes:

El creador del término, NICK SZABO, en la obra Smart Contract, Building Blocks for Digital Markets, 1996, concibió el "smart contract" como "a set of promises, specified in digital form, including protocols within which the parties perform on these promises", inspirándose en el sencillo ejemplo de la máquina expendedora que, de forma automática, y sin la intervención del hombre, ejecuta la prestación consistente en la entrega del producto adquirido al comprador previa comprobación de la inserción de una moneda de curso legal por el precio convenido.

El mismo autor, en el White Paper llamado "Smart Contracts: 12 Uses Cases for Business and beyond. A technology, legal and Regulatory Introduction", from the Smart Contracts Alliance, Chamber of Digital Commerce, december 2016, p.8, (traducción propia de la autora) añade que los principales rasgos característicos son: a) Un conjunto de obligaciones, que pueden tener naturaleza contractual o extracontractual. b) Las obligaciones adquieren un formato digital a través del softawe que las transforma en código. c) Un Protocolo informático con forma de algoritmo constituye el conjunto de reglas por el que cada parte debería procesar los datos respecto al smart contract. d) Se puede ejecutar automáticamente y es irrevocable, por cuanto no es posible detener el cumplimiento del código.

De especial interés es la defincón otorgada por la Chamber of Digital Commerce de USA, que en la página web www.digitalchamber.org señala que "smart contracts are computer code progammed to execute transactions based on pre-defined conditions. These can be dimple, automated bill pay arrangements, for exemple".

[11] En este sentido, conviene traer a colación la distinción que efectúa TUR FAÚNDEZ, C.E., Smart Contracts. Análisis jurídico, Ed. Reus, Madrid, 2018, pp. 139 a 141 entre dos categorías; la de mero "smart contract" carente de cualquier valor jurídico, que define como "secuencias de códigos y datos que se almacenan en una determinada dirección de una concreta cadena de bloques", y la de "contratos legales inteligentes", como contratos electrónicos celebrados a través de una página web accesible para las partes (o una aplicación móvil) cuya forma está constituida por la interfaz de usuario de la aplicación externa y uno o varios programas autoejecutables (smart contracts) residentes en la cadena de bloques con capacidad para inteactuar recíprocamente y con dicha interfaz".

El régimen jurídico aplicable a los "*smart contracts*" para que sean verdaderos negocios jurídicos se halla, asimismo, en el artículo 23 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información, y de Comercio Electrónico, y, en su caso, en la normativa que tutela los derechos del consumidor o adherente, ya sea la Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación, o la Ley General para la Defensa de Consumidores y Usuarios aprobada por RDL 1/2007, de 16 de noviembre. Salvo en algunos negocios concretos, rige el principio de libertad de forma, por lo que ninguna exigencia se requiere para que el contrato plasmado en formato digital obligue a las partes siempre que concurran los restantes presupuestos.

Ahora bien, habida cuenta la necesidad de que el "*smart contract*" sea automáticamente ejecutable por un dispositivo tecnológico, resultará esencial a los fines negociales no sólo el empleo de un particular lenguaje comprensible en términos informáticos, sino también el elemento técnico que permita ejecutar la función que le es propia.

En este ámbito, conviene analizar cuáles son las distintas fases de desarrollo del "*smart contract*"[12], así como las fuentes y medios probatorios disponibles al efecto de acreditar el contenido de derechos y obligaciones asumidos por los contatantes.

[12] Las fases de gestación de este tipo de contratos suelen ser las siguientes:
1.- Especificaciones o Toma de Requisitos. Necesidades que demanda el cliente para que le sean cubierta, y que el desarrollador debe reflejar perfectamente detalladas en un documento de Toma de Requisitos.
2.- Análisis. Valoración técnica y económica del alcance definido en el paso 1 o "Toma de Requisitos".
3.- Funcionalidades o Alcance. Características o alcance que cubre el sistema informático, además de las características técnicas necesarias (arquitectura, comunicaciones, interfaces), proporcionadas en soporte electrónico y en papel por el Desarrollador juntamente con el programa informático.
4.- Desarrollo. Construcción del software en diversos programas informáticos, detallando el lenguaje utilizado en cada momento, la arquitectura del mismo, etc. Este desarrollo se entregará, una vez finalizado, con las pruebas unitarias de sistema, interfaces, o de rendimiento.
5.- Certificación. Período de tiempo o etapa en la que el cliente ve el software desarrollado, realizando unas pruebas, demostraciones y revisiones conjuntas en un entorno de certificación del desarrollador.
6.- Errores. Fallos y deficiencias en el programa que impiden parcial o totalmente su utilización, o que no permiten realizar todas las funcionalidades específicas, por lo que el Desarrollador se compromete a subsanarlos. Puede surgir durante la Certificación, o durante la Producción.
7.- Aceptación. Aceptación y conformidad por escrito del cliente, con el desarrollo entregado y certificado, para proceder a su implantación.
8.- Implantación. Entrega de la versión (proporcionada en soporte electrónico y en papel) tanto del software desarrollado, como de los manuales de uso y explotación. Incluye la instalación de este software en el entorno de producción y en los componentes hardware necesario, así como la formación al usuario.
9.- Actualizaciones. Nueva versión del programa que, o bien corrija errores en el programa informático, o bien incorpore nuevas mejoras (de funcionalidad o rendimiento) a las definidas en las especificaciones iniciales, amparado bajo las obligaciones del desarrollador en el presente contrato.
10.- Migración de datos al programa informático. Los datos del actual aplicativo utilizado por el cliente, serán migrados o cargados, a la nueva aplicación o sistema informático.
11.- Soporte usuario. El desarrollador dará servicio al cliente y al usuario para consultas, o formación procedimientos de trabajo posteriores a la implantación.
12.- Explotación del sistema. El desarrollador realizará la explotación (monitorización de caídas, mejorías rendimiento, o administración interna.), posteriores a la implantación.

5.3. Las fases de formación del contenido negocial[13].

a) Fase de negociación del contrato y codificación del mismo.

El primer aspecto esencial es la determinación de la identidad de los sujetos contratantes. En la contratación digital o electrónica, se denomina "*acto de autenticación*" al mecanismo por el que una persona física concreta revela la creación de su correspondiente identidad digital, y "*acto de verificación*", el mecanismo por el que los restantes usuarios lo reconocen como tal.

Al operar en la cadena de bloques, el usuario puede obtener la denominada "*identidad soberana*", en la que voluntariamente asocia datos personales, como su nombre apellidos, o DNI, con su identidad, a través de un sistema de "*atestación*", en el que un tercero de confianza, como pudiera ser un Notario, otorga fe de la existencia de pruebas que evidencian la correlación entre el usuario físico y el usuario digital.

Según el *Reglamento e-IDAS nº 910/2014, de 23 de julio de 2014, del Parlamento Europeo y del Consejo*, relativo a la identificación electrónica y los terceros de confianza, existen tres niveles de confianza en la contatación electrónica; bajo, sustancial y alto, lo que vendrá determinado por factores de autenticación de posesión, de conocimiento o personales[14].

Por tanto, el profesional encargado de diseñar esta primera fase negocial deberá asegurar la correcta correlación de la parte contratante con el usuario digital, bien mediante la remisión a un tercero de confianza, bien mediante el empleo de los mecanismos criptográficos disponibles al efecto.

En un segundo estadio, las partes deben negociar el contenido del contrato, identificando cada una de las prestaciones, y consintiendo expresamente las mismas. En un ejemplo de contrato de compraventa de determinadas acciones sólo si la cotización de las mismas en un mercado secundario oficial

[13] Basándonos en el esquema desarrollado en el White Paper "Smart Contracts: 12 Uses Cases for Business and beyond. A technology, legal and Regulatory Introdiction", Smart Contracts Alliance, Chamber of Digital Commerce, December 2016, p. 12, existen seis fases en la creación de un smart contract:

(1) Las partes muestran la voluntad de alcanzar un acuerdo.
(2) Determinación de las condiciones del contrato, por las partes, o a partir de un hecho externo.
(3) Se escribe el código informático que poermiriá la ejecución automática cuando sucedan los hechos previstos en el mismo.
(4) Cada una de las transacciones se encripta mediante sistemas de autenticación y verificación seguros en la cadena de bloques.
(5) Ejecución y procesamiento: cada una de las transacciones registrada en el bloque se verifica por el sistema de consenso, ejecutándose automáticamente la prestación.
(6) Ejecutada la prestación, todos los nodos del sistema la reconocen como tal, siendo inalterable en la cadena de bloques.

[14] GALLEGO FERNÁNDEZ, L.A., "Cadenas de bloques y registros de derechos", en "Revista Crítica de Derecho Inmobiliario", nº 765, págs. 97 a 141: "Para asegurar que el mensaje es auténtico e íntegro, es decir, para acreditar la identidad del remitente y que el mensaje enviado no ha sido modi ficado, se utilizan técnicas de firma electrónica mediante criptografía asimétrica o criptografía de dos claves. Para ello, las aplicaciones cliente generan pares de claves criptográficas compuestos, cada uno de ellos, por una clave pública y una clave privada, las cuales no son independientes, sino que se encuentran ligadas matemáticamente. Las claves públicas son cadenas alfanuméricas de 26 a 35 caracteres que comienzan por un '1' o un '3'.

supera el valor X, las partes deberían prever la obligatoria transmisión de la titularidad de la mismas del usuario A a B sólo en el supuesto de que su valor supere la cantidad X, transfiriendo la cantidad Y desde el monedero del sujeto B al sujeto A, en el plazo negocial establecido.

Surgen en este ámbito dos cuestiones esenciales. La primera de ella, es la necesidad de garantizar la correcta traducción del contenido del contrato redactado en lenguaje natural, al lenguaje o código máquina, labor correspondiente al programador. En la órbita de responsabilidad del programador del software se incardina la correcta transformación de cada una de las secuencias contractuales del lenguaje humano al rígido código máquina.

Sin embargo, hay que destacar que cualquier discrepancia entre el contenido de la voluntad negocial libremente pactado y las secuencias efectivamente reflejadas en el "código" por el programador, puede derivar, bien de un error de programación, bien de las limitaciones intrínsecas del "software" para contemplar matices en la realización de las prestaciones que a posteriori se revelen mprescindibles, lo que deberá ser objeto de análisis en cada caso concreto.[15]

Cualquier actividad probatoria exigira la aportación por la parte *in bonis* de los términos literales del contrato suscrito, así como la traducción del código máquina al lenguaje humano. Ello permitirá al juez analizar la eventual imposibilidad de prever, bien órdenes de secuencias distintas a las contempladas, aptas para dar entrada a dichos matices, bien la rigidez del lenguaje de programación. La prueba pericial informática resulta la más conveniente por su evidente carácter técnico.

La segunda cuestión esencial es la necesidad de que el técnico asegure que las prestaciones programadas van a ser objeto de ejecución automatizada siempre que tenga lugar el supuesto de hecho predeterminado.

En la medida en que resulta imposible prever de forma anticipada en qué concreto momento tendrá lugar este hecho incierto, en ocasiones se plantea la necesidad de acudir a una fuente externa que provea dicha información.

El elemento externo apto para proporcionar a los nodos datos relevantes para la ejecución del programa recibe la denominación de "*oráculo*", siendo su función insertar en la cadena de bloques la información relevante de forma segura, disponible, e inmutable para todos los nodos implicados.

Además, el oráculo podría servirse del "*internet de las cosas*" para la correcta ejecución de los términos negociales, lo que en el futuro inmediato conducirá asimismo al norma empleo de técnicas de inteligencia artificial.

[15] Piénsese, por ejemplo, en la cláusula que en un lenguaje natural obliga a devolver el vehículo prestado en leasing "en perfecto estado". Si el arrendatario entrega la cosa al arrendador, la máquina puede interpretar que tratándose del mismo objeto, la prestación ha sido satisfactoriamente cumplida. Sin embargo, si una de las ruedas está pinchada, o contiene un rasguño, el sistema será incapaz de modular el grado de cumplimiento de la obligación contraída. Y en este caso, sería muy discutible la responsabilidad del porgramador que objetivamente ha trasladado al código máquina la cláusula redactada en lenguaje natural.

Así, en un ejemplo de conducción de un vehículo "inteligente", el programador puede implementar un dispositivo que permita al vehículo detenerse automáticamente en caso de que observe algún obstáculo en un radio cercano (información que proporcionará el oráculo a través de un radar interactivo mediante el uso de la tecnología "*internet of things*"), correspondiendo a dicho técnico la debida programación coordinada de dichos elementos, en la forma solicitada por las partes, y aportando conocimientos que sólo a él competen.

En dicho contexto, la prueba de cualquier defecto en la coordinación de los dispositivos, a partir de un dictamen pericial informático bastaría como indicio relevante para invertir la carga de la prueba. Sería en este caso la parte contraria quien debería acreditar que, pese al defecto en la codificación el daño fue causado por otros motivos.

b) Fase de ejecución del contenido negocial.

El correcto registro en la cadena de bloques del "*software*" que codifica los términos negociales permitirá que, verificado el supuesto de hecho que las partes han previsto, el sistema ejecute garantice de forma automatizada el cumplimiento de la obligación[16].

En el ejemplo que analizamos, el "oráculo" verificará que en el día indicado se ha producido la cotización en la Bolsa de Madrid de las acciones del contratante A por encima del valor X, lo que automáticamnete supondrá la transmisión de la titularidad de las mismas al contratante B, y la salida del precio desde el monedero o "*wallet*" del adquirente Sr. B al vendedor Sr. A. Estas transacciones quedarán registradas en la cadena de bloques, de forma que todos los nodos podrán comprobar los sucesos indicados, y validar la transacción mediante el sistema de consenso o mayorías ya expuesto.

Sin embargo, diversos hechos pueden tener lugar en la fase de ejecución de las prestaciones.

El primero de ellos es que exista un error durante la fase de ejecución del código cuya causa sea una deficiente traslación de los términos negociales al lenguaje máquina escogido. Imaginemos que la transferencia del dinero desde el monedero del comprador Sr. B no se realiza al transmitente de las acciones Sr. A sino a un tercero, que recibe en su cuenta el ingreso del precio estipulado. En este caso, el código ha sido correctamente ejecutado por el sistema tal y como fue programado, siendo la causa del defecto un error en la tarea del programador.

En este caso, la responsabilidad del programador frente al titular de las acciones Sr. A puede ser de tipo contractual, si ha negociado directamente el

[16] Como destaca FELIU R, J. ob cit., p. 16, "(...) cualquier operación llevada a cabo es inmodificable, potencialmente ireeversible (absoluta certeza sobre el cumplimiento de la obligación) e imparable (la imposibilidad para intervenir en los términos establecidos una vez formalizado en la plataforma).

contrato de obra consistente en la programación del smart contract, bien con un tercero, que le ha subcontratado.

La prueba del daño causado consistente en la privación del precio producto de la venta de las acciones queda acreditado a través de la propia veracidad que otorga el sistema *blockchain*, per se inmutable e inmodificable, al verificar la transmisión del dinero al Sr. C.

Por tanto, la prueba del error en la programación puede ser el aspecto más controvertido. En el supuesto de haber celebrado las partes un previo documento privado que recoja en lenguaje natural las obligaciones de cada parte, será éste la fuente probatoria principal, por cuanto la propia literalidad en sus términos no dejará lugar a dudas.

En otro caso, la prueba pericial será el mecanismo apto para probar cómo debió realizarse la programación a los fines de evitar el error detectado, esto es, la debida *lex artis*.

La segunda posibilidad es que se produzca una circunstancia sobrevenida e imprevista. Imaginemos que la Bolsa de Madrid sufre un error en el suministro de los datos y registra una cotización de las acciones por encima del valor X cuando ésta realmente nunca se ha producido. El sistema verificará que se ha dado el supuesto de hecho previsto a través del oráculo, lo que provocará que la máquina dé cumplimiento a la instrucción del "*smart contract*" transfiriendo el importe pactado desde el monedero del Sr. B al Sr. A.

En este caso, el oráculo ha proprocionado una información errónea, si bien dicho error no pertenece a la esfera de responsabilidad del programador, en la medida en que el oráculo siempre actúa como fuente externa independiente, ajena a su control.

El único mecanismo de responsabilidad se producirá si las partes le han conminado a prever una cláusula que permita al código revertir la ejecución de la trsnacción ante un supuesto de esta naturaleza, extremo que nuevamente dependerá del tenor literal del contrato pactado en lenguaje natural.

c) Fase de "resarcimiento" en caso de incumplimiento.

La cualidad inherente al *smart contract* consistente en el automatismo en la ejecución de las prestaciones previamente programadas exige un esfuerzo adicional para resolver cómo es posible resarcir al contratante que observa cómo el dispositivo tecnológico ejecuta la prestación en estricto cumplimiento de las secuencias codificadas a pesar de que se ha producido alguna infracción relevante que produce, bien su nulidad por falta de consentimiento, objeto y causa, bien su incumplimiento, por error imputable al prograamdor.

Ante la dificultad de interrumpir el cumplimiento del contrato inteligente, surge la necesidad de incluir un código técnico adicional en el "*smart contract*" que deje sin efecto el anterior ante un supuesto de urgencia, llamado por ese motivo "*código rojo*" o "*código suicida*".

Otra posibilidad exigiría modular el sistema de consenso de los nodos en la "*blockchain*", introduciendo restricciones a partir de "*sistemas de plataforma de blockchain privada*", capaces de identificar a los nodos cualificados para revertir instrucciones ejecutadas, lo que resulta prácticamente imposible en los sistemas estrictamente descentralizados.

Se abre, así, una vía para garantizar la reversibilidad de la operación ante supuestos de error en la codificación o concurrencia de circunstancias imprevisibles.

Por tanto, la última esfera para eludir un eventual régimen de responsabilidad atañe a la diligencia en el momento de prever la incorporación de dichos mecanismos técnicos al sistema diseñado, y ello a los efectos de asegurar, bien la posibilidad de dar cumplimiento al contrato en sus exactos términos, bien la resolución del mismo y correspondiente restitución de efectos.

Una sugerencia a los efectos de solventar dicha problemática sería constituir al juez en el "*Oráculo decisor*", especialmente en el urgente régimen de medidas cautelares, a modo de tercero de confianza idóneo para confirmar el hecho base de cada prestación con carácter previo a que el sistema ejecute la orden, garantizando el debido cumplimiento de las obligaciones asumidas por cada parte contractual, pero también salvaguardando los fallos técnicos del sistema.