FACULTAD DE DERECHO

PROBLEMAS CON LA EJECUCIÓN DE LOS LEGAL SMART CONTRACTS

Autor: Paloma del Río Castillo
5º E3 D
Derecho Mercantil
Tutor: Javier Wenceslao Ibáñez Jiménez

Madrid

Junio 2019

ÍNDICE

LISTA DE ABREVIATURAS

B2C – Business to Consumer

BFT- Bizantine-fault tolerant

DAO – Decentralized Autonomous Organization

DLT - Distributed Ledger Technology

DO – Decentralized Organization

EE.UU. – Estados Unidos

ESMA – European Securities and Markets Authority

GDPR – General Data Protection Regulation

IA – Inteligencia Artificial

ITU- International Telecommunication Union

ISO/TC 307 - International Organization for Standardization Technical Committee 307

LSSI - Ley de Servicios de la Sociedad de la Información y de comercio electrónico

PoW – Proof of Work

SPOF – Single Point of Failure

UE – Unión Europea

1. Introducción

En los últimos años hemos podido observar el auge de nuevas tecnologías que han transformado la forma que tienen tanto las empresas como los consumidores de operar en el tráfico jurídico. Entre ellas destaca la tecnología de registro distribuido o *DLT,* tecnología que ha permitido en los últimos años el desarrollo de aplicaciones muy diversas, desde la creación e intercambio de *bitcoin* y otras criptomonedas, hasta el uso de los *smart contracts*. Ante todas estas innovaciones tecnológicas los operadores jurídicos se han mantenido atentos, pero de momento no se han promulgado grandes paquetes regulatorios que determinen el sentido que tendrá dicha normativa o incluso si esta existirá en el futuro.

La autorregulación de las nuevas tecnologías se encuentra condicionada por sus características durante el desarrollo tecnológico y a su vez existe un silencio normativo por parte del poder legislativo. Ante la ausencia de estas normas, el objetivo de este trabajo es establecer el funcionamiento básico desde el punto de vista jurídico que tienen los *smart contracts* y los principales problemas que plantea su uso en la actualidad. Con el fin de dotar a este trabajo de una mayor coherencia, primero tenemos que entender el funcionamiento de la tecnología *DLT* en general, para poder posteriormente centrarnos en un mejor análisis de los *smart contracts.* Una vez analizado el funcionamiento y características de los *smart contracts,* podremos abordar los problemas jurídicos que estos pueden plantear, así como los posibles remedios a dichos retos, atendiendo a los intereses que se quieran proteger. Debido a esto empezaremos analizando la tecnología *DLT*, sus ventajas y amenazas. A continuación, nos centraremos en estudiar: el funcionamiento de los *legal smart contracts,* los instrumentos a los que estos acuden para su ejecución, es decir los oráculos, las denominadas *DAOs* y la integración legal que estos poseen en el contexto UE en la actualidad. La cuarta parte del trabajo se centrará en los problemas que plantea la ejecución de los *legal smart contracts,* debido a las características que estos poseen. A continuación, se expondrán los posibles remedios que proponen expertos legales para remediar los retos que la ejecución de los *legal smart contracts* plantea. Finalmente se realizará un resumen de las principales conclusiones que se derivan del trabajo. La bibliografía será la última parte del trabajo e incluirá las obras doctrinales y fuentes legales consultadas.

Los *legal smart contracts* se encuentran aún en una fase muy temprana de su desarrollo, pero si se les consiguiera dotar de una mayor seguridad jurídica, sin perder la gran ventaja que otorgan en términos de eficiencia, su implantación podría ser mayor en los próximos años.

2. Tecnología *DLT*: *Blockchain*

La tecnología *blockchain* consiste en el uso de un registro distribuido y descentralizado para la verificación y registro de transacciones[1]. Dicha tecnología facilita el envío, recepción y registro de información, por medio de una red entre iguales (*peer-to-peer*).

Originalmente la red *blockchain* se creó con el fin de facilitar la ejecución y el registro de operaciones realizadas con criptomoneda *bitcoin.* La red *blockchain* facilita este fin al operar como una infraestructura tecnológica adecuada y como base de datos.

Con carácter previo al uso de redes *blockchain,* no era posible realizar operaciones entre usuarios de internet sin que mediase un tercero que dotase de confianza a estas transacciones. Muchos críticos de la tecnología de registro distribuido se apoyaban en el denominado "problema de los generales bizantinos", argumentando que no era posible que estas redes funcionasen sin que existiera una autoridad central, superior al resto de nodos o usuarios[2]. Una red DLT resuelve este problema técnico al exigir que la información transmitida a todos sus usuarios formule problemas matemáticos que requieren un alto poder computacional para su adecuada resolución. De esta forma se ponen mayores dificultades a potenciales hackers, ya que, para introducir información falsa y corromper la red, se ha de tener un alto porcentaje (mayoría) del poder computacional de la red.

Otro problema técnico, aunque con repercusión normativa, al que se enfrentan las redes *blockchain* es el control y bloqueo de aquellas transacciones que son ilegítimas, evitando su registro. Para comprobar esto, la red verifica que la transacción es válida por medio de un proceso de minado, esto es, que los *miners* van a desarrollar un trabajo computacional muy exigente para validar cada bloque, controlando que no invalide transacciones ya aceptadas y registradas. Solamente se registrarán en un bloque al final de la cadena de

[1] Kakavand, H., Kost De Sevres, N. y Chilton, B. (2017), *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*.

[2] Wright, A. y De Filippi, P. (2015), *Decentralized Blockchain Technology and the Rise of Lex Cryptographia.* Dicho problema plantea que tres divisiones del ejercito bizantino se encuentran acampadas a las puertas de una ciudad con el objetivo de conquistarla. Los generales de estas tres divisiones solo se pueden comunicar entre sí, para acordar la mejor estrategia de ataque, acudiendo a mensajeros. Sin embargo, cualquiera de ellos podría ser un traidor e intentar dar mensajes erróneos al resto de generales, o incluso que los traidores fueran los mensajeros. Si no existe una autoridad central con más peso, que dé la orden y proporcione la información de manera adecuada, el ataque no tendrá éxito.

bloques, cuando los nodos de la red acuerden de forma unánime la validez de la transacción. Al consenso para incluir la nueva transacción se puede llegar a través de diversos mecanismos de votación, entre ellos uno muy común es el *Proof of Work* (*PoW*).

La característica más relevante de esta tecnología es el carácter indeleble que tienen las operaciones ya validadas e incluidas en la red de bloques. Todos los nodos de esa red pueden ver los datos de la operación y realizar nuevas operaciones que se añadan a este u otros bloques.

Blockchain es un tipo de tecnología de registro distribuido (denominada *DLT* o *Distributed Ledger Technology*). La *DLT* proporciona a sus usuarios la habilidad de acceder a una plataforma con información sobre transacciones en una base de datos compartida y común, que no requiere la intervención de un sistema de validación central para operar correctamente[3]. Cada red *DLT* ha de establecer sus propias normas y procesos, para operar correctamente. Este tipo de redes se diferencia de otras redes de registro en que las transacciones producidas a través de ella no son validadas por una autoridad central, sino que obtienen su validez al ser aprobadas por un conjunto de usuarios distintos, distribuidos en la red (nodos validadores). Una segunda particularidad que encontramos en las redes *DLT* es el uso de codificación criptográfica como medio para almacenar activos y validar transacciones[4]. Las redes *DLT* en resumen reducen significativamente la necesaria intervención de intermediarios que doten de confianza a los mercados en los que se producen operaciones comerciales entre dos o más partes. Debido a esto, uno de los ámbitos que puede verse afectado por esta tecnología es el sector financiero, ya que se reduciría el número de intermediarios (ej. bancos y brókeres).

En términos generales una *blockchain* es una plataforma digital que registra y verifica el historial de transacciones entre sus usuarios, de forma que no se puede manipular ni alterar dicho registro de datos. Las transacciones entre usuarios se codifican mediante algoritmos que verifican el contenido y son agrupadas en bloques. Una vez codificado el bloque se envía a cada uno de los nodos validadores de la red. Cada bloque es verificado por los nodos validadores de la red y se añade a la *blockchain*. Dichos bloques se unen los unos a los otros de forma que se vuelven inalterables y debido a todo este proceso, a

[3] ESMA. (2016*), Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets*.
[4] Kakavand, H., Kost De Sevres, N. y Chilton, B. (2017), *The Blockchain Revolution*…op. cit, pp.6.

estas redes se las denomina redes de cadena de bloques/*blockchains.* La red *blockchain* que contiene las cadenas de bloques se sincroniza automáticamente en todos los nodos, que son iguales entre sí, de forma que no se requiere que un intermediario proporcione confianza al sistema, al tener todos ellos acceso a todas las operaciones contenidas en la red y los detalles sobre las mismas. Gracias al uso de esta tecnología, partes independientes y desconocidas pueden llegar a realizar operaciones entre sí en la red, sin necesidad de acudir a un tercero independiente para que conozca y autorice la transacción y sus características.

El proceso por el que nuevas transacciones se "insertan" en una red *blockchain* consta de varios pasos. En primer lugar, las partes intervinientes en el acuerdo han de ser usuarios de la red *blockchain* elegida por ellas. El acuerdo que alcancen dichas partes, normalmente se dará en formato de lenguaje ordinario, por lo que será necesaria su codificación, para su inserción en la red. En tercer lugar, una vez codificado el acuerdo, se emitirá el código a la red elegida. Antes de incorporarse a otros acuerdos que ya se encuentran en la red, el acuerdo se habrá de validar por parte de los nodos que operan en la red, también denominados nodos validadores. A continuación, se producirá la unión del acuerdo a otros ya existentes en la red, para formar un bloque juntos a estos. Finalmente, se dará la unión del bloque, que está compuesto por numerosos acuerdos, a otros bloques, formándose así la cadena de bloques.

Cada bloque puede contener una o varias transacciones y en él quedarán registradas la hora y las transacciones que se ajusten a las normas de la red en la que se opere. Cada bloque contiene una huella digital (*hash*) de las transacciones que en él se acumulan y también contendrá el *hash* del bloque anterior, de manera que será imposible alterar dicho bloque o introducir uno nuevo entre los dos bloques, perfeccionándose así la característica de la inmutabilidad de las redes *blockchain*.

El uso de las cadenas de bloques conlleva tres rasgos principales. En primer lugar, el consenso, ya que para que una operación quede registrada correctamente en la red se requiere que todos los participantes de dicha red estén de acuerdo. En segundo lugar, el registro, dado que las redes *blockchain* facilitan que sean observables tanto los cambios de titularidad de los activos registrados en la red, como el momento de registro de los mismos en la red *DLT*. En tercer lugar, el rasgo más destacable de la cadena de bloques

es la inmutabilidad de lo establecido en ella, que no podrá ser manipulado por las partes ni por terceros, desde el momento de su registro y validación[5].

Las transacciones no se registran de manera completa en los bloques de la red, sino que, a través de la denominada *Proof of Existence*, servicio que facilita que se incorpore únicamente a la cadena la huella digital de la transacción, no resulta necesario volcar todo el contenido del acuerdo. No se puede introducir en los bloques de la *blockchain* todo el contenido del acuerdo que funda la transacción, sino que se incorporará únicamente la huella digital original (*hash*). En principio las redes *DLT* no permiten registrar estos ficheros con los acuerdos completos en sus bloques y, aunque lo permitieran, el tamaño de los archivos dispararía los costes de operar en ellas (costes de almacenamiento). Servicios que se dan en redes *blockchain*, como *Proof of Existence,* aumentan el nivel de inmutabilidad de la red ya que, al contener el *hash,* ni las partes ni terceros ajenos a la transacción podrán modificarla y, además, se podrá comprobar que la transacción sigue siendo la originalmente establecida, ya que cualquiera podrá aplicar el *hash* y comprobar si la función alfanumérica que posee coincide con la original o no.

A continuación, distinguimos entre redes *blockchain* públicas o privadas, o lo que es lo mismo, redes no permisionadas o permisionadas. Las redes públicas o no permisionadas son aquellas a las que cualquiera puede acceder, operar en ellas y visualizar todos los datos de las operaciones producidas en ella, ya que, aunque estos datos sean anónimos, serán públicos. Entre estas redes no permisionadas destacamos algunas como son: *Bitcoin, Etherum, Litecoin o Dash*. El resto de redes *blockchain* son las privadas o permisionadas; en estas redes los usuarios han de ser invitados para poder operar en ellas. Esto ocurre en redes como *R3* o *Hyperledger*. Los participantes de la red tienen el privilegio de aceptar o no a nuevos participantes y en ellas no existe el anonimato, sino que todos los participantes conocen la identidad del resto. Dependiendo de la red privada, el nivel de acuerdo para que se produzca la entrada de nuevos usuarios varía, pudiendo exigirse desde la unanimidad, hasta la mera invitación por parte de un único usuario de la red junto con el cumplimiento de unos requisitos predeterminados.

[5] Faúndez, C. T. (2018), *Smart contracts: análisis jurídico*.

2.1 Peligros del uso de redes DLT

Podemos agrupar en cuatro grupos distintos los riesgos que pueden surgir en el uso de redes *DLT*[6].

En primer lugar, existen riesgos como el ciberriesgo, riesgo de fraude y el de blanqueo de capitales. En el caso de un ciberataque, al almacenarse la información de la *blockchain* en cadenas de bloques, si se consigue acceder a una información determinada, se tendrá acceso a todas las que compartan su naturaleza y estén almacenadas conjuntamente. Incluso si se llegase a dar el caso de que la técnica de encriptación empleada sufriera un ciberataque, al ser todas las redes *DLT* parecidas en este aspecto, habría riesgo de contagio a todas ellas. Las claves privadas o públicas de los usuarios podrían robarse y usarse de manera fraudulenta para realizar transacciones, sin que concurra la voluntad del usuario afectado. Además, a través de redes *DLT,* al no emplear sistemas de control estrictos, los usuarios pueden ocultar su identidad, así como su historial de transacciones y, de esta forma, blanquear capitales o financiar actividades terroristas.

Otra categoría de riesgo que encontramos son los riesgos derivados del automatismo de las redes *DLT*. Si bien es cierto que al ejecutarse automáticamente las transacciones en redes *DLT* se evitan errores humanos, la pérdida de control humano, una vez introducido el código necesario para la producción de las operaciones, puede dejar a las partes en una situación de indefensión. En resumen, gracias a la tecnología *DLT* los errores pueden reducirse, pero su impacto podría ser mayor en caso de que se produjesen.

Podrían producirse situaciones de desigualdad competitiva, ya que una red *DLT* podría imponer a determinados potenciales usuarios condiciones económicas o de otro tipo que resulten inviables para poder acceder a su red, creándose con el tiempo un monopolio con consecuencias negativas en el precio y en la calidad del servicio.

En el corto plazo existe el riesgo de que la complejidad de las operaciones aumente, ya que los datos encriptados son más complejos de supervisar y controlar. Aunque en principio el uso de estas redes sirva para visualizar claramente las transacciones producidas y su historial, al encriptar dicha información, se va a requerir un proceso complejo de desencriptación, que retrasará a su vez el proceso de supervisión.

[6] ESMA. (2016), *Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets*.

Pese a todos estos peligros que observa el *ESMA* (*European Securities and Markets Authority*), son numerosos los usos y ventajas de la tecnología *blockchain*. Entre estos usos destacan: la creación de un mercado monetario de criptomonedas, el uso de *smart contracts* de ejecución automática y los sistemas de voto ciberseguros.

2.2 Redes permisionadas

Hemos mencionado en el apartado dos de este trabajo las diferencias entre redes permisionadas y redes no permisionadas. Sin embargo, debido a que los *legal smart contracts* solo se pueden desarrollar en redes públicas y permisionadas, detallamos a continuación las principales características de este tipo de redes *DLT* y las formas por las que se obtiene el consenso en ellas.

En redes *DLT* públicas o no permisionadas, cualquiera que desee ser usuario de las mismas podrá serlo, sin tener que cumplir una serie de requisitos referidos a su identidad. Este tipo de redes normalmente vinculan su funcionamiento a una criptomoneda y se sirven del consenso basado en el *Proof of Work* (*PoW*). El uso de *PoW* es relevante ya que son los usuarios los encargados de verificar las transacciones contenidas en la red y no los *miners*. Dichos *miners* se limitan en estas redes a asegurar la fortaleza e incorruptibilidad de la cadena de bloques, labor que requiere un alto nivel de poder computacional. Los usuarios de la red son los encargados de verificar el contenido de nuevas transacciones que se incorporarán o no en los bloques de la cadena. Para realizar esta labor los usuarios de la red requieren cierto poder computacional, pero dicho poder será menor que el que requieran los *miners* para poder dotar de una mayor seguridad a la cadena de bloques, por ello se les delega la tarea de la verificación. En redes no permisionadas, en las que se utiliza el sistema *PoW*, el nivel de seguridad de la cadena de bloques será proporcional al nivel de poder computacional que le dediquen los *miners*[7]. Ejemplos de este tipo de redes serían *Bitcoin* o *Litecoin*.

Las redes permisionadas operan entre usuarios cuya identidad es conocida por el resto. Estas redes permiten a sus participantes interactuar, aunque no confíen ciegamente los unos en los otros, pero existan intereses comunes entre ellos. La principal diferencia que

[7] Catalini, C. y Gans, J.S. (2019), *Some Simple Economics of the Blockchain*.

encontramos entre este tipo de redes y las no permisionadas es que el acceso a estas es restringido. En redes permisionadas los usuarios han de decidir quién tiene acceso a dichas redes y quien puede validar las transacciones que se registren en ella. Existen diversas formas de alcanzar el consenso en este tipo de redes, entre ellas destacamos el *Bizantine-fault tolerant* (*BFT*) consenso[8] o el consenso Nakamoto.

Las redes permisionadas son más eficientes que las no permisionadas, ya que solo los nodos designados para esa labor serán los encargados de validar las transacciones, evitándose así trabajo computacional redundante, que sí se produce en las redes no permisionadas. Otra característica de las redes permisionadas es que poseen un órgano de gobierno y una estructura clara, que facilita enormemente la toma de decisiones, en caso de problemas con la *blockchain*. Existen redes como Alastria que denominamos públicas y permisionadas. Esto se debe a que no está vinculada o tiene como objeto principal el movimiento de una criptodivisa (característica de redes no permisionadas), pero sí tiene un número mayor que otras redes permisionadas de nodos validadores, dotándole de una mayor seguridad. En concreto esta red utiliza como sistema de validación de las transacciones producidas en ella el Istanbul Byzantine-Fault Tolerant (IBFT), que es un sistema similar al BFT pero con modificaciones. En este sistema se requiera varias rondas de votaciones para poder validar un bloque. Cada nodo validador decide si valida o no atendiendo a sus criterios computacionales, es independiente, sin basarse en los de un líder o nodo validador anterior.

3. Smart contracts

En 1994, Nick Szabo ya acuñó un concepto de *smart contract*. Szabo afirmó que son un conjunto de promesas, establecidas en formato digital, que mediante un mecanismo/protocolo digital se ejecutan.

Los *smart contracts* son transacciones o contratos que se someten a un proceso de codificación para su agilización, ejecución y cumplimiento en una red *blockchain* de

[8] Androulaki, E., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., … Laventman, G. (2018), *Hyperledger fabric: a distributing operating system for permissioned blockchains.*

acuerdos comerciales entre dos o más partes[9]. De acuerdo con la *International Telecommunications Union* (*ITU*) son contratos cuyos términos son registrados en código compatible con la *blockchain* y cuya ejecución es automática[10]. Sin embargo la International Organization for Standardization Technical Committee 307 (ISO/TC 307) los define como programa automático, registrado en una red *DLT*, que registra además el consenso alcanzado sobre los efectos de la ejecución[11]. La idea básica que subyace al uso de los *smart contract*s es el realizar automáticamente transacciones por medio de algoritmos, de manera que la propiedad de los activos quede registrada en la red *DLT* y que se puedan negociar y transferir derechos sobre los mismos entre las partes[12]. El valor añadido fundamental que proporcionan los *smart contract*s al sistema mercantil actual es la ejecución automática de los mismos[13].

Cada *smart contract* involucra el procesamiento de un conjunto de órdenes de cumplimiento automatizado, que se ejecutan cuando un agente, externo a la cadena de bloques, denominado oráculo, verifica el cumplimiento de una condición[14]. Una vez cumplida la condición, el evento digital programado se cumple automáticamente. Si el evento desencadenado por el *smart contract* produce efectos jurídicos, es entonces cuando el contrato habrá de ser estudiado desde un punto de vista legal.

La denominación *smart contracts* ha inducido a que numerosos abogados y reguladores no entiendan realmente si estos son verdaderos contratos o no. Para entender esto, primero tenemos que establecer que los *smart contracts* no son *"smart"* por dos razones: no entienden el lenguaje ordinario -solo entienden lo codificado-, y por sí mismos, en numerosas ocasiones, no pueden verificar el cumplimiento de las condiciones para su ejecución, sino que han de acudir a fuentes externas (los denominados oráculos)[10].

En segundo lugar, tenemos que entender que los denominados *smart contracts* pueden ser de dos tipos. Los *legal smart contracts* son aquellos que, a partir de un contrato jurídico preexistente en el mundo real (tanto un contrato firmado en soporte físico, como los firmados en páginas web), codifican algunas de sus disposiciones para que estas se

[9] Kakavand, H., Kost De Sevres, N. y Chilton, B. (2017), *The Blockchain Revolution*…op. cit, pp.6.
[10] ITU. (2017), *Distributed Ledger Technologies and Financial Inclusion*.
[11] ISO/TC 307. (2018), *Blockchain and distributed ledger technologies.*
[12] Goorha, P. (2018), *A Comprehensive Contracting Solution using Blockchains.*
[13] Finck, M. (2019), *Smart Contracts as a Form of Solely Automated Processing Under the GDPR*.
[14] Ibáñez Jiménez, J. W. (2018), Blockchain: Primeras cuestiones en el ordenamiento español.

ejecuten automáticamente cuando se cumplan las condiciones programadas. Por otra parte, existen los *smart contracts* que no se basan en un instrumento contractual previo del mundo real, ya que son operaciones realizadas enteramente al amparo de la *blockchain* entre sus usuarios. Este último tipo de *smart contract* permite a los usuarios pactar transacciones entre sí, sin tener que acudir a medios jurídicos como son los contratos. Son una fuente material que puede, en algunos casos, producir efectos jurídicos[15]. Los *smart contracts*, como establece Ibáñez Jiménez, son relevantes jurídicamente por ser un *modus adimpleti contractus*, es decir un modo de ejecutar un contrato[14](Ibáñez Jiménez, 2018, p. 92). Los *legal smart contracts* son contratos ordinarios, diseñados para producir efectos jurídicos, cuya peculiaridad reside principalmente en su transcripción a código informático y su carácter autoejecutable[16]. Se trata de un contrato escrito en código informático que facilita la ejecución del contenido pactado[11]. En este trabajo nos vamos a centrar en el estudio de los *legal smart contracts*.

Tenemos que distinguir los supuestos de contratación automática, en los que no existe una intervención humana y por ello la doctrina considera que no puede existir una relación contractual, de los supuestos de contratación mediante *legal smart contracts* que operan en una red *DLT*. En el caso de los *smart contracts* podemos observar la intervención humana en el momento inicial, cuando el usuario o parte contratante introduce los datos necesarios para que se ejecute el *smart contract*, dadas unas determinadas condiciones, manifestando así su voluntad de obligarse[11]. La diferencia por tanto la encontramos en que mientras que, sí puede existir un contrato con efectos jurídicos que se ejecute mediante un *smart contract*, en la contratación automática no existe un verdadero contrato, al no producirse la requerida intervención humana.

Los *smart contracts* se diferencian de los contratos ordinarios principalmente por poseer dos características muy particulares: garantía y auto ejecutoriedad. No funcionan como un sistema garante tradicional, ya que no existe un tercero independiente, ajeno a las partes, que dote de una mayor seguridad a lo establecido. Sin embargo, es cierto que garantizan el cumplimiento al no producirse el mismo hasta que las condiciones preestablecidas en el *smart contract* se cumplan. Se aumenta también la función garante

[15] Ibáñez Jiménez, J. W. (2018). *Derecho de Blockchain y de la tecnología de registros distribuidos*.
[16] Legerén-Molina, A. (2019). *Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de blockchain.*

de un *smart contract*, al retener en la *blockchain* en estado de suspensión, es decir que devienen efectivamente inutilizables los activos necesarios para que se ejecute el acuerdo, hasta que se cumpla la condición. Por otro lado, la auto ejecutoriedad de los *smart contracts* es una característica esencial de los mismos, ya que implica no solo un remedio ante la posibilidad de un incumplimiento contractual, sino la imposibilidad de producción de dicho incumplimiento, así como la prevención de los costes derivados del incumplimiento y la litigiosidad relacionada con este[17]. El proceso de auto ejecución que pone en marcha la red, una vez cumplidas las condiciones preprogramadas, remplaza la ejecución judicial que requerirían los contratos que se encuentran ante situaciones de incumplimiento[18]. La reducción de costes que supone el uso de *smart contracts* no solo se limita a la reducción de costes derivados del incumplimiento (el cual deviene imposible), sino que también se reducen los costes de agencia y de transacción, al no existir un intermediario (ej. un bróker o una entidad de contrapartida central).

Para generar un *legal smart contract,* algunas disposiciones contractuales son codificadas y subidas a la red *blockchain*, produciendo un *smart contract*, que no requiere la intervención de un tercero independiente para el registro y cumplimiento del mismo. Para que determinadas partes de los contratos que se quieren convertir en autoejecutables se puedan codificar, es necesario que las órdenes que se quieran codificar tengan una lógica booleana, es decir, que tengan la estructura *if/then/else*. Dicha estructura funciona de forma que si se cumple una condición (*if*), se ha de producir un resultado programado (*then*) y si no se produce, entonces se producirá otro resultado programado (*else*)[19].Uno de los límites a la implantación de los *smart contracts* se debe precisamente a esta necesaria estructura para su codificación, ya que no se admitirán cláusulas que requieran interpretación para ser ejecutadas. No se podrán introducir conceptos jurídicos indeterminados, muy utilizados en el ámbito jurídico, como son: buena fe, diligencia debida, caso fortuito, fuerza mayor, etc.

La principal ventaja que encontramos en el uso de los *legal smart contracts* es que no cabe la ambigüedad en los términos contractuales al utilizar un lenguaje simple para su codificación y tampoco cabe acudir a valoraciones acerca de la producción efectiva de la

[17] Ibáñez Jiménez, J. W. (2018). *Derecho de Blockchain...*op. cit, pp, 14.
[18] Werbach, K., & Cornell, N. (2017), *Contracts ex machina.*
[19] Legerén-Molina, A. (2019). *Retos jurídicos que plantea…*op. cit, pp. 14.

condición de cumplimiento. En una *blockchain*, una vez detectado el cumplimiento de las condiciones programadas, se produce la ejecución automática programada y prevista de las cláusulas contractuales. Otra ventaja considerable consiste en la longevidad e inmutabilidad de lo establecido en la red. Ninguna de las partes podrá modificar su contenido o declarar la inexistencia de contrato alguno, una vez que el mismo sea codificado e introducido en la cadena de bloques. Atendiendo a lo anterior y a la ausencia de autoridades centrales que los controlen, los *smart contracts* suponen un nuevo tipo de procedimiento contractual más rápido, sencillo y barato.

Los *legal smart contracts* serán contratos válidos para el derecho siempre que cumplan con los requisitos de consentimiento válido (oferta y aceptación), objeto cierto y causa válida[20]. A la hora de determinar si un *legal smart contract* cumple con el requisito de consentimiento de las partes que integran un acuerdo, se habrá de atender a sí las partes han otorgado efectivamente sus claves criptográficas privadas para aportar recursos o activos y comprometerse así con lo acordado. De esta forma, se comprobará la concurrencia válida de oferta y aceptación. Algunos autores como Ibáñez Jiménez asumen que existen dos voluntades distintas que han de concurrir: una sería la relativa a la propia operación buscada (ej. venta de un activo) y otra sería la del consentimiento a la ejecución automática de las consecuencias preprogramadas (Ibáñez Jiménez, 2018, p.95). Otros autores entienden que el consentimiento se da en un único acto, ya que al introducir la operación deseada con las condiciones pactadas en la red *DLT*, habría un consentimiento expreso de la operación en sí y un consentimiento tácito relativo a la auto ejecución de la misma en la *blockchain*. El problema de esto lo encontramos cuando existe un error en el contenido de lo pactado o una imprecisión o falta de compleción del mismo. Lo habitual, si no se empleasen *legal smart contracts* sería que se paralizase la ejecución y se completase o resolviese la cuestión; no obstante, con el uso de *legal smart contracts* no cabe paralizar una ejecución o acudir a una tutela judicial que complete el contenido del contrato, simplemente se dará por válido el contenido programado. Otro problema relativo al consentimiento en relación con este tipo de contratos consiste en que, mientras que en un contrato ordinario -aun cuando sus términos sean claros, completos y precisos- si una de las partes sufriera violencia o intimidación y acudiera a la tutela judicial, se le

[20] Ibáñez Jiménez, J. W. (2018). *Derecho de Blockchain...*op. cit, pp, 14.

podría excusar del cumplimiento de lo pactado, en el caso de los *smart contracts* se ejecutaría su contenido sin tener en cuenta dichas circunstancias. Aunque la mayoría de los seres humanos no seamos capaces de descifrar el código del *smart contract*, afortunadamente poseemos máquinas para poder transformarlo en lenguaje humano y salvar de esta forma el cumplimiento del requisito de consentimiento contractual informado. Es cierto que, en algunos casos, como cuando se trate de contratos con consumidores, para la validez del contrato se requeriría su plasmación en lenguaje ordinario. En caso de discrepancia entre el script y los términos del contrato en lenguaje ordinario prevalecerían estos últimos, ya que en ellos encontramos el consentimiento necesario para la ejecución.

Una de las facilidades más importantes que la tecnología *blockchain* aporta en el ámbito de los *legal smart contracts* es que no es necesaria la confianza entre los contratantes o de los contratantes hacia un tercero independiente. Los *smart contracts* son validados y ejecutados bilateralmente en la red *DLT*, sin que sea necesaria la intervención de un tercero independiente que dote de confianza las operaciones. Incluso en redes *DLT* se puede incorporar, para dotar de un mayor control al *smart contract*, una función *multi-sig*, esto es que se requiera el consentimiento de dos o más partes para que se ejecute alguna disposición del acuerdo.

Cuando la ejecución de un *legal smart contract* dependa del cumplimiento de condiciones que se encuentren fuera de la red, se utilizan los denominados oráculos para verificar y monitorizar los eventos producidos en el mundo real (ej. precio de un activo), esto será desarrollado en mayor profundidad en el apartado 3.1 del presente trabajo.

El pago, en una transacción articulada mediante un *legal smart contract*, está automatizado y esto facilita enormemente el efecto liberatorio, extintivo y satisfactivo del pago. No cabe un incumplimiento contractual del contenido codificado en un *smart contract*: la ejecución no solo la facilita el uso de *smart contracts*, sino que la hacen inevitable[21]. La inevitabilidad del cumplimiento de lo pactado y su ejecución automática puede conllevar también algunos problemas, por ejemplo, en el caso de que lo pactado

[21] Legerén-Molina, A. (2019), *Retos jurídicos que plantea…*op. cit, pp. 14.

adolezca de una nulidad absoluta por ser contrario a la ley, a la moral o al orden público, aunque en la mayoría de los casos aportará ventajas y una mayor seguridad.

El *smart contract* creado para que se produzca la ejecución automática del *legal smart contract* preexistente podrá, cuando se verifique la condición a la que se somete la ejecución, entre otras cosas: recibir fondos, cobrar automáticamente y transferir fondos, retener fondos, recibir información sobre hechos externos a la red y modificar el funcionamiento de mecanismos electrónicos exteriores interconectados con ella (encender, apagar, detener, bloquear, etc.)[22]. Haciendo uso de todas las facultades que se otorgan a estos instrumentos, los *smart contracts* podrían extenderse a sectores muy variados y distintos entre sí. Dichos contratos podrían facilitar desde transacciones financieras, hasta la ejecución automática de sucesiones o el ágil funcionamiento de sistemas de financiación colectiva[23].

Frente a todos los problemas que mencionaremos y especialmente a los dos problemas elegidos en el apartado 4 del presente trabajo, al no existir una tutela judicial efectiva anterior a la ejecución de los *smart contracts*, es previsible que las partes dediquen una mayor diligencia a la hora de elaborar mejores *legal smart contracts* para no tener que enfrentarse a problemas no previstos en el momento de la ejecución. Podrá incluso surgir un nuevo perfil de abogados se especialicen en la elaboración y tutela de este tipo de acuerdos.

Existen numerosas aplicaciones que podrían tener los *smart contracts* en diversas áreas. Entre ellas destacamos algunas como son que ante prestamos en los que un deudor incumple, se podría facilitar la pérdida automática de su acceso a los fondos prestados. Otro potencial uso sería su funcionamiento como retenedor del pago hasta que se produzca efectivamente la entrega, en el caso de las compras online. Destacamos también su potencial uso como medio para votar.

[22] Faúndez, C. T. (2018), *Smart contracts…* op. cit, pp. 9.
[23] Werbach, K., & Cornell, N. (2017), *Contracts …*op. cit, pp.15.

3.1 Los Oráculos

Un oráculo puede ser una o múltiples personas, grupos o programas que proporcionan a la red *DLT* la información que esta requiere para poder ejecutar el contenido de los bloques que la componen. Lo que facilitan los oráculos es que el *legal smart contract* contenido en la *blockchain* tenga acceso a los eventos que se producen en el mundo real[24].

Existen dos tipos de oráculos en función de cómo accedan a la información requerida, esto es, dependiendo de si la obtienen de manera automática o utilizando medios personales.

Lo oráculos de funcionamiento autónomo proporcionan la información a la red *DLT* en tres pasos. Primero, el *smart contract* establece la información que el oráculo ha de encontrar y recabar. A continuación, el oráculo busca la información en sus bases de datos. Finalmente, el oráculo proporciona al contrato la información recibida. Aquí vemos que existe diferencia entre el oráculo y la base de datos de la que se extrae la información requerida. En este caso el oráculo es meramente el que facilita o "transporta" la información requerida y no es la fuente de la misma. Dentro de esta categoría de oráculos existen dos tipos: *software* oráculos y *hardware* oráculos[17].

Los oráculos "humanos" son distintos de los autónomos, ya que las solicitudes de información a estos pueden ser bastante más complejas que las realizadas a los autónomos. Los "humanos" podrán dar respuesta a condiciones más abstractas o que requieran una valoración subjetiva. Sin embargo y precisamente por lo anterior, en los oráculos humanos no podemos distinguir en la mayoría de los casos la fuente o base de datos, del propio oráculo. Los oráculos de este tipo son a la vez bases de datos y oráculos o facilitadores de información.

Cuando los términos de un *legal smart contract* versan sobre un activo complejo sobre el cual varias de sus características son de difícil registro o varían durante la transacción, la automatización contractual no resulta la mejor opción. Debido a esto, necesitamos otros métodos externos a la *blockchain* para poder reforzar el uso y ejecución de los *smart contracts*.

[24] Egberts, A. (2017), *The Oracle Problem - An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems.*

A partir de esta idea de requerir asistencia externa para el cumplimiento de los términos de un *smart contract* que versan sobre las diversas características de un activo, objeto de la transacción, llegamos al uso necesario de los oráculos. Aunque en un primer momento pueda parecer que acudir a una fuente externa para comprobar el cumplimiento de términos codificados en un *smart contract* conlleve perder la ventaja de la autoejecución de los mismos y se introduzca así un componente subjetivo o directamente la intervención de un tercero independiente, sin embargo, la mayoría de los oráculos se encuentran en la propia red *DLT*[25].

En los casos en los que sea preciso acudir a fuentes externas a la red *DLT* para comprobar el cumplimiento de las condiciones codificadas para la ejecución de un *smart contract*, aunque en principio no se requiera la intervención de una autoridad central, está claro que se depende de una fuente externa informativa. Debido a esto, paradójicamente en el fondo sí que se requiere confiar plenamente en la fuente externa, que es un tercero independiente[26]. Es más, el uso de los oráculos hace que la red *blockchain* pierda su alto nivel de seguridad, que evita el punto único de fallo (*Single Point of Failure* o *SPOF*). Cuando se acude a un oráculo para solicitar información necesaria, el oráculo podrá provocar fallos tanto por errores en su propio funcionamiento, como por errores en la base de datos o fuente a la que acuda. Si el oráculo es el que falla en su funcionamiento al tratar la correcta información obtenida de forma incorrecta o si por ser un oráculo "humano" da una respuesta incorrecta a la solicitud informativa, entonces el error es del propio oráculo. Podría ocurrir también que el oráculo tuviese problemas de conectividad con la red *DLT* (por censura, por suspensión del servicio, etc.) y entonces los *smart contracts* no recibirían respuesta, ni se ejecutarían, lo que supondría un grave problema. Frente a estos problemas los oráculos no tendrán más remedio que mejorar la calidad de sus servicios, ya que, si alguno sufre un grave fallo, su reputación se verá mermada, lo que supondrá que deje de cobrar las cuotas por sus servicios. Es por ello que los oráculos a pesar de ser un medio necesario para el funcionamiento de los *smart contracts,* pueden provocar que una gran parte de la red falle como consecuencia de su uso.

[25] Goorha, P. (2018), *A Comprehensive Contracting Solution*...op. cit, pp. 13.
[26] Egberts, A. (2017), *The Oracle Problem - An Analysis…*op. cit, pp. 19.

Mientras que el uso de redes *blockchain* facilita que las partes no tengan que depositar su confianza en ellas ni en terceros independientes, si un *smart contract* requiere la intervención de un oráculo, las partes tendrán que prestar su confianza tanto a la fuente o base de datos correspondiente, como al propio oráculo que provea la información. Por lo tanto, para hacer efectivo el cumplimiento de numerosos *smart contracts,* se reintroduce de nuevo el requisito de la confianza. Dado que en una red *blockchain* los contratos serán ejecutados una vez que la información obtenida concuerde con el cumplimiento de las condiciones, y que la red no verifica el origen ni realiza un control *ex ante* de lo aportado por el oráculo, la confianza que las partes han de depositar en los oráculos y sus bases de datos es aún mayor. Podrá darse un control ex post, que en muchas ocasiones será difícil, sobre el cumplimiento de lo pactado, pero no habrá forma de evitar los efectos de la ejecución extemporánea del *smart contract*, ya que este se ejecutará automáticamente[27].

Existe el peligro de que al aumentar el número de usuarios en los próximos años de *smart contracts,* los oráculos creíbles y ampliamente utilizados sean escasos e incluso que la tendencia sea su reducción progresiva. El riesgo que encontramos es que los oráculos se transformen en un sistema de oligopolio de forma que, si alguno de ellos falla, el impacto en las transacciones de la red DLT será mucho más relevante que si existiese un numero de oráculos mayor. Cuando una de las partes quiera establecer un *smart contract* para automatizar la ejecución de todo o parte de un contrato, tendrá que depositar su fe en el correcto funcionamiento del oráculo al que vincula el *smart contract* y por ello tendrá que dedicar tiempo y dinero en la mejor comprensión sobre la fiabilidad del oráculo y de la base de datos de la que su *smart contract* depende. Incluso podrán existir casos en los que las partes se cubran del riesgo de fallos en el oráculo designado mediante la contratación de seguros[20].

El problema que plantea el uso de oráculos en el funcionamiento de los *smart contracts* es por tanto doble. Por un lado, por potenciales errores en su funcionamiento y, por otro lado, por fallos en las bases de datos o fuentes a las que este acude. Esto supone que las partes del *smart contract* se vean obligadas a depositar su confianza en ambas. Los usuarios racionales velarán por evaluar correctamente el grado de fiabilidad tanto del

[27] Egberts, A. (2017), *The Oracle Problem - An Analysis…*op. cit, pp. 19.

oráculo, como de las bases de datos designadas. Todo ello supone una pérdida de la eficiencia pretendida con el uso de tecnologías de tipo *DLT*.

A través del uso de los oráculos, los contratos que encontramos en una *blockchain* pueden contener condiciones para su ejecución más complejas y variadas, ya que acudiendo a las fuentes externas a las que los oráculos facilitan la conexión, se observará el cumplimiento o no de las mismas. El objetivo actualmente buscado de sofisticación y mejora de los *smart contracts*, requiere para su cumplimiento un mayor uso de los oráculos, ya que, para poder establecer condiciones más flexibles y variadas de cumplimiento, es necesario que existan oráculos que faciliten la comprobación de dicho cumplimiento.

En resumen, el uso de oráculos es necesario si se quiere aumentar la utilización y alcance de los *smart contracts.*

3.2 Organización Autónoma Descentralizada (DAO)

Se pueden crear en redes *blockchain* las denominadas organizaciones descentralizadas o *DOs* (en inglés, *decentralized organizations*), mediante la vinculación de varios *smart contracts*, que operen de acuerdo con un conjunto de reglas y procedimientos establecidos por los *smart contracts*[28].A través de las *Dos,* grupos organizacionales pueden operar por medio de *smart contracts* y así evitar la necesidad de crear entidades con o sin personalidad jurídica. El gobierno corporativo se podrá ejercer eficientemente, al llevar un registro de todas las decisiones tomadas, se conseguirá más transparencia a la hora de determinar quién es el responsable de cada decisión o acuerdo adoptado y se reducirán los costes operativos. A la hora de limitar a determinadas personas las decisiones más importantes de la empresa/organización, se podría utilizar la ya mencionada función *multi-sig*. Dicha función evitará que la decisión se tome y se produzcan sus efectos hasta que las partes así designadas den su consentimiento.

Un uso interesante de este tipo de organizaciones es la participación directa que se podría facilitar a los socios en la toma de decisiones. Podría pensarse en la posibilidad de facilitar a cada uno de los accionistas sistemas de voto descentralizados para que voten sobre decisiones que afectan a la marcha de la empresa. Sus decisiones tendrían de esta forma

[28] Wright, A. y De Filippi, P. (2015), *Decentralized Blockchain Technology*...op. cit, pp.6.

un impacto más directo, sin tener que mediar en ellas los ejecutivos o directivos de la misma.

A través de *blockchains* se podrían realizar, en mayor cuantía y con menor riesgo de corrupción u opacidad informativa, acciones colectivas. Por ejemplo, un mayor número de personas estaría dispuesta a realizar donaciones si supieran exactamente a qué se dedica su dinero. La *blockchain* proporciona un nivel de seguridad y transparencia informativa que son fundamentales en ámbitos de acción colectiva como el de fundaciones sin ánimo de lucro.

Las organizaciones autónomas descentralizadas (*DAOs*) son un tipo específico de organización descentralizada, ya que son autónomas y autosuficientes. Una vez creadas, estas no dependen de la intervención de los usuarios o incluso de su creador para operar, es decir, son totalmente independientes.

En relación con ellas existe un amplio debate doctrinal sobre si se requiere que constituyan un nuevo tipo de entidad jurídica y si se ha de determinar a qué jurisdicción se han de someter, especialmente cuando se desconoce la ubicación de sus socios[29].

Aunque poseen numerosas ventajas, las *DAOs* también poseen cierto peligro. En junio de 2016, un *hacker* desconocido transfirió, aprovechando un fallo en un *smart contract* que componía una *DAO*, *ethers* por valor de cuarenta millones de dólares. Cuando la *Etherum Foundation* sometió a debate cómo lidiar con este asunto, hubo dos corrientes de pensamiento enfrentadas. Por un lado, los que consideraban que era un robo que requería reparación, y por otro lado, los que argumentaban que, si el código del *smart contract* tenía esa vulnerabilidad, había que asumir que ese fallo de programación era un riesgo inherente al propio sistema y que debía ser asumido por los participantes de la red. Finalmente prevaleció la idea de realizar un "*hard fork"*, esto es, al no poder modificar el contenido de los bloques, volver al bloque inmediatamente anterior al de la transferencia fraudulenta y establecer una cadena de bloques posterior y alternativa a la cadena problemática. Para poder realizar esta compleja e inhabitual operación y dejar los bloques problemáticos fuera del registro, era necesario el acuerdo de la mayoría de los nodos validadores para la adhesión a la nueva cadena alternativa. Todo esto supuso un

[29] EU Blockchain Observatory and Forum. (2018), *The legal and regulatory framework for blockchain and smart contracts.*

cisma en la red *Ether*, ya que algunos querían mantenerse fieles a sus ideales de respeto absoluto al funcionamiento de la red y por ello a la *blockchain* original, mientras que otros se adhirieron a la cadena creada *ex profeso* para solucionar el robo. El cisma fue de tal importancia que finalmente se crearon dos cadenas de bloques distintas y con distinto nombre (Ethereum Classic y Ethereum).

3.3 Adaptación legal de los legal smart contracts

Ante cualquier avance tecnológico significativo como es el desarrollo y aplicación de los *legal smart contracts*, los legisladores, tanto a nivel nacional como a nivel europeo, tienen básicamente dos opciones. Por una parte, pueden optar por no regular ni modificar la ley preexistente adaptándola y aplicar directamente los principios y normas fundamentales contenidos en ella, permitiendo que el mercado autorregule libremente los nuevos sistemas de contratación. Otra opción sería la de crear un paquete normativo dedicado exclusivamente a la regulación de los *legal smart contracts* y *smart contracts* autónomos, como ocurrió en EE.UU. con la aprobación del *Digital Millenium Copyright Act* cuyo objetivo fue regular la aparición de internet y los problemas de derechos sobre la propiedad intelectual que se originaron[30].

A nivel comunitario el *EU Blockchain Observatory & Forum* realizó en 2018 una serie de recomendaciones en la Unión Europea para establecer un marco legal adecuado que regule el uso de los *legal smart contracts*. Dicho foro considera que, en general, no es necesario crear un nuevo marco normativo, salvo para regular las *DAOs*. El foro recomienda aplicar la normativa existente que les sea aplicable (civil y mercantil) y analizar caso por caso las relaciones entre las partes fuera de la red, en caso de conflicto legal.

Uno de los mayores problemas que presenta el uso generalizado de *smart contracts* dentro de la UE es su conformidad y respeto hacia el nuevo Reglamento General de Protección de Datos de la Unión Europea (*GDPR*). Un *smart contract*, aunque no tenga un soporte jurídico en el mundo real (es decir aún sin constituir un *legal smart contract*) siempre conllevará para su ejecución el automático tratamiento y proceso de datos y, en la medida

[30] EU Blockchain Observatory and Forum. (2018), *The legal and regulatory*...op. cit, pp. 23.

que ello afecte a datos de carácter personal, tendrá que ajustarse a lo establecido en el ya mencionado Reglamento[31].

El primer factor a considerar que podría determinar la aplicación o inaplicación del Reglamento, es que el *smart contract* conlleve el tratamiento de datos personales o no. Sin embargo, incluso en el caso de que los datos introducidos en el *smart contract* no sean de carácter personal, puede resultar de aplicación el Reglamento, debido a que el resultado de la ejecución del *smart contract*, si conlleve el tratamiento de datos personales.

El artículo 22.1 del *GDPR*, establece que "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.". Para analizar si podría considerarse que un *smart contract* se encuentra sujeto a esta disposición tenemos que analizar dos aspectos de los mismos.

En primer lugar, tenemos que determinar si estos procesos son decisiones basadas únicamente en el tratamiento automatizado de datos o no. El requisito necesario para que esta primera afirmación fuera aplicable a los *smart contracts*, es que no hubiese ningún tipo de intervención humana en el proceso de toma de decisiones. Si entendemos que el proceso de toma de decisiones queda reducido únicamente a la ejecución del *smart contract* una vez cumplidas las condiciones programadas, entonces si podríamos decir que en principio el artículo 22 es aplicable a los *smart contracts.* Sin embargo, si entendemos que el proceso de toma de decisiones engloba un marco temporal mayor, incluyendo la decisión inicial de las partes de transformar sus pactos o acuerdos en *smart contracts*, o que, si existe intervención humana al tratarse de contratos que dependen de lo que disponga un oráculo humano (en algunos casos), entonces se podría escapar el uso de *smart contracts* del artículo 22. Al continuar examinando este artículo, observamos que en su segundo apartado se establece, como excepción al primer apartado, la decisión necesaria para la "celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento". Si en el primer apartado se integrase el consentimiento de las partes en la elaboración del mismo, no estaría expresamente contenida la excepción en el segundo apartado del artículo. Por ello consideramos que si se encuentra sujeto al artículo 22 en este aspecto, aunque a continuación observaremos si se cumplen el segundo

[31] Finck, M. (2019), *Smart Contracts as a Form of…*op. cit, pp. 13.

requisito en cualquiera de sus variantes, ya que el proceso de toma de decisiones se refiere únicamente a la ejecución del *smart contract*, por lo que se cumple el requisito de ausencia de intervención humana[32].

En segundo lugar, hemos de determinar si lo ejecutado por un *smart contract* produce efectos jurídicos o no. Aunque algunos *smart contracts* no pueden producir efectos jurídicos en personas ya que funcionan como transacciones entre máquinas (Internet of Things), la gran mayoría de los *smart contracts* producen efectos jurídicos en las partes, ya que se produce el cambio en los derechos y obligaciones que tienen las partes sobre los activos objeto de la transacción. Por ejemplo, en un pago en *bitcoins* hay un cambio en la propiedad de los mismos, por lo que los derechos de las partes se verán modificados, produciéndose así efectos jurídicos. Todos los *smart contracts* que produzcan efectos jurídicos entre las partes y que en su ejecución no exista intervención humana, se someterán al Reglamento, en cuanto al tratamiento de datos de carácter personal.

En tercer lugar, es necesario determinar si aun cuando el *smart contract* no produzca efectos jurídicos, el tratamiento de datos personales le afecta significativamente de modo similar. A estos efectos, en cada *smart contract* tendremos que analizar si los efectos producidos por la ejecución sin intervención humana del mismo son suficientemente relevantes para su regulación, dichos efectos podrán ser tanto positivos como negativos. Estos habrán de modificar significativamente la situación de las partes, su comportamiento o sus decisiones durante un período prolongado o de manera permanente[22]. Para cada *smart contract* tendremos que determinar si sus efectos son suficientemente relevantes como para que le sea de aplicación dicho Reglamento.

En resumen, si existe un *smart contract* cuya ejecución se produce sin intervención humana y tiene efectos jurídicos o efectos (no jurídicos) significativos, que afecten al tratamiento de datos de carácter personal, entonces el uso de estos contratos en la UE se verá limitado por lo dispuesto en el Reglamento UE 2016/679. En los casos en los que les sea de aplicación, se prohibiría en principio el tratamiento y ejecución automática de los mismos. Sin embargo, esta prohibición no es absoluta, se podrá justificar la ejecución

[32] Finck, M. (2019), *Smart Contracts as a Form of…*op. cit, pp. 13.

automática de los mismos si cumplen el artículo 22.2 del Reglamento UE 2016/679, cuando les sea aplicable.

Aun en los casos en los que se establece la posibilidad de automatizar la ejecución sin que se requiera en principio la intervención humana, la propia *GDPR* en el apartado tercero del artículo 22 establece que "el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión". La interpretación de este apartado que facilitaría el uso de los *smart contracts* sería el considerar que, con que las partes ostenten una clave privada que rige el contrato, ya se estaría cumpliendo con el requisito de la intervención humana.

El Reglamento UE 2016/679 contiene numerosas exigencias que podrían complicar su implantación en la UE, entre ellas cabe destacar: el derecho a la información sobre el tratamiento de los datos, el deber de llevar a cabo una evaluación del impacto en la protección de los datos y la evaluación y control de los datos tratados (para que sean el menor número posible e imprescindibles, mediante un control *ex ante* de los mismos). Todos estos requisitos legales que numerosos *smart contracts* tendrían que cumplir en la zona UE, podrían llevar a que no tuviera sentido servirse de ellos, al perder estos su principal ventaja (eficacia y auto ejecutoriedad), ya que han de intervenir autoridades centrales de control y ha de facilitarse un mínimo de intervención humana en ellos.

La mayoría de los *smart contracts* actuales no cumplen con los requisitos marcados en el artículo 22 del GDPR, para ser legalmente válidos en la UE. Sin embargo, no hay una incompatibilidad total entre estos y la normativa, por lo que podrían ser diseñados para cumplir con sus requisitos. Para que cumplan con estos requisitos los *smart contracts* tendrán que adaptarse al mundo real y mitigar su completa e inevitable fuerza auto ejecutoria, aunque esta sea una de las principales ventajas de su uso.

4. Problemas jurídicos que plantea el uso de los legal smart contracts

Existen numerosos retos en la adaptación e incorporación de los *legal smart contracts* al tráfico jurídico ordinario. Uno de los principales problemas a los que se enfrentan los *legal smart contracts* a la hora de gozar de fuerza jurídica es la observancia de lo requerido en legislación muy diversa; desde el cumplimiento con la nueva GDPR hasta el cumplimiento con la Ley de Condiciones Generales de la Contratación y la Ley General de la Defensa de Consumidores y Usuarios, entre otras. Otro de los grandes retos del uso de esta nueva tecnología viene precisamente por la gran ventaja que otorga la ejecución automática. Esta deviene un problema cuando limita la eficacia o el poder ejecutivo de las sentencias dictadas por el poder judicial o las decisiones adoptadas por autoridades externas a la *blockchain*. El uso de tecnologías tan avanzadas como son estas supone que en ocasiones resulte muy complicado delimitar y establecer correctamente la responsabilidad de todas las partes que intervienen, ya sea de manera directa o indirecta en un *smart contract*, en caso de que ocurran fallos en su codificación o ejecución. Convendría que esta responsabilidad se pudiera determinar *ex ante*, para evitar así la inseguridad jurídica que genera a numerosos potenciales usuarios y creadores de plataformas *blockchain*. Finalmente existe riesgo en el uso de los oráculos, ya que tanto estos, como las bases de datos a las que acuden, pueden contener errores que produzcan numerosos fallos en todas las redes *DLT;* es por ello que el uso de los mismos y su fiabilidad son un reto para conseguir una mayor implantación de los *legal smart contracts.*

Antes de centrarnos en los principales retos a los que los *legal smart contracts* se enfrentarán en los próximos años con el fin de lograr una mayor implantación, mencionaremos aquí otros problemas relevantes.

Para empezar, hemos de mencionar los problemas con las leyes de protección de consumidores y usuarios. Parece en principio complicado conjugar esta nueva tecnología con algunas disposiciones de estas leyes, por ejemplo, con los denominados derechos de revocación o el derecho a la recepción de una copia escrita de la oferta u otros derechos que no encajan con los beneficios que pretende aportar la tecnología *DLT*. Podría resultar también problemático, que sea un requisito para el uso de las redes *DLT* el conocimiento de sus respectivos términos y condiciones de uso y que sea obligatoria su aceptación. Convendría que, en ellos, junto con las previsiones legales necesarias, se estableciese

cómo se determinará la responsabilidad en caso de que sea necesario delimitarla. Una corriente doctrinal cree que siempre será responsable una de las partes contratantes (mientras no sean IA) ya sea directa o indirectamente y por ello los programadores nunca podrán ser los responsables, ya que, sino tendrían que contratar siempre seguros para cubrir este riesgo. Se llegan incluso a plantear si es mejor otro sistema y no el de términos y condiciones, ya que la mayoría de los usuarios no los leería o no los entendería. Cuando se elaboren estos contratos de manera masiva o en serie y dirigidos a consumidores, se habrá de aplicar otro conjunto normativo, ya que la relación entre las partes, al ser una de ellas un consumidor (*B2C*) requiere de una mayor protección, que se asegura en el ordenamiento jurídico español por medio de otras leyes. Dicho conjunto normativo se compondría de: la Ley de Condiciones Generales de la Contratación y la Ley General de la Defensa de Consumidores y Usuarios.

Otro grupo de potenciales problemas cuyas causas ya hemos apuntado brevemente en el apartado 3.1 de este trabajo consiste en los problemas que pueda causar en la ejecución el mal funcionamiento de los oráculos. Antes de analizarlo aclaramos que, al intervenir un oráculo en la ejecución de los *smart contracts*, vuelve a aparecer el componente de la confianza que recae en estos oráculos. La ausencia de confianza en una autoridad central era una de las principales ventajas del uso de redes *DLT* que, de esta forma, desaparece. Como ya hemos apuntado, el mal funcionamiento puede provenir tanto del propio oráculo, al tratar o trasladar la información recabada, o de las bases de datos o fuentes a las que acuda el oráculo para obtener la información requerida. Además, a medida que algunos oráculos ganan en fiabilidad para los usuarios de las distintas plataformas, el mercado de oráculos se irá reduciendo, hasta formar un oligopolio. Cuando esto ocurra, cualquier fallo tanto en el oráculo como en las bases a las que acuda, podrá provocar grandes fallos en todas las redes *blockchain*.

El último problema que trataremos brevemente, antes de centrarnos en los problemas más complejos, es el de limitar la seguridad o la intervención de las autoridades policiales. Decimos que existe este problema ya que, en el caso de que se dicte una orden judicial de interceptación de las comunicaciones de un individuo, actualmente la autoridad competente (policía, guardia civil, policías autonómicas), puede acudir a la autoridad central de dichas comunicaciones (ej. Google, Telefónica, Skype, etc.) y solicitar todo lo que la orden habilite (el contenido de sus comunicaciones, los nombres de las personas

con las que mantiene comunicaciones, etc.). Sin embargo, tanto en las redes *DLT* como en otras nuevas tecnologías, al no existir una autoridad central competente a la que acudir para solicitar la interceptación de las comunicaciones, la policía no tendrá en principio la posibilidad de interceptar dichas comunicaciones. Una forma de solucionar este problema sería que cada red habilitase un mecanismo que posibilitara que la policía de cada Estado, cuyos ciudadanos participen en la *blockchain*, tenga acceso a todas las operaciones en las que intervienen sus ciudadanos. Sin embargo, al habilitar que un tercero ajeno a la operación tenga acceso a la información vertida en la red *DLT*, se podría reducir el nivel de ciberseguridad de dicha red, ya que los hackers podrían también hacer uso de esta "puerta de entrada" y así modificar y atacar las transacciones contenidas en ella. En este caso nos encontramos ante un dilema relevante como es que prime la ciberseguridad y por ello la policía no pueda intervenir lo registrado en la DLT, o que haya una mayor seguridad real, ya que la policía cumple con su labor de protección frente al delito, al intervenir por orden judicial las comunicaciones y actividades de un ciudadano.

A continuación, nos centraremos en los dos problemas más complejos con los que han de lidiar los expertos legales en *legal smart contracts*: la irreversible ejecución automática y la compleja determinación de la responsabilidad contractual.

4.1 Problemas que plantea la ejecución automática y su irreversibilidad

En un *smart contract*, una vez cumplida la condición preestablecida en el mismo, es inevitable la ejecución. No existe la oportunidad de paralizar, anular o suspender la ejecución, ni siquiera por parte de autoridades judiciales o arbitrales que se encuentren juzgando la validez del *legal smart contract* que da soporte al *smart contract* que se autoejecutará[33]. El problema surge porque la sentencia pierde su carácter ejecutivo si el juez declara la nulidad del legal smart contract. Dicha sentencia no provocará la ineficacia del *smart contract* subyacente, ya que este producirá los efectos previstos ante el cumplimiento de lo programado; así quedará vacía de contenido la resolución judicial. Las partes de un acuerdo que deviene autoejecutivo por medio de un *smart contract*, quedan despojadas de su derecho a obtener una tutela judicial efectiva sobre sus derechos,

[33] Werbach, K., & Cornell, N. (2017), *Contracts…* op. cit, pp. 15.

pierden su derecho a litigar. Debemos mencionar que, aunque la red *DLT* ejecute automáticamente los *smart contracts* contenidos en ella, siempre las partes podrán acordar el uso de una función "*multisig*" o multifirma, para ratificar su voluntad de ejecutar lo pactado. Con esto vemos que las partes recuperan, aunque sea parcialmente, el control de su voluntad; aun así, no cabría en principio litigar y defender sus derechos ante un juez o árbitro, ya que la autoejecución se terminaría produciendo.

En resumen, el principal problema de la ejecución automática de los *smart contracts,* es que una vez incorporados a la red DLT, ya no se les puede someter en principio a un control de contenido (ex post) para determinar si el mismo es válido o no conforme a derecho. Debido a ello es muy importante que, a la hora de negociar los términos contractuales, se realice un control *ex ante* de la legalidad de estos. Aun existiendo este control *ex ante*, este puede ser insuficiente en casos de extrema onerosidad sobrevenida o de cláusulas en el contrato de tipo *rebus sic stantibus*.

Por otra parte, la ejecución automática tiene ventajas, ya que reduce los costes tanto de la negociación como de la transacción o ejecución final de lo pactado. La pérdida del valor ejecutivo de algunas sentencias judiciales, que no podrán paralizar o suspender dicha ejecución automática, supondrá una reducción en tiempo y costes litigiosos enorme, aunque también, como ya hemos señalado, conlleve otras desventajas. Las ventajas que puede otorgar en términos de eficiencia y abaratamiento de los costes, que aportan los *smart contracts*, podría suponer un aumento del número de contratos, ya que muchos contratantes que no disponen de medios para obtener un servicio de asesoría jurídica, no necesitarían obtenerlo utilizando un *smart contract*.

En teoría, al poder imponerse condiciones y excepciones a los *smart contracts*, se podría limitar la ejecución automática de los mismos, estableciendo como condición para su ejecución la intervención de un juez o árbitro. Sin embargo, limitando la ejecución automática de esta manera, se perdería una de las principales ventajas que nos aportan las redes *DLT*, eficiencia y abaratamiento. Este es un dilema que en el futuro se tendrá que solventar decidiéndose si merece la pena frenar las ventajas que la ejecución sin intervención nos aporta (eficiencia, automatismo, abaratamiento), o bien resulta más conveniente limitar las ventajas de la ejecución, en pos de una intervención (judicial o

arbitral) para eliminar los riesgos que en algunas ocasiones supondría la ejecución automática para los derechos de las partes.

Parece impensable que, aunque el uso de *smart contracts* sea mucho más eficiente y barato (en tiempo y dinero) que el recurso a un juez o tribunal determinado, al final sean los *smart contracts* los que realicen la función de juez y la jurisdicción ordinaria se vea eliminada. Simplemente consideramos que el uso generalizado de los *smart contracts* podría ser un medio para evitar la solicitud de ejecución de numerosos contratos, sin que en ningún momento pueda dicha tecnología reemplazar a la función judicial prevista. No se eliminará la necesidad de tutela judicial sobre contratos, sino que se modificará lo solicitado en el proceso. Se pasará de solicitar el cumplimiento contractual ante incumplimientos, a solicitar la restitución de lo ejecutado por medio de un *smart contract*, junto a la correspondiente indemnización por daños. De esta forma se modificarían los roles de las partes en el proceso, ya que la parte que se ha visto obligada -presuntamente de manera injusta- a soportar la ejecución del contrato, será ahora la parte demandante que solicitará la restitución, mientras que, si estuviésemos ante una demanda por incumplimiento, esta sería la parte demandada.

El problema de la ejecución automática también se deriva de que el uso de redes *DLT* (públicas y permisionadas) puede conllevar los ya mencionados potenciales errores a la hora de transcribir a lenguaje codificable las cláusulas de un contrato. Aun cuando estas fuesen llevadas a cabo sin errores y sin límites, por ejemplo, con asistencia de la Inteligencia Artificial (IA), cabría que los resultados obtenidos con la ejecución no fueran óptimos para una o incluso para todas las partes afectadas por la transacción. Podríamos encontrar supuestos en los que la mejor opción para todas las partes de un acuerdo es la falta de ejecución del mismo. Ante estas situaciones, los *smart contracts* presentan graves problemas, ya que normalmente no conceden la opción de que las partes puedan, posteriormente a la codificación del mismo, decidir libre y conjuntamente si les es conveniente o no la ejecución. Esto podría remediarse imponiendo la función *multisig* a determinados casos o mediante la codificación de cláusulas que limiten la obligación de ejecución ante casos de fuerza mayor y demás supuestos necesarios (onerosidad sobrevenida, etc.), aunque se perdería la ventaja que posee el uso de las redes *DLT* y resulta sumamente complejo poder codificar un lenguaje tan ambiguo.

Asimismo, es un problema que mientras que, en la legislación contractual española, las partes pueden acordar modificar el contenido inicial del acuerdo, si se utilizase un *legal smart contract* en el que *ab initio* no se especificase la posibilidad de su modificación, entonces sería imposible realizar esta modificación pactada y bilateral del acuerdo ya acoplado a la cadena de bloques. La ausencia de la posibilidad de modificar el contrato, previo acuerdo de las partes, una vez introducido el *legal smart contract* en la red *DLT*, quiebra el principio de autonomía de la voluntad de las partes, que sí se respetaría empleando otros medios de ejecución.

Debido a todo lo anterior vemos la diferencia entre el derecho contractual que habilita las modificaciones y demás cambios, e incluso la no ejecución de lo pactado en determinados casos y pretende una relación constante entre las partes del acuerdo y lo obtenido mediante un *legal smart contract* que supone una única transacción cuya ejecución es imparable y en principio resultaría inmodificable por las partes, es decir es más una relación estanca. El control *ex ante* del contrato lo han de realizar las partes, atendiendo y previendo todos los potenciales conflictos y renegociaciones que pueden surgir entre ellos. El control judicial o *ex post* consiste en resolver los potenciales conflictos no contemplados y no resueltos en el propio contrato a la luz de lo establecido en el mismo, o en la legislación. Los *smart contracts* quiebran la intención del legislador de mantener dicho control *ex ante y ex post*, al atomizarlos, de forma que descartan la dimensión temporal y su posible evolución, así como la potencial resolución judicial sobre la validez y el contenido de los mismos[34].

Lo más adecuado ante los casos en los que la ejecución automática se produce mediante una red *DLT*, como son los contratos válidos, pero no ejecutables conforme a la legislación (por violencia, intimidación, etc.) sería solicitar judicialmente y con posterioridad a la ejecución del contrato en la red, la restitución de los daños sufridos. Sin embargo, encontramos numerosos problemas con esta hipotética solución de ejecutar primero y resolver después (indemnizando por los daños), ya que en algunos casos no se debe permitir la ejecución como cuando se trate de contratos con objeto ilegal o cuando la restitución no resulte posible. Algunos autores, como Albacar, deducen de los arts. 1271 a 1273 del C.C. que los requisitos para que el contrato sea válido es que exista un

[34] Werbach, K., & Cornell, N. (2017), *Contracts…* op. cit, pp. 15.

objeto: lícito, útil, determinado, valorable en dinero y que se encuentre dentro del comercio de los hombres[35]. A la hora de determinar si existe o no un objeto y por lo tanto un contrato, existen dos corrientes diversas: la de la representación y la de la programación. Para los primeros, el objeto ha de estar presente o representado a la hora de que las partes otorguen su consentimiento. Para los autores más modernos, que apoyan la programación el objeto ha de estar presente, pero no necesariamente en un momento inicial cuando se preste el consentimiento, sino que ha de estar presente a lo largo del proceso temporal que dure la vida del contrato. Se niega reiteradamente por parte tanto de la doctrina como por parte de la jurisprudencia que el objeto del contrato deba encuadrarse para su validez en un contrato tipo o con un determinado *nomen iuris*[35]. Una sentencia muy relevante que facilitaría el desarrollo y validez de los *legal smart contracts* es la Sentencia del Tribunal Supremo de 12 de abril de 1971, en ella se permite la determinación del objeto del contrato, tanto por parte de las partes como del juez, con posterioridad a la celebración de mismo. Sin embargo, Lacruz Berdejo y de los Mozos nos recuerdan que "la licitud o la ilicitud no ha de establecerse en relación con el objeto mismo, sino en relación con el negocio jurídico mismo. La solución a un objeto de contrato ilícito será la declaración de la nulidad radical del contrato." Esto plantea numerosos problemas con los *legal smart contracts*, ya que, aunque tengan objeto ilícito y se declare la nulidad radical de los mismos, su ejecución será inevitable.

Si se codificase mediante un *legal smart contract* una donación ordinaria, observamos que se diferencia de un contrato ordinario, ya que estos contratos de donación en la legislación no obligan *ex ante* al cumplimiento y ejecución de la donación. Mientras que atendiendo al derecho contractual no se impone la ejecución de ninguna donación, si se orquestase dicha donación mediante un *legal smart contract*, obligatoriamente se habría de ejecutar, imponiéndose así obligaciones *ex ante*. De todo esto extraemos en claro que mientras que los contratos se establecen en la legislación ordinaria como forma de controlar la relación de obligaciones recíprocas entre las partes, en el caso de los *smart contracts* no solamente sirven para controlar la ejecución y cumplimiento de estos, sino que cualquier tipo de obligación que se codifique, aún sin contraprestación, será autoejecutable en la red DLT. Estos contratos no requieren el conocimiento de las

[35] Aguilera Silván, F-J. (2011), *El objeto como elemento esencial del contrato.*

relaciones entre las partes, ni siquiera que exista una contraprestación entre ellas, lo único que les es relevante es lo codificado; operan atendiendo al principio de abstracción y no al principio de causalidad, ya que esto les resultaría imposible.

Para algunos autores, como Ibáñez Jiménez, sería necesario potenciar la seguridad jurídica y la eficiencia a la vez, mediante ocho cuestiones de control *ex ante* (Ibáñez Jiménez, 2018, p.114-118). En primer lugar, para poder introducir un *smart contract* en cada *blockchain* se tendría que cumplir con las previsiones establecidas por la misma, en materia de formación y celebración del contrato, así como con las previsiones legales que serán principalmente las contenidas en la LSSI. Se habrán de reducir los costes de aseguramiento de la capacidad e identidad de las partes, sin quebrar con la privacidad, de manera que la identidad y demás datos necesarios de las partes queden registrados en un sistema de negociación seleccionado[36]. Esta medida aumentaría enormemente la seguridad y confianza de las partes y podría fomentar un aumento en el uso de redes *blockchain*. En tercer lugar, se ha de asegurar que las partes han prestado su consentimiento efectivo tanto para la operación en sí, como para que se ejecute automáticamente el *smart contract* al introducirlo en la red *DLT*. Sería también relevante el regular las consecuencias de la concurrencia de la oferta y aceptación a distancia tanto en un primer momento cuando se añade el *smart contract* a la plataforma correspondiente, como después, cuando el contrato se ejecuta efectivamente. Cuestión vital a la hora de ejecutar los *smart contracts* sería establecer mecanismos: de ejecución fuera de la red (por si existiesen fallos en la ejecución programada en la misma), de reclamación, de determinación de la ley aplicable y de resolución conflictual, mediación o arbitraje. Para Ibáñez Jiménez convendría establecer cláusulas de arbitraje, ya que acudiendo a los árbitros se podría solucionar la cuestión clave de la indeterminación de la jurisdicción competente (Ibáñez Jiménez, 2018, p.117). Considera también en la misma obra que al no poder detener la ejecución de los *smart contracts*, una vez cumplidas las condiciones para su ejecución, para los casos de extraordinaria onerosidad sobrevenida o para la aplicación de cláusulas *rebus sic stantibus*, se han de prever mecanismos de indemnización o compensación alternativa fuera de la red *DLT*. Otro aspecto que resulta fundamental para dotar a la *blockchain* de mayor seguridad jurídica sería establecer

[36] Ibáñez Jiménez, J. W. (2018). *Derecho de Blockchain...*op. cit, pp, 14.

mecanismos de registro (*off-chain*) de las condiciones generales de contratación, sus términos, de forma que jurídicamente se considere válido el cumplimiento mediante el uso de un *smart contract.* Como ya hemos establecido en el tercer apartado de este trabajo, en caso de discrepancias entre el contrato en lenguaje codificado y el contrato en soporte físico, prevalecería siempre este último, por ser la fuente original donde inicialmente queda plasmada la voluntad de los contratantes. En resumen, se ha de ajustar la normativa existente en las *blockchains* a todas las especialidades que el cumplimiento contractual por medio de un *smart contract* conlleva[37].

Será la labor de equipos legales especializados en redes *DLT* y *smart contracts* el diseñar sistemas y mecanismos que permitan superar este doble reto: superar el anonimato digital y la irrevocabilidad en el cumplimiento[32].

4.2 Problemas para la determinación de la responsabilidad en los legal smart contracts

Son numerosas las dudas que surgen en torno a la responsabilidad contractual cuando acudimos a los *legal smart contracts*: ¿Qué ocurre cuando hay un error en el código programado?, ¿es responsable el *miner*?, ¿Si el contrato ha sido verificado y auditado entonces, es el auditor el responsable?, ¿Han de tener los auditores un seguro?

Aunque nuestro ordenamiento jurídico resuelve algunas cuestiones como es, por ejemplo, el lugar de producción del pago o de la obligación a la hora de determinar el pago, que para ello hemos de atender a lo dispuesto en el artículo 1171 del Código civil en el que se establecen tres reglas subsidiarias para su determinación. En general existen numerosas dudas sobre cómo lidiar con la responsabilidad contractual al intervenir numerosas partes en la elaboración, codificación y ejecución de un *legal smart contract* (ej. *miners, validators, pseudonymus actors*, etc.). Cuando nos encontramos ante relaciones contractuales en las que interviene una autoridad central, por ejemplo, cuando entre las partes encontramos a una entidad central de contrapartida, el régimen de responsabilidad de todos los intervinientes en la relación queda claro desde el inicio de la misma. Lo más relevante si los *smart contracts* quieren gozar de una mayor seguridad jurídica es que, o

[37] Ibáñez Jiménez, J. W. (2018). *Derecho de Blockchain...*op. cit, pp, 14.

bien por medios legales o bien por términos generales de contratación de cada plataforma *blockchain,* al tratarse de relaciones sin entidad central, quede muy claro qué labor desempeñan en cada fase contractual: las partes, la empresa propietaria de la *DLT*, los *miners*, etc.

Si nos encontrásemos ante un asunto de ciberseguridad, la responsabilidad sería de los programadores de la red. Si se tratase de un asunto de servicio propio de la red, serían entonces responsables los proveedores de dicho servicio y se aplicaría esta lógica al resto de los casos. Para algunos autores como Legerén-Molina, el ideal a la hora de determinar la responsabilidad contractual de un *legal smart contract* consiste en acudir a lo establecido en el contrato que se encuentra en el mundo real, que habrá establecido los criterios legales para resolver controversias (Legerén-Molina, 2019, p. 227). Sin embargo, nos podríamos encontrar con numerosos conflictos cuya resolución, en cuanto a la delimitación de responsabilidad, no pudiese completarse acudiendo únicamente al contrato en soporte físico.

Al no existir regulación específica para estos contratos en España, se habrá de acudir a la normativa civil y mercantil general de los contratos, a la que regula la contratación electrónica y a la relativa a los servicios de la información, a pesar de que no den una respuesta acabada a todos los eventuales conflictos legales que puedan surgir. A los *smart contracts* que no tengan respaldo jurídico en el mundo real, les será de aplicación el artículo 23 de la Ley de servicios de la sociedad de la información y de comercio electrónico (LSSI), la cual remite al Código Civil y al Código de Comercio y establece los requisitos necesarios para su validez y efectos jurídicos que son: objeto cierto, causa y consentimiento. Además, es recomendable para evitar errores de codificación o *bugs* una auditoría sobre el código, realizado por técnicos que no hayan intervenido en la codificación del *legal smart contract*. Resulta aún más complicado resolver la responsabilidad contractual en algunos casos como son: ataque a la red *DLT*, que una parte retire los activos de la cuenta pactada para su transferencia, que un tercero manipule la información aportada por los oráculos o el código de la transacción, que se produzca el mal funcionamiento de los nodos, etc. Para poder dar respuesta a todas estas diversas situaciones que se pueden generar, ante las que actualmente el ordenamiento jurídico español no da una respuesta clara y definitiva sobre quiénes serían responsables, es necesario o bien una resolución casuística en manos de los jueces basada en lo ya

dispuesto legalmente, lo que inicialmente podría generar inseguridad jurídica, o bien un desarrollo normativo para cubrir lagunas y vacíos legales, dotando así de una mayor seguridad jurídica a este tipo de tecnología innovadora.

El problema que encontramos en la regulación casuística de la responsabilidad, además de la inseguridad jurídica que esto conllevaría, está vinculado con la irreversibilidad en la ejecución de lo introducido en la *blockchain*. Los jueces o tribunales no podrían entrar a determinar quién es responsable del fallo y paralizar la ejecución del *smart contract* hasta aclarar esta cuestión o incluso eliminar el contrato, si el fallo tiene la suficiente entidad para considerar esta como la mejor opción. Todos estos problemas relativos a la irreversibilidad de la ejecución automática ya los hemos tratado en el apartado 4.1 de este trabajo.

5. Sistemas alternativos de cumplimiento

Inicialmente ni los *smart contracts,* ni en general las aplicaciones de tipo *DLT* tenían en cuenta los requisitos legales que tenían que cumplir, ni los efectos que su ejecución podía provocar en el mundo real. Sin embargo, con el tiempo han sido numerosas las plataformas *blockchain* que han buscado obtener un reconocimiento legal, con el fin de aumentar su uso y alcance.

En el caso de los *smart contracts,* la sofisticación de los mismos se produce intentando mantener su principal ventaja que es la ejecución automática, pero intentando mitigar su principal inconveniente, que es su inevitabilidad en algunos casos.

Esta tendencia se pretende conseguir dotando de una mayor flexibilidad terminológica a los *legal smart contracts* a la hora de codificarlos (más allá del *if/then/else*), pudiéndose abrir de esta forma una puerta a sistemas de verificación como el *multisig,* ya mencionado en el apartado anterior. La estructura *if/then/else* podría funcionar en numerosas transacciones, por ejemplo, ante un préstamo de un coche, *if* (si) no se recibe la contraprestación cuando es debida, *then* (entonces) la propiedad del coche volverá a

recaer en el prestamista[38]. Por otra parte, para contratos que sean más compeljos, se podría utilizar la función *multisig* de forma que solo se ejecutarían los *smart contracts* cuyas partes hubiesen verificado, mediante un sistema de activación del *software* al utilizar sus claves privadas, el cumplimiento de lo pactado. En tanto no hubiese problemas en la ejecución entre las partes, ambas activarían el *software* usando su clave privada y de esta forma se ejecutaría el *smart contract.* Si ante la ejecución, las partes no se pusieran de acuerdo en cuanto a la validez en el cumplimiento de las condiciones pactadas para la ejecución, entonces un tercero imparcial (árbitro o juez) utilizaría su clave privada para así realizar la ejecución, si le pareciese conveniente y de la forma más adecuada.

Asimismo, se están desarrollando en algunas plataformas *DLT* sistemas arbitrales por los que resolver, dentro de la propia red *blockchain*, este tipo de disputas. Los árbitros, elegidos por las partes o por la propia red, tomarían sus decisiones dentro de la red, de forma que sus pronunciamientos se añadirían a la cadena de bloques como nuevas transacciones, indicando la indemnización o pago procedente conforme al fallo emitido. No se modificaría el bloque que contiene la transacción original, de forma que este se ejecutaría automáticamente, sino que se añadiría una nueva transacción independiente de esta. Se crearía así una jurisdicción interna que mitigaría la irreversibilidad de la ejecución automática.

Para el caso de que el *smart contract* tuviese un error, se podría incluir en él un *hash* que lo vinculase al contrato real (en papel), de forma que, si el contrato codificado fallase, prevalecería el contrato que se encuentra en el mundo real. Esta tendencia aboga por que ante cualquier disputa se pueda suspender, litigar, reanudar o incluso modificar el *software* original acudiendo a un sistema arbitral que permita la intervención humana. El árbitro que se establezca dentro de la red *DLT* será el que establezca la red entre todos sus participantes, o el profesional independiente que establezcan las partes o incluso en el futuro podría ser un juez de la jurisdicción ordinaria con clave privada en la plataforma[39].

En todo caso, algunos autores como Wright o De Filippi, consideran que la actividad de la jurisdicción civil ordinaria, se vería reducida en el futuro si se implementasen estas soluciones o remedios dentro de la propia red *DLT.* Con la intervención de jueces o

[38] Raskin, M. (2017), *The Law and Legality of Smart Contracts*.
[39] Finck, M. (2019), *Smart Contracts as a Form of…*op. cit, pp. 13.

árbitros dentro de la *blockchain*, se reduciría enormemente el recurso de las partes a la jurisdicción ordinaria en los próximos años[40].

6. Conclusiones

Tras haber observado a lo largo de este trabajo las ventajas y numerosos retos que supone la aparición de nuevos instrumentos de ejecución contractual, como son los *legal smart contracts*, en conjunción con el uso de nuevas tecnologías (redes *DLT*), procedemos a establecer las principales conclusiones observadas.

Para conseguir una mayor implantación de los *legal smart contracts*, los equipos legales especializados en *blockchain* de las distintas redes *DLT*, junto con las autoridades legislativas competentes habrán de decidir cómo afrontar los numerosos retos, ya mencionados en este trabajo, que entraña el uso de este tipo de contrato.

En cuanto a la determinación de la responsabilidad de las partes que intervienen en la elaboración y ejecución de un *smart contract*, hemos concluido que se habrá de determinar atendiendo a lo dispuesto en el propio contrato y en su defecto o ante la nulidad de lo dispuesto, se determinará atendiendo a las condiciones generales de contratación a las que se adhirieron las partes o, en última instancia, a lo que establezcan las leyes que se desarrollen sobre la responsabilidad en estas nuevas tecnologías.

Por otra parte, en cuanto a la irreversibilidad de la ejecución automática, lo que se quiere conseguir es mitigar dicha irreversibilidad, para así evitar situaciones no deseadas por el derecho, sin perder la gran ventaja que supone la ejecución automática. Se pueden dar diversas soluciones a este problema. En primer lugar, se podrían codificar términos más complejos que comprueben oráculos más avanzados y fiables, aunque se introduzca un cierto nivel de confianza y subjetividad. Dicho proceso contribuiría enormemente a la requerida sofisticación de los *smart contracts*. Otra solución a este problema podría ser incorporar a contratos complejos de ejecutar una función *multisig*, de forma que existiese cierto control e intervención humana en su ejecución, aunque se perdiese cierto

[40] Wright, A. y De Filippi, P. (2015), *Decentralized Blockchain…*op. cit, pp. 6.

automatismo. En tercer lugar, algunas plataformas se plantean incorporar un sistema de arbitraje para dirimir conflictos sobre los *smart contracts* dentro de la propia red *DLT*. Consideramos que esta solución es muy prometedora y la desarrollamos con mayor amplitud en el quinto apartado de este trabajo. En resumen, todas las soluciones a la irreversibilidad de la ejecución necesariamente conjugan una mayor intervención humana, confianza y subjetividad, con la principal ventaja del uso de las *blockchain* que es la ejecución automática, sin intervención. En los próximos años podremos observar cómo se desarrollan estas tendencias que mitigan la irreversibilidad y qué intereses finalmente priman más (automatismo o control). Todas las soluciones buscadas tienen como fin conjugar un mayor control jurídico (por medio de árbitros en la *blockchain*, doble consentimiento al introducir la función *multisig*) y humano con la ejecución automática.

Si los consejos directivos de las plataformas de *blockchain*, junto con los distintos legisladores nacionales encuentran la forma de mejorar la seguridad jurídica de este método de ejecución y mantienen la eficiencia que aporta, es probable que en el futuro podamos observar un proceso de normalización de estos contratos, que nos lleve a una mayor implantación de los mismos en el trafico jurídico. Por tanto, la definición de estándares para los *legal smart contracts* es también una vía con un enorme potencial a la hora de resolver ese difícil equilibrio entre automatismo y tutela de los derechos de las partes. A través de este proceso de normalización, podrían preverse y resolverse la mayor parte de los potenciales conflictos que la ejecución de los *legal smart contracts* plantea. En definitiva, el reto principal aquí puede resumirse en la enorme dificultad que supone intentar codificar el universo de las posibles relaciones y transacciones jurídicas, así como su evolución temporal. Y hacerlo, además manteniendo la equidad entre las partes.

7. Bibliografía

7.1 Fuentes legales

Código Civil

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE 13 de julio de 2002).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

7.2 Obras doctrinales

Aguilera Silván, F-J. (2011), El objeto como elemento esencial del contrato. Artículos doctrinales, Noticias jurídicas. Consultado el 13/06/2019 de http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4648-el-objeto-como-elemento-esencial-del-contrato/.

Androulaki, E., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., … Laventman, G. (2018), Hyperledger fabric: a distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference on - EuroSys '18*. Consultado el 13/06/2019 de http://delivery.acm.org/10.1145/3200000/3190538/a30-androulaki.pdf?ip=79.146.112.146&id=3190538&acc=OA&key=4D4702B0C3E38B35%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35%2ED8F734396A7AA47F&__acm__=1560415537_5a4097130823cad1601de49ad02b5a65.

Catalini, C. y Gans, J.S. (2019), Some Simple Economics of the Blockchain. *Rotman School of Management Working Paper No. 2874598*; *MIT Sloan Research Paper No. 5191-16.* Consultado el 12/06/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598.

Egberts, A. (2017), The Oracle Problem - An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems. *EBS Law School.* Consultado el 04/06/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3382343.

ESMA. (2016), Discussion Paper: The Distributed Ledger Technology Applied to Securities Markets. Consultado el 15/04/2019 de https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf.

ESMA. (2017), Report: The Distributed Ledger Technology Applied to Securities Markets. Consultado el 15/04/2019 de https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf.

Faúndez, C. T. (2018), Smart contracts: análisis jurídico. *Madrid: Editorial Reus.* Consultado el 25/05/2019 de https://books.google.es/books?hl=es&lr=&id=wPFUDwAAQBAJ&oi=fnd&pg=PP1&dq=ejecucion+smart+contracts&ots=jLHh020E9P&sig=4Vx8z4_Gw8b2WfoololpKHrobTg#v=onepage&q=ejecucion%20smart%20contracts&f=false.

Finck, M. (2019), Smart Contracts as a Form of Solely Automated Processing Under the GDPR. *Max Planck Institute for Innovation & Competition Research Paper,* (19-01). Consultado el 03/06/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370.

Goorha, P. (2018), A Comprehensive Contracting Solution using Blockchains. *SSRN*, Consultado el 02/06/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3237076.

Ibáñez Jiménez, J. W. (2018), Blockchain: Primeras cuestiones en el ordenamiento español. *Madrid: Dykinson.*

Ibáñez Jiménez, J. W. (2018), Derecho de Blockchain y de la tecnología de registros distribuidos. *Navarra: Aranzadi.*

Kakavand, H., Kost De Sevres, N. y Chilton, B. (2017), The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. *SSRN*, Consultado el 12/04/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251.

Legerén-Molina, A. (2019), Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de blockchain. *Revista de Derecho Civil*, 6(1), 177-237. Consultado el 26/05/2019 de http://www.nreg.es/ojs/index.php/RDC/article/view/356.

Pilkington, M. (2015), Blockchain Technology: Principles and Applications. *Research Handbook on Digital Transformations*. Consultado el 13/04/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660.

Raskin, M. (2017), The Law and Legality of Smart Contracts. 1 Georgetown Law Technology Review 304. Consultado el 13/06/2019 de https://poseidon01.ssrn.com/delivery.php?ID=482106013031117019070113099094004111052032042016084026027093125022114101102029016109096023059100025126046118020075126030029067024015069044007119077095095124125113100052018084084122068081025031024012072100015096022119066027000015003068116001104089067025&EXT=pdf.

Werbach, K., & Cornell, N. (2017), Contracts ex machina. *Duke Law Journal*, 67, 313. Consultado el 26/05/2019 de https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj.

Wright, A. y De Filippi, P. (2015), Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN*, Consultado el 16/04/2019 de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

7.3 Otras fuentes

EU Blockchain Observatory and Forum. (2018), The legal and regulatory framework for blockchain and smart contracts. Consultado el 24/05/2019 de https://www.eublockchainforum.eu/reports.

ITU. (2017), Distributed ledger technologies and financial inclusion. *Focus group technical report, ITU-T*. Consultado el 13/06/2019 de https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-on-DLT-and-Financial-Inclusion.pdf.

ISO/TC 307. (2018), Blockchain and distributed ledger technologies. *ISO/TC 307/WG 1*. Consultado el 13/06/2019 de https://lists.hyperledger.org/g/perf-and-scale-wg/attachment/439/0/ISO-TC307_N0327_TC307_WG1_report.pdf.