



**COMILLAS**  
UNIVERSIDAD PONTIFICIA

ICAI

ICADE

CIHS

FACULTAD DE DERECHO

# **SMART CONTRACTS Y SU APLICACIÓN AL DERECHO MERCANTIL**

Análisis de sus funcionalidades, encaje jurídico  
y posibles aplicaciones

Autor: Carlos Estévez Rincón

5ºE3-A

Derecho Mercantil

Tutor: Prof. Fernando Vives Ruiz

Madrid  
Abril 2019

## RESUMEN

Existen numerosas áreas en las que el Derecho deberá ser actualizado mediante la digitalización. Una de ellas es la contratación privada que, a través del aprovechamiento de la *Distributed Ledger Technology* y su aplicación del *smart contract*, aspira a conseguir un proceso considerablemente más rápido, autónomo y eficiente.

El presente trabajo tiene como objetivo fundamental demostrar que tal aspiración es posible gracias a la aplicación del *smart contract* a través de sus múltiples cualidades. Para llevar a cabo dicha demostración se abordarán: las diferentes limitaciones de los contratos privados convencionales, el estudio de la naturaleza y funcionamiento de los *smart contracts*, sus ventajas, el encaje legal de su aplicación y, finalmente, la identificación de las diferentes áreas mercantiles en las que pueda ser aplicado.

**Palabras clave:** *smart contract*, *Distributed Ledger Technology*, *Blockchain*, encaje jurídico, aplicaciones, contrato convencional, limitaciones, derecho privado.

## **ABSTRACT**

There are numerous areas in which Law requires to be updated through digitization. One of them is the private contracting process which, through the use of the Distributed Ledger Technology and its smart contract application, aims to achieve a considerably faster, more autonomous and more efficient procedure.

The main goal of the present paper is to prove that such aspiration is possible, thanks to the implementation of the smart contract application, through its multiple qualities. In order to carry out such demonstration, the following issues will be addressed: the various limitations of conventional private contracts, the study of the nature and functioning of the smart contracts, their advantages, the legal framework of their application and, finally, the identification of the different commercial areas in which they can be applied.

**Key words: smart contract, Distributed Ledger Technology, Blockchain, legal framework, applications, conventional contract, limitations, Private Law.**

## ACRÓNIMOS

DLT	Distributed Ledger Technology
BC	Blockchain
SC	smart contract
PL	Public Ledger
IoT	Internet of Things
IA	Inteligencia Artificial
CC	Código Civil
TS	Tribunal Supremo
BTC	Bitcoin
EDI	Electronic Data Interchange
ID	Identidad
TRLGCU	Texto Refundido que aprueba la Ley General de Consumidores y Usuarios
LCGC	Ley de Condiciones Generales de Contratación
LSSI	Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico
API	Application Programming Interface
P2P	Peer to Peer

ITO Initial Token Offering

## ÍNDICE DE CONTENIDOS

<b>1. INTRODUCCIÓN .....</b>	<b>1</b>
<b>1.1 Objetivos .....</b>	<b>1</b>
<b>1.2 Metodología .....</b>	<b>1</b>
<b>1.3 Estado de la cuestión.....</b>	<b>2</b>
<i>1.3.1 Limitaciones de los contratos privados convencionales .....</i>	<i>2</i>
<i>1.2 Blockchain y smart contracts.....</i>	<i>4</i>
<b>2. FUNCIONAMIENTO, CARACTERÍSTICAS, Y VENTAJAS DE LOS SC .....</b>	<b>6</b>
<b>2.1 Cadena de bloques .....</b>	<b>6</b>
<b>2.2 Ejemplo de configuración de un <i>smart contract</i>:.....</b>	<b>8</b>
<b>2.3 Naturaleza del <i>smart contract</i>.....</b>	<b>11</b>
<b>2.3.1 Naturaleza condicional.....</b>	<b>11</b>
<b>2.3.1.1 Vertiente lógica .....</b>	<b>11</b>
<b>2.3.1.2 Vertiente jurídica.....</b>	<b>11</b>
<b>2.3.2 Software auto ejecutable.....</b>	<b>12</b>
<b>2.3.3 Naturaleza del objeto de las prestaciones de un <i>SC</i>.....</b>	<b>13</b>
<b>2.4 Redes permissionadas vs redes no permissionadas (privadas vs públicas) .....</b>	<b>13</b>
<b>2.4.1 Redes no permissionadas (abiertas).....</b>	<b>13</b>
<b>2.4.2 Redes permissionadas (cerradas).....</b>	<b>14</b>
<b>2.5 Ventajas que puede aportar la BC a la contratación.....</b>	<b>14</b>
<b>2.5.1 Ejecución rápida y autónoma.....</b>	<b>14</b>
<b>2.5.2 Posibilidad de desintermediación en su BC.....</b>	<b>16</b>
<b>2.5.3 Autogobierno sobre identidad y privacidad.....</b>	<b>16</b>
<b>2.5.4 Transparencia .....</b>	<b>17</b>
<b>2.5.5 Confianza.....</b>	<b>20</b>
<b>2.5.6 Desarrollo en software .....</b>	<b>21</b>

2.5.7 Seguridad e inmutabilidad.....	22
2.5.8 Posible coordinación con Internet de las Cosas .....	23
<b>3. LIMITACIONES EN LA APLICACIÓN DE LOS SC: ANÁLISIS JURÍDICO.....</b>	<b>25</b>
<b>3.1 Sobre los elementos esenciales para la validez del contrato.....</b>	<b>25</b>
3.1.1 Consentimiento de los contratantes.....	25
3.1.1.1 Sobre la redacción de los SC .....	27
3.1.1.2 Sobre los contratos estandarizados y contratos de consumo.....	28
3.1.2 El objeto cierto que sea materia del contrato.....	30
3.1.2.1 Imposibilidad de incumplimiento .....	30
3.1.2.2 Análisis jurídico de las condiciones de ejecución de un SC.....	31
3.1.3 Causa válida que se establezca .....	32
<b>3.2 Sobre la forma de los contratos .....</b>	<b>32</b>
3.3.1 La forma y el lenguaje de los SC.....	33
3.3.2 Requisitos de forma del contrato.....	33
<b>3.3 Necesidad de objetivación de la realidad.....</b>	<b>34</b>
a) Los datos requieren de una valoración subjetiva .....	35
b) Los datos pueden ser fácilmente objetivables por dispositivos: oráculos.....	35
<b>3.4 Sobre la legalidad del contenido de los SC .....</b>	<b>37</b>
<b>3.5 Sobre la ejecución de los SC.....</b>	<b>38</b>
3.5.1 Análisis de la ejecución de los SC .....	38
3.5.2 Problemas en cuanto al automatismo y la irreversibilidad .....	38
3.5.3 Problemas en cuanto a la ejecución de las consecuencias del incumplimiento..	40
3.5.4 Mención sobre los remedios ante la ejecución defectuosa.....	40
<b>3.6 Sobre la prueba de los smart contracts en el proceso .....</b>	<b>40</b>
<b>3.7 Sobre la función del abogado, juez, notario y registrador .....</b>	<b>41</b>
Especial mención al Derecho notarial y registral.....	42

<b>4. APLICACIONES MÁS PRÓXIMAS DE LOS SMART CONTRACTS AL DERECHO MERCANTIL .....</b>	<b>44</b>
<b>4.1 Comercio electrónico .....</b>	<b>44</b>
<i>4.1.1. Generación de confianza entre los clientes.....</i>	<i>44</i>
<i>4.1.2 Minimización de los costes de transacción .....</i>	<i>44</i>
<i>4.1.3 Control de ventas secundarias.....</i>	<i>45</i>
<b>4.2 Propiedad Intelectual.....</b>	<b>45</b>
<b>4.3 Sector financiero .....</b>	<b>46</b>
<i>4.3.1 Banca comercial.....</i>	<i>46</i>
<i>4.3.1.1 Sistema de pagos y transferencias a distancia .....</i>	<i>46</i>
<i>4.3.1.2 Compensación de créditos.....</i>	<i>46</i>
<i>4.3.1.3 Contabilidad y registro.....</i>	<i>47</i>
<i>4.3.2 Banca de inversión.....</i>	<i>47</i>
<i>4.3.3 Financiación de proyectos empresariales .....</i>	<i>48</i>
<i>4.3.4 Contrato Escrow desintermediado.....</i>	<i>49</i>
<i>4.3.5 Sistema monetario.....</i>	<i>49</i>
<b>4.4 Sector asegurador .....</b>	<b>49</b>
<b>4.5 Logística y trazabilidad .....</b>	<b>50</b>
<b>5. CONCLUSIONES.....</b>	<b>52</b>
<b>Bibliografía .....</b>	<b>55</b>
<b>1. Legislación .....</b>	<b>55</b>
<i>Europea: .....</i>	<i>55</i>
<i>Nacional: .....</i>	<i>55</i>
<b>2. Jurisprudencia.....</b>	<b>55</b>
<b>3. Obras doctrinales .....</b>	<b>56</b>



## **1. INTRODUCCIÓN**

### **1.1 Objetivos**

Este trabajo de investigación académica tiene como principal objetivo estudiar la naturaleza del *smart contract* y sus posibles aplicaciones al derecho privado. Para ello, será preciso realizar un análisis sobre el encaje dentro del marco legal actual y las posibles implicaciones jurídicas de su implantación.

El interés de este campo deriva de la multitud de funcionalidades que tales elementos poseen y las diferentes implementaciones y aplicaciones que pueden tener en el derecho privado.

### **1.2 Metodología**

En lo relativo a la metodología utilizada, en primer lugar, se ha recopilado y analizado información de diversas fuentes para definir el marco en el que se va a encuadrar el trabajo de investigación. Para tal cometido, se ha realizado una revisión de la bibliografía contenida en artículos, páginas web y papers relacionados con la materia, así como de la regulación aplicable.

El trabajo se ha estructurado de la siguiente manera: en primer lugar, se analiza los problemas que los contratos convencionales pueden plantear, posteriormente se presenta el *smart contract* (su concepto, naturaleza y funcionamiento) y se analiza las diferentes aportaciones en cuanto a funcionalidades adicionales que puedan completar la operatividad de los contratos convencionales. Finalmente, se realiza un estudio detallado sobre cuáles son las diversas aportaciones que aquéllos presentan para el derecho privado.

En lo respectivo a las fuentes empleadas, cabe destacar dos aspectos. En primer lugar, que al ser los SC basados en tecnologías de registro distribuido (DLT – *Distributed Ledger*

*Technology*) un fenómeno de reciente aparición<sup>1</sup> y al tener una fuerte implicación tecnológica, una parte relevante de las fuentes han sido artículos doctrinales, papers de iniciativas de desarrollo de proyectos de *Blockchain* y páginas web. En segundo lugar, al tratarse de un asunto especialmente desarrollado en el mundo anglosajón, una gran cantidad de las fuentes consultadas y referenciadas han sido en lengua inglesa. Habida cuenta de que, además de analizar el escaso contenido existente en castellano sobre la materia, hace un análisis integral sobre el tema en la misma lengua, este trabajo presenta un valor añadido especialmente meritorio para el campo de la contratación privada y la aplicación de la tecnología DLT al Derecho español.

### 1.3 Estado de la cuestión

#### 1.3.1 Limitaciones de los contratos privados convencionales

Hoy en día, los contratos privados convencionales padecen alguna (si no la totalidad) de las siguientes insuficiencias o limitaciones (algunas de las cuales se hacen patentes especialmente con la aparición de entornos operativos o transaccionales automatizados a gran escala):

#### **A. Su cumplimiento no está garantizado de antemano**

Se pueden diferenciar cuatro tipos de situaciones posibles respecto al cumplimiento en relación con las expectativas del acreedor<sup>2</sup>: a) cumplimiento (se ha realizado la obligación según lo esperado); b) cumplimiento defectuoso (se ha llevado a cabo la ejecución de forma irregular, no cumpliendo satisfactoriamente lo esperable en cuanto a medios o resultado); c) cumplimiento tardío (se lleva a cabo satisfactoriamente la obligación, pero no en el momento debido); y d) incumplimiento (no se lleva a cabo la obligación). Pues bien, en los contratos convencionales privados la confianza en que la ejecución sea correcta, y según lo esperado en

---

<sup>1</sup> El concepto de “Smart Contract” se formuló por Nick Szabo a mediados de los 90, aunque no asociado a las tecnologías DLT/*Blockchain*. Los entornos basados en estas tecnologías sí que son más recientes, pero a su vez se fundamentan en una combinación de tecnologías que ya existían anteriormente.

<sup>2</sup> GOMEZ POMAR, F., *El incumplimiento contractual en el Derecho español*. Publicado en Revista para el Análisis del Derecho, vol. 3, 2007 (p. 17).

cuanto a tiempo y forma, no se encuentra en el contrato en sí<sup>3</sup>, sino en las acciones humanas de las partes, de terceros o de las circunstancias que pudieran afectarle<sup>4</sup>.

### **B. Costes del contrato**

Existen múltiples gastos en los que puede incurrirse a la hora de formalizar un contrato. Éstos variarán dependiendo de cuál se trate y de las condiciones que le afecten en cuanto a los trámites que deba seguir<sup>5</sup>. Por lo general, estos costes pueden ser de dos tipos: a) costes de tramitación (elevarlo a público, registrarlo, pago de impuestos etc.) y/o b) costes de asesoramiento legal (pago al profesional del Derecho).

### **C. Pueden estar afectados por fallos de causa humana**

Habida cuenta de que quienes intervienen en su redacción o formalización son humanos, las cláusulas que los componen pueden contener fallos en su contenido: no sólo en su semántica sino, también, por no cubrir la totalidad de la casuística deseada<sup>6</sup> bien sea por errores u olvidos. Además de los fallos en cuanto a su formalización, existen otros que también pueden afectarle, dada la naturaleza humana de aquellos individuos que crean la ley (errores del legislador) o que la aplican (errores de jueces y tribunales)<sup>7</sup>.

### **D. Pueden ser deteriorados, perdidos o, malintencionadamente modificados**

Independientemente de la forma final que el contrato adopte, ésta no es inmutable: los archivos o documentos en los que conste registrado el contrato están sujetos a su posible manipulación, deterioro o pérdida. Incluso si éste se encontrara custodiado en un registro, el mismo podría

---

<sup>3</sup> LEGERÉN-MOLINA, A., *Los contratos Inteligentes en España: la disciplina de los smart contracts* publicado en la Revista de Derecho Civil (vol. V, núm. 2) en abril-junio de 2018 (p. 200).

<sup>4</sup> GAYLE HYMAN, M. y DIGESTI MATTHEW P., *New Nevada legislation recognizes Blockchain and Smart Contract technologies*, junio de 2017 (p.1).

<sup>5</sup> Baste como ejemplo mencionar las tarifas notariales y registrales (*Instrucción de 22 de mayo de 2002, de la Dirección General de los Registros y el Notariado, por la que se convierten a euros los Aranceles de los Notarios y Registradores de la Propiedad y Mercantiles*): <https://www.boe.es/buscar/doc.php?id=BOE-A-2002-12290> (Consulta válida a 20/03/19) o los honorarios que cobra el abogado, que variará según el tipo de asesoría legal, consulta o defensa.

<sup>6</sup> GROSSMAN SANFORD, J. y OLIVER, H., *The costs and benefits of ownership: A theory of vertical and lateral integration*, *Journal of Political Economy*, 1986 (p. 698).

<sup>7</sup> SEGURA ORTEGA, M., *Problemas interpretativos e indeterminación del Derecho*. Publicado en revista *Derecho* (vol 22) en noviembre de 2013 (p. 677). El profesor Segura realiza una aproximación sobre los fallos en la aplicación judicial en su apartado *Efectos de la indeterminación en la actividad judicial*. En este epígrafe destaca como segunda indeterminación del Derecho el propio de la actividad de su aplicación llevada a cabo por los jueces. En él analiza cómo aumentar el peso del aplicador del Derecho sobre el del legislador puede llevar a una excesiva indeterminación ante la flexibilidad aumentada de aquéllos.

sufrir un accidente inesperado (*i.e. un incendio*) o desaparecer. Además, quien custodia el documento en el que se recoge el contrato podría llegar a modificar o falsificar malintencionadamente su contenido para alterar la realidad jurídica que afecta a las partes.

### **E. Su coordinación con las nuevas tecnologías es lenta y difícil (si no imposible)**

Por no haber sido concebidos para tal fin, la formulación de acuerdos contractuales no facilita la integración de sus previsiones y su programa de ejecución para provocar consecuencias y desencadenar efectos en entornos transaccionales automatizados (como los basados en IoT o la IA, con algunas excepciones muy anecdóticas como la operativa de las máquinas de vending<sup>8</sup>).

## **1.2 Blockchain y smart contracts**

Teniendo en cuenta lo anteriormente mencionado sobre las limitaciones de los contratos privados convencionales, en 1996 el ingeniero informático americano Nick Szabo publica *Smart Contracts: Building Blocks for Digital Markets*<sup>9</sup>, un white paper en el que se construye un nuevo concepto denominado *smart contract* (en adelante SC) presentado por el autor como un invento que cambiaría por completo la forma de llevar a cabo contratos en la sociedad<sup>10</sup>. El así definido<sup>11</sup> como contrato inteligente<sup>12</sup>, se conceptualizó como un software cuyo contenido

---

<sup>8</sup> La venta a través de las máquinas de vending representa el ejemplo paradigmático a la hora de explicar el concepto de *smart contract*. Fue propuesto por Nick Szabo (creador del SC) como la modalidad más primaria de contrato inteligente que podía ser concebida: *la máquina toma las monedas y, a través de un simple mecanismo automatizado, devuelve el cambio y el producto seleccionado*.

<sup>9</sup> SZABO, N., *Smart Contracts: Building Blocks for Digital Markets*, 1996. Disponible en [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html) Consulta válida a 21/3/2019.

<sup>10</sup> Prácticamente al inicio del documento, el autor señala lo siguiente: “[...] a broad statement of the key idea of smart contracts, then, is to say that contracts should be embedded in the world”. Lo que podría traducirse como “[...] una amplia afirmación sobre la idea de los contratos inteligentes sería que éstos debieran estar integrados en el mundo”.

<sup>11</sup> Cabe destacar que, aunque el concepto de SC fue ideado por Nick Szabo en 1996, no fue hasta el 2013 cuando realmente fue desarrollado de forma eficaz. Sus creadores, haciendo homenaje al ingeniero informático, decidieron denominarlo de esta manera. No obstante, el software programado no ostentaba la condición de contrato, únicamente decidieron apodar así a la secuencia de código informático que tuviera la capacidad de ejecutar de manera automática prestaciones propias de un verdadero contrato.

<sup>12</sup> En lo que respecta a la terminología empleada en el trabajo, se hará uso de manera indistinta de términos en español e inglés para referirnos al mismo concepto (*i.e. smart contract - contrato inteligente o Blockchain – cadena de bloques*) únicamente por motivos de estilo literario y como forma de evitar redundancias.

consistía en un conjunto de instrucciones destinadas a ser ejecutadas sin intervención humana<sup>13</sup>, desplegando los efectos jurídicos propios de un contrato<sup>14</sup>.

La idea de los SC, de difícil implementación<sup>15</sup> más allá de operativas muy concretas, ha tomado forma y aplicación práctica sólida dentro de las redes basadas en *Blockchain* o en DLTs como una de sus aplicaciones. Partiendo de esta base, procedemos al análisis de la proposición de valor que los SC presentan respecto a los contratos convencionales y que, fundamentalmente, se basa en su capacidad para completar su efectividad de asegurar el cumplimiento de las prestaciones pactadas, así como de la no ejecución de aquéllos respecto de los que no se han cumplido las condiciones establecidas; para finalmente estudiar si es jurídicamente viable su aplicación al derecho Privado.

---

<sup>13</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 56).

<sup>14</sup> LEGERÉN-MOLINA, A., *Los contratos Inteligentes en España: la disciplina de los smart contracts*. Publicado en Revista de Derecho Civil, (vol. V, núm. 2) en abril-junio, 2018 (p. 194).

<sup>15</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 88). El autor reconoce que un SC no se convierte en contrato por el mero hecho de integrar en su código fuente condiciones programadas con transcendencia jurídica, motivo por el cual existen múltiples iniciativas por parte de los desarrolladores de Solidity (principal lenguaje de programación en el que se basan los SC) para crear una correcta integración entre la traducción del SC en un contrato convencional y su ejecución propia reflejada en un SC puro.

## 2. FUNCIONAMIENTO, CARACTERÍSTICAS, Y VENTAJAS DE LOS SC

### 2.1 Cadena de bloques

Como anteriormente se ha comentado, los contratos inteligentes han sido desarrollados sobre la base de la tecnología comúnmente conocida como *Blockchain* (en adelante BC). Ésta se fundamenta, principalmente, en la utilización de una base de datos descentralizada (en lugar de una base de datos única centralizada custodiada por un nodo central único) que registra en cada una de las réplicas distribuidas de la base de datos aquellas transacciones e interacciones que se producen entre los usuarios de una red, utilizando criptografía de clave pública asimétrica<sup>16</sup> (para evitar que se alteren los registros de las bases de datos) y un algoritmo de consenso que permite asegurar la consistencia de los registros de transacciones (evitando que se generen transacciones falsas y que existan divergencias entre las réplicas de la base de datos descentralizada). La base de datos se configura a partir de distintos bloques que van incluyendo el registro de diversas transacciones validadas y, a su vez, cada nuevo bloque queda enlazado al bloque anterior formando una cadena.

Cuando las interacciones completas son validadas en la red, son almacenadas en dicha base de datos o libro mayor (PL - *public ledger*) que, a través de múltiples procesos tecnológicos<sup>17</sup>, consigue reunir las características de veracidad, seguridad y transparencia<sup>18</sup>, configurando un entorno a prueba de manipulación. En la red participan unos computadores (denominados nodos) que recolectan todas las interacciones que tienen lugar entre los miembros que forman parte de la comunidad y las empaquetan en un bloque.

La validación de estos bloques puede llevarse a cabo de formas diversas, dependiendo del algoritmo de consenso<sup>19</sup>. Normalmente éstos están fundamentados en que los nodos validadores

---

<sup>16</sup> GUTIÉRREZ, P., *Tipos de criptografía: simétrica, asimétrica e híbrida*.

<https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida> (párrafo 6º). Consulta válida a 3/4/2019.

<sup>17</sup> BUTERIN, V., *Ethereum White Paper: A next generation smart contract & decentralized application platform*, 2013. (p. 2 y ss.). Disponible en: [http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf) Consulta válida a 21/3/2019.

<sup>18</sup> NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009. Disponible en: <https://bitcoin.org/bitcoin.pdf> Consulta válida a 21/3/2019.

<sup>19</sup> Explicación de los algoritmos de consenso en: <https://medium.com/coinbundle/consensus-algorithms-dfa4f355259d> (párrafo 6º). Consulta válida a 2/4/2019.

de la red resuelvan complejos cálculos matemáticos<sup>20</sup> hasta poder validar el contenido del mencionado bloque, lo que a su vez permite aportar un elevado nivel de seguridad y generar un entorno a prueba de manipulación. Entre los principales métodos de validación encontramos los siguientes<sup>2122</sup>:

- Proof of Work: se fundamenta en la atribución de un incentivo a aquel nodo (minero) que primero valida el bloque.
- Proof of Stake: el premio corresponde a un validador aleatoriamente elegido, siendo la posibilidad de ser seleccionado directamente proporcional a las monedas virtuales de que dispone.

No obstante, existen otros modelos de consenso (que no entraremos a valorar por cuestiones de espacio), teniendo cada uno de ellos sus virtudes y sus defectos. Gracias al proceso anteriormente mencionado, la cadena de bloques goza de las virtudes de descentralización e inmutabilidad<sup>23</sup>. Dicha descentralización, junto con la utilización de criptografía y funciones de hash soportadas por un alto poder de computación, proporcionan una gran resistencia ante ataques informáticos y solidez ante posibles manipulaciones.

La explicada tecnología de la cadena de bloques tenía como propósito inicial ser aplicada únicamente a transacciones en las que se validasen los parámetros de: emisor, receptor y cantidad transaccionada<sup>24</sup>. No obstante, en 2013 el ingeniero informático ruso Vitalik Buterin decide extender el concepto abstracto de los *smart contracts* planteados por Szabo<sup>25</sup> a la tecnología propuesta por Satoshi Nakamoto<sup>26</sup> para el desarrollo del Bitcoin (en lo sucesivo,

---

<sup>20</sup> SEANG, S. y TORRE, D., *Proof of Work and Proof of Stake consensus protocols: a Blockchain application for local complementary currencies*, 2018. En este paper se hace un análisis detallado de cómo se produce la validación por nodos. Disponible en: <https://gdre-scpo-aix.sciencesconf.org/195470/document> Consulta válida a 5/4/2019.

<sup>21</sup> NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009 (p. 3). Disponible en: <https://bitcoin.org/bitcoin.pdf> Consulta válida a 21/3/2019.

<sup>22</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 31).

<sup>23</sup> <https://medium.com/@Disruptpreneur/an-introduction-to-cryptoassets-7be277c6bead> (párrafo 7º). Consulta válida a 22/3/2019.

<sup>24</sup> NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009 (p. 1). Disponible en: <https://bitcoin.org/bitcoin.pdf> Consulta válida a 21/3/2019.

<sup>25</sup> SZABO, N., *Smart Contracts: Building Blocks for Digital Markets*, 1996. Disponible en [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo\\_best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo_best.vwh.net/smart_contracts_2.html) Consulta válida a 21/3/2019

<sup>26</sup> No se conoce la identidad real del autor del protocolo de Bitcoin, que se publicó bajo el pseudónimo de Satoshi Nakamoto. De hecho, ni siquiera se conoce si fue una persona concreta o un grupo de desarrolladores.

BTC) en su white paper *Bitcoin: A Peer-to-Peer Electronic Cash System*<sup>27</sup>. De esta forma, ya no se tendrían en cuenta sólo tales inputs y outputs (emisor, receptor y cantidad), sino que también pasarían a formar parte de la cadena de bloques los parámetros propios de un contrato: partes, obligaciones de dar o hacer y condiciones a las que se debe llevar a cabo (tiempo, lugar y forma). Tras avanzarse en el estudio e implementaciones del concepto de SC, en la actualidad se ha desarrollado una tecnología capaz de reunir todas las características que anteriormente afirmábamos para simples transacciones de dinero, y aplicarlas a los SC, gozando así éstos de las propiedades de inmutabilidad, descentralización, transparencia y seguridad.

```
pragma solidity ^0.4.17;
contract SimpleDeposit {
    mapping (address => uint) balances;

    event LogDepositMade(address from, uint amount);

    modifier minAmount(uint amount) {
        require(msg.value >= amount);
        _;
    }

    function SimpleDeposit() public payable {
        balances[msg.sender] = msg.value;
    }

    function deposit() public payable minAmount(1 ether)
    {
        balances[msg.sender] += msg.value;
        LogDepositMade(msg.sender, msg.value);
    }

    function getBalance() public view returns (uint
        balance) {
        return balances[msg.sender];
    }

    function withdraw(uint amount) public {
        if (balances[msg.sender] >= amount) {
            balances[msg.sender] -= amount;
            msg.sender.transfer(amount);
        }
    }
}
```

A la izquierda se puede observar un ejemplo extremadamente simple de un smart contract en el que se detallan:

- Tipo de contrato (2)
- Acción de dar (5)
- Partes del contrato (13)
- Ejecución del contrato y circunstancias en las que ésta se da (12-28)

*Ejemplo de programación de smart contract*

## 2.2 Ejemplo de configuración de un smart contract:

Para explicar con términos sencillos la configuración de los posibles términos que vertebran un SC (sin recurrir a conceptos de ingeniería informática ni desarrollo de software) acudiremos al ejemplo expuesto por MATTILA J. y SEPPÄLÄ T. en su obra *Smart Contracts: How will*

<sup>27</sup> BUTERIN, V., *Ethereum White Paper: A next generation smart contract & decentralized application platform*, 2013. (p. 2 y ss.). Disponible en: [http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf) Consulta válida a 21/3/2019.



*Blockchain Technology Affect Contractual Practices*<sup>28</sup>. No obstante, el propio ejemplo ha sido desarrollado y ampliado por quien escribe para detallar en mejor medida tanto el funcionamiento como las condiciones propias de un contrato inteligente.

*Supongamos la celebración de un contrato de prestación de servicios por parte de una empresa (A) con otra (B) consistente en la mejora de posicionamiento de (B) en búsquedas de Internet a cambio del pago de una determinada cantidad (de B a A). De esta manera, el contrato inteligente debe llevar a cabo dos funciones básicas: (1) la comprobación de que el servicio ha sido llevado a cabo satisfactoriamente<sup>29</sup> y (2) en caso de que así haya sido, ejecutar la contraprestación del contrato (transferencia de dinero<sup>30</sup>). El contrato inteligente quedaría redactado en los siguientes términos<sup>31</sup>:*

---

<sup>28</sup> MATTILA, J. y SEPPÄLÄ, T., *Smart Contracts: How will Blockchain Technology Affect Contractual Practices*. Publicado por The Research Institute of the Finnish Economy (vol. 68) en enero de 2017 (p. 18).

<sup>29</sup> En el ejemplo planteado por los investigadores finlandeses tal servicio es el posicionamiento entre los tres mejores resultados de búsqueda.

<sup>30</sup> Esta transferencia sería algo similar a la dispuesta en el contrato programado de la página anterior (*function: deposit*).

<sup>31</sup> Por motivos de espacio y, sobre todo técnica, el contrato dispuesto tiene lenguaje castellano imitando las funcionalidades que dispondría uno redactado en código de programación. No obstante, pretende reproducir la lógica del lenguaje que éste estructuraría.

***Términos del contrato:***

1. *Contrato de servicios*
2. *Tipo de servicio: posicionamiento web*
3. *Web para posicionar: www.ejemplo.com*
4. *Web en la que se realiza posicionamiento (W): www.google.es*
5. *Posicionamiento:*
6. *Condición (C):  $V.M \leq V.X \leq V.m$*
7. *Si, cumplimiento de Condición (C); entonces, pago*
8. *Si, no cumplimiento de Condición (C); entonces, no pago*
9. *Definición de valores:*
10. *V.M: valor máximo: 1º posición en (W)*
11. *V.m: valor mínimo: 3º posición en (W)*
12. *V.X: valor realizado: input final (I)*
13. *Valor final: Input (I)*
14. *Función: pago*
15. *Pago: entrega de Cantidad (€) de C.A a C.B*
16. *Cantidad: 5.000 €*
17. *Cartera A (C.A): cuenta bancaria de empresa A*
18. *Cartera B (C.B): cuenta bancaria de empresa B*
19. *¿Input (I)?*

Como puede observarse, quedan definidas tanto las partes como el evento que activa la ejecución (incluso la propia ejecución). Únicamente quedaría a la espera de la introducción de un campo input (I) para que fuese ejecutado. Tal dato vendría proporcionado por un elemento externo al SC -sea desde dentro de la propia red *Blockchain*, de una fuente online ajena a la misma o, incluso, del mundo físico- denominado oráculo (que será posteriormente analizado en el apartado 3.3: *Necesidad de objetivación de la realidad*).

Como también puede comprobarse en la lógica del lenguaje, tanto la *no introducción* de este campo (nunca se llega a comprobar) como la *introducción y no cumplimiento satisfactorio* (se comprueba, pero no satisface la condición) son posibles y, en cualquier escenario, válidas en cuanto a los intereses del cliente de la empresa prestadora de servicios se refiere.

## **2.3 Naturaleza del *smart contract***

### **2.3.1 Naturaleza condicional**

Como se ha podido comprobar en el apartado anterior, los SC poseen una ejecución condicionada tanto en su vertiente lógica como jurídica:

#### **2.3.1.1 Vertiente lógica**

Como software programado que son, los SC disponen secuencias de códigos que muestran de forma proposicional una sucesión de condiciones con la estructura *if/then/else*: si A, X; si no A, Y. Esta construcción hace del sistema una ramificación binaria de *consecuencias* a través del cumplimiento de condicionantes: siguiendo con la estructura anterior, primero se valida la condición A (verdadero/falso); de darse la verdad, se ejecuta la consecuencia X; de no darse, se procede a la ejecución de la consecuencia Y.

#### **2.3.1.2 Vertiente jurídica**

Esta estructura lógica de condicionantes hace que los contratos inteligentes tengan la naturaleza jurídica de obligaciones sujetas a condición (arts. 1113 a 1124 CC). La principal diferencia entre las obligaciones puras y las condicionadas reside en que éstas dependen de un suceso o acontecimiento futuro e incierto, del que las partes hacen depender la eficacia del negocio<sup>32</sup>. Como se ha podido comprobar anteriormente, esta condición podrá ser satisfecha (o no) por el suceso, que en este caso dependerá de la introducción del input. En virtud de lo dispuesto en el art. 1114 CC, y dependiendo de los efectos que provoque tal input de información, la mencionada condición podría tener carácter suspensivo (la obligación no despliega efectos hasta el cumplimiento de aquella *-i.e. ejemplo de posicionamiento en motor de búsqueda del apartado 2.2-*) o resolutorio (los efectos cesan cuando aquella tiene lugar *-i.e. empresa eléctrica deja de suministrar luz a un hogar en caso de impago durante un número determinado de mensualidades-*).

---

<sup>32</sup> ARIJA SOUTULLO, C., *La condición en el contrato. Inscripción en el Registro de la Propiedad*, publicado en la Revista de Derecho Civil (vol. V, núm. 2) en abril-junio de 2018 (p. 282).

### **2.3.2 Software auto ejecutable**

Como habíamos comentado anteriormente, el SC consiste en un conjunto de condiciones expresadas en código informático que posibilitan su ejecución de forma automática. Estas condiciones pueden haber sido directamente redactadas en lenguaje de programación o haberse trasladado previamente desde un contrato convencional escrito en lenguaje común (ya sea a través de una simple traducción de sus condiciones, o bien redactándose un contrato convencional vinculante formulado posteriormente en código).

Generalmente, el primer tipo es apto para entornos expertos o automatizados si existe un marco de contratación que lo habilita (como ocurría en su día en los entornos EDI – Electronic Data Interchange<sup>33</sup> entre empresarios), mientras que el segundo tipo de uso procederá cuando las partes sean consumidores o no dispongan de los conocimientos necesarios para entender y valorar el contenido de la expresión de su voluntad.

Teniendo en cuenta la explicación anterior cabe realizar dos aclaraciones:

1. Todos los SC son contratos de soporte digital, pero no todos los contratos digitales son SC. La diferencia básica y fundamental en éstos es la programación de sus condiciones en lenguaje informático (y su consiguiente característica de auto ejecución).
2. Cabe la posibilidad de que un SC no afecte a la totalidad de un contrato (SC puros), sino sólo a una determinada parte del mismo (SC híbridos o contratos legales inteligentes), perteneciendo la otra a un contrato convencional y utilizándose el código para determinadas funcionalidades: ejecución material o almacenamiento de datos. *Es precisamente éste último tipo sobre el que llevaremos a cabo la mayoría del estudio en el presente trabajo, dada su mayor facilidad de aplicación (en una primera fase) en el sistema legal actual*<sup>3435</sup>.

---

<sup>33</sup> *What is EDI?:* [https://www.up.com/suppliers/order\\_inv/edi/what\\_is\\_edi/](https://www.up.com/suppliers/order_inv/edi/what_is_edi/) (párrafo 1º). Consulta válida a 3/4/2019.

<sup>34</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 88).

<sup>35</sup> Solución de integrar un contrato legal inteligente en un SC puro propuesta por BRAENDGAARD, P. en *Simple Convention for Human Readable Terms for Smart Contracts:* <https://blog.stakeventures.com/articles/smart-contract-terms> (párrafo 9º). Consulta válida a 6/4/2019.

### **2.3.3 Naturaleza del objeto de las prestaciones de un SC**

Como contratos, los SC tienen por objeto la realización de prestaciones de dar, hacer o no hacer. Al poder estar conectado con el mundo exterior a la cadena de bloques (off-chain), los SC pueden tener por objeto prestaciones tanto sobre activos alcanzables dentro de la propia BC (*i.e. entrega de criptomonedas o criptotokens*) como fuera de la misma (*i.e. suministro de luz por una compañía eléctrica*).

## **2.4 Redes permissionadas vs redes no permissionadas (privadas vs públicas)**

Dependiendo del nivel de descentralización en la validación del consenso en la cadena de bloques, podemos diferenciar entre redes permissionadas y no permissionadas (o abiertas y cerradas). Por otro lado, podemos diferenciar redes en función de si los datos que contienen son públicos (redes públicas) o no (redes privadas).

### **2.4.1 Redes no permissionadas (abiertas)**

En estas BC cualquier persona puede unirse al sistema y participar del protocolo común. Estas redes son descentralizadas y nadie tiene el control sobre ellas. Una vez validados los datos en su cadena, no se pueden modificar. Sus ventajas son que sus validaciones son anónimas y escalables, mientras que entre sus desventajas podemos destacar que es más lenta (dado el nivel de participantes) y que es más propensa a recibir ataques (pueden introducirse agentes no deseados).

Ejemplos de pública abierta: *criptomonedas públicas como Bitcoin en las que se conoce qué carteras realizan la transacción, en qué momento y el valor de la misma. En ellas las transacciones son validadas de forma pública.*

Un ejemplo de privada abierta sería *el voto en unas elecciones gestionado en DLT, en las que los datos sobre quién vota y a qué partido son privados, pero la validación de ellos es pública.*

### **2.4.2 Redes permissionadas (cerradas)**

Los usuarios que están dentro de la cadena tienen derecho a decidir si permiten el acceso a nuevos integrantes (existen diferentes métodos de tomar esta decisión, aunque la comúnmente llevada a cabo es la democrática). Generalmente son centralizadas: los validadores son pocos y bien definidos. Sus principales ventajas son: que es más rápida (menor número de participantes), y que tiene mayor control sobre posibles amenazas externas; mientras que sus mayores desventajas son que su gestión puede no ser transparente (sus validadores se coordinan al margen de los usuarios), que no genera total confianza (depende de la voluntad y gestión de los validadores) y que su escalabilidad es más limitada.

Ejemplos de red cerrada son *informes financieros de empresas o balanza de pagos del exterior. En ellas los datos son públicos, pero se validan de forma privada.*

Ejemplos de privada cerrada: *declaraciones de Hacienda o informes militares, los datos son privados y se validan de forma privada.*

## **2.5 Ventajas que puede aportar la BC a la contratación**

Basándonos en lo anteriormente expuesto, en el siguiente apartado procederemos al análisis de las diferentes proposiciones de valor que los contratos inteligentes suponen respecto a las limitaciones que los contratos privados convencionales que actualmente operan en derecho presentan:

### **2.5.1 Ejecución rápida y autónoma**

Cada vez que se produce una transacción en el sistema, es agrupada junto a otras transacciones para formar un bloque. De esta manera, la jerarquía de información resulta de la siguiente manera: bloque > transacciones > datos. Todo bloque nuevo permanece siempre unido al

bloque inmediatamente anterior en el tiempo a través de un código alfanumérico generado algorítmica y aleatoriamente que, a su vez, queda registrado también en la cadena<sup>36</sup>.

Para que una transacción sea validada y, por lo tanto, pueda ser ejecutada cuando proceda, es preciso que el bloque sea cerrado<sup>37</sup>. Como se ha expuesto anteriormente, tal cierre depende del algoritmo de consenso que siga la BC.

Aunque la dificultad de este proceso pudiera inducirnos a pensar que la validación de una transacción dura un tiempo excesivo, este proceso anteriormente mencionado tiene un lapso de duración que va desde segundos a unos pocos minutos. Una vez que la transacción es validada, el sistema ya la puede ejecutar. De esta manera evitamos cualquier tiempo de retraso o mora en la ejecución que pudiera darse en los contratos convencionales. A pesar de esta alta velocidad, existen quejas recientes respecto al tiempo de procesamiento en determinadas BCs debido a la reducción del incentivo asociado al minado de transacciones (*caso que tiene lugar con el Bitcoin, por ejemplo*), en un entorno de dificultades para que nodos mineros acepten y asuman el minado de determinadas transacciones. No obstante, se han desarrollado soluciones de muy diversa naturaleza a este problema: *ejemplos de ello son el aumento del tamaño de bloques<sup>38</sup>, uso del Lightning Network<sup>39</sup> o implementación de BC alternativas (i.e. Litecoin para BTC)*.

Esta cualidad de automatización que poseen los SC permite que puedan ser ejecutados sin la necesidad de acudir al auxilio de terceros (jueces o tribunales). Ello suele ser más claro en el caso de que la transacción tenga como objeto activos “alcanzables” dentro de la misma red *Blockchain (i.e. criptoactivos -como las criptomonedas-que hayan quedado depositadas en el propio SC)*, pero no tanto cuando se trata de activos inalcanzables dentro de la propia red (*i.e. fondos en una cuenta bancaria o activos del mundo off-chain -como un inmueble o un paquete de acciones -*).

---

<sup>36</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 40).

<sup>37</sup> ANKALKOTI, P., *A relative Study on Bitcoin Mining*, 2017 (p.2).

<sup>38</sup> *Bitcoin Cash aumenta el tamaño de sus bloques*: <https://criptomonedastop.com/bitcoin-cash-aumenta-tamano-los-bloques/> (párrafo 1º). Consulta válida a 1/4/2019

<sup>39</sup> *What Is Lightning Network And How It Works*: <https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works> (explicada en todo el artículo). Consulta válida a 1/4/2019.

### **2.5.2 Posibilidad de desintermediación en su BC**

La cadena de bloques supone prescindir de cualquier tipo de intermediario en las BC no permitidas (*ver apartado 2.4*); habida cuenta de que puede ser la propia red la que valide de forma descentralizada la existencia y precisión de los propios datos contenidos en ella (operaciones, contratos, transacciones, etc.)<sup>40</sup>.

Como ya se comentó en el apartado 2.1, a través de una serie de procesos matemáticos la cadena prueba la secuencia de eventos y los integrantes del sistema que los llevaron a cabo. Una vez que se ha realizado la comprobación matemática, no es necesaria la intervención de un mediador o intermediario, ya que todo queda registrado tal y como tuvo lugar en el momento de producirse. Esta ventaja derivará, a su vez, en otra de suma importancia: la reducción de costes en las transacciones inherentes al proceso de contratación<sup>41</sup>.

### **2.5.3 Autogobierno sobre identidad y privacidad**

El procesamiento de datos personales se ha convertido, a día de hoy, en un negocio en auge y multimillonario para las empresas tecnológicas, tanto de forma directa<sup>42</sup> (data analytics) como indirecta<sup>43</sup> (principalmente a través de la publicidad). Ello ha derivado en dos tendencias: 1) el enorme interés suscitado por las mayores compañías del mundo en manejar ingentes cantidades de datos de sus clientes y 2) la creciente preocupación, tanto de la sociedad como de sus gobernantes, por proteger la privacidad y confidencialidad de los mismos<sup>44</sup>.

---

<sup>40</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 40).

<sup>41</sup> PANISI, F., *Blockchain and Smart Contracts: Fintech Innovation to Reduce the cost of Trust*, 2017 (p. 8). El autor destaca los principales costes de creación, monitoreo y ejecución de las transacciones.

<sup>42</sup> Se estima que llegue a los 190.000 millones en 2019. OVLAVSRUD, T., *Big data and analytics spending to hit \$187 billion* <https://www.cio.com/article/3074238/big-data-and-analytics-spending-to-hit-187-billion.html> (párrafo 1º). Consulta válida a 23/3/2019

<sup>43</sup> PÉREZ, V., *Cuánto dinero ganan Facebook, Instagram, Twitter y Google con tus datos personales*: <https://www.businessinsider.es/esto-es-dinero-que-ganan-facebook-instagram-twitter-google-tus-datos-personales-198114> (párrafo 7º). Consulta válida a 23/3/2019

<sup>44</sup> Baste con leer la exposición de motivos del 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 (Diario Oficial de la Unión Europea).



Por los motivos anteriormente expuestos será de gran utilidad la implementación de una tecnología que, por un lado, blinde la protección del derecho a la privacidad de datos personales<sup>45</sup> y, por otro, garantice la libre disposición de éstos<sup>46</sup>.

Probar nuestros datos personales en el mundo físico es bastante sencillo y seguro: contamos con carnés de identidad, títulos universitarios de nuestros estudios, licencia de conducir, etc. que el público considera fidedignos porque confía en la institución que los emite. No obstante, no existe una forma rápida y sencilla de enviar digitalmente esta autenticación. Por otro lado, la tarea de verificación y gestión de identidades en internet tiene dos grandes inconvenientes: puede no ser cierta y puede usarse con fines no deseados.

Mediante el uso de la tecnología de la *Blockchain*, los integrantes de la red pueden almacenar sus datos en sus dispositivos (móvil, pc, tablet, etc.) y ponerlos únicamente a disposición de un validador automático. Es este validador (generalmente un wallet de IDs<sup>47</sup>) quien asegura a la institución demandante de información que ésta es cierta. De esta forma se evita el almacenamiento de datos en entidades privadas que puedan conocer (y analizar) la identidad de los sujetos intervinientes<sup>48</sup> al mismo tiempo que se garantiza que la información es válida y correcta.

#### **2.5.4 Transparencia**

La tecnología de la cadena de bloques permite diferentes grados de transparencia dependiendo de los niveles de dominio e injerencia de la aplicación en los contratos<sup>49</sup>. Aunque en función de la programación del sistema, la casuística de la transparencia en juego pueda variar, estos niveles, generalmente, pueden ser agrupados en tres<sup>51</sup> (de mayor a menor, siguen el siguiente

---

<sup>45</sup> *Data protection and online privacy*: [https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index\\_en.htm](https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm) (explicación de la privacidad online en toda la página). Consulta válida a 23/3/2019.

<sup>46</sup> GRECH, A. y CAMILLERI, A., *Blockchain in Education*, 2017 (p.19).

<sup>47</sup> <https://sovrin.org/> *Ejemplo de empresa dedicada a la creación de un ID wallet*. Consulta válida a 2/4/2019.

<sup>48</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 43).

<sup>49</sup> KRITIKOS, M., *What if Blockchain offered a way to reconcile privacy with transparency?*, 2018 (p. 1).

<sup>50</sup> En el caso que nos ocupa vamos a centrarnos en las anteriormente explicadas *permissionless chains*. Para ampliar el conocimiento sobre el concepto ver: <https://coincenter.org/entry/what-does-permissionless-mean> Consulta válida a 23/3/19.

<sup>51</sup> CIAIAN, P., *Blockchain Technology and Market Transparency*, 2018 (p. 11).

orden: pública, híbrida y privada). Al igual que hicimos anteriormente en este trabajo, procederemos a explicar la prelación en la transparencia de los SC a través de un ejemplo ficticio redactado bajo un lenguaje no existente pero próximo al castellano, aunque manteniendo la lógica del lenguaje programático de un *smart contract*. Para ello, acudimos a un contrato inteligente perteneciente a una cadena que opera en una web de subastas<sup>52</sup>:

*Supongamos que una casa de subastas online quiere: que sus usuarios puedan realizar pujas a ciegas (es decir, sin saber lo que otros usuarios están pujando), que cuando termine el proceso de puja los participantes sepan cuáles fueron todas las ofertas de otros usuarios (anónimas) y que, finalmente, se muestre al público en general el ítem subastado y su precio. Como podemos comprobar, en dicho código existen los tres niveles anteriormente mencionados, conteniendo la siguiente información y condiciones:*

- *Nivel privado: cuál es la puja que tú realizas.*
- *Nivel híbrido: todas las pujas (anónimas), y si has conseguido el ítem.*
- *Nivel público: ítem subastado y su precio (quién se lo llevó es anónimo).*

*\* Se computa, pero no se muestra: todas las pujas antes de que llegue el momento de adjudicación. Los participantes pueden conocer cuánta gente va a poder pujar, pero su identidad es anónima.*

*Así pues, el smart contract podría tener una estructura similar a la siguiente:*

---

<sup>52</sup> KOSBA, A., MILLER, A., SHI, E., WEN, Z. y PAPAMANTHOU. C., *Hawk: The Blockchain Model f Cryptography and Privacy-Preserving Smart Contracts*, 2016 (p. 3).

**Términos del contrato:**

1. *Contrato de venta*

# *Nivel público*

2. *Modalidad de venta: subasta de ítem*

3. *Ítem subastado (I): producto ejemplo*

4. *Precio final de subasta: valor puja máxima (PM); moneda €.*

# *Nivel híbrido*

5. *Función subasta:*

6. *Conjunto ordenado (O): ordenar conjunto de  $P_1$  a  $P_n$*

7. *Precio final: valor máximo (PM) del conjunto ordenado (O); moneda: €;*

8. *Adjudicación de subasta: cartera correspondiente a valor máximo (PM)*

9. *Muestra del resultado de subasta:*

10. *Conjunto de pujas: conjunto ordenado (O) de  $P_1$  a  $P_n$*

11. *Resultado (R): adjudicación de ítem (I) a  $C_i$  tal que  $P_i = PM$ .*

# *Nivel privado*

12. *Identidad privada: ID creado por usuario<sub>u</sub>*

13. *Identidad pública: ID asignado a usuario<sub>u</sub>:  $C_u$*

14. *Puja privada: valor introducido en Input ( $P_u$ ) por  $C_u$*

15. *Función cobro:*

16. *Si,  $P_u$  es el valor máximo de (O); entonces, ítem adjudicado a  $C_u$ .*

17. *Si,  $P_u$  no es el valor máximo de (O); entonces, ítem no adjudicado.*

18. *Si ítem adjudicado a  $C_u$ ; entonces, cobro ( $P_u$ ) a  $C_u$*

19. *Si ítem no adjudicado a  $C_u$ ; entonces, no cobro ( $P_u$ ) a  $C_u$*

20. *¿Input ( $P_u$ )?*

Como puede comprobarse en el SC anterior, la conjugación de los conceptos de confidencialidad y transparencia es perfectamente factible en la cadena de bloques. Ello permite mostrar procesos que requieran transparencia en cuanto a resultados pero, al mismo

tiempo, privacidad en cuanto a identidad de usuarios intervinientes y el resultado individualizado de su participación<sup>53</sup>.

### **2.5.5 Confianza**

La confianza es un juicio sobre el riesgo que implica la relación entre varias personas, organizaciones o naciones. En el ciberespacio, ésta se mide según dos parámetros<sup>54</sup>:

- Autenticación: eres capaz de probar que eres quien dices ser.
- Autorización: eres capaz de probar que reúnes los permisos necesarios para hacer aquello que solicitas.

Adicionalmente, la confianza en las transacciones con terceros no confiables en este entorno se basa en la capacidad de generar pruebas suficientes relativas a la “integridad” de las manifestaciones de voluntad formuladas por las partes, a fin de poder generar evidencias no manipulables por cualquiera de las partes o por un tercero.

Si alguna de las partes involucradas no queda satisfecha con la respuesta de la otra, alguna de las dos estará incurriendo en un riesgo<sup>55</sup>. En una economía digital y global, los retos de mantener la confianza se están convirtiendo en cada vez más caros, lentos e ineficientes<sup>56</sup>. No obstante, la tecnología del *Blockchain* puede generar, de forma viable, un cambio de paradigma procedimental y organizacional. Mediante la tecnología de registros distribuidos es posible conseguir la automatización de las funciones de validación de identidades y de sus interacciones y su preservación de forma segura. Tal validación será llevada a cabo de forma más o menos centralizada dependiendo del nivel de permisionado de la red.

---

<sup>53</sup> Un ejemplo paradigmático relativo al uso de estos niveles en la cadena de bloques es su aplicación a un proceso electoral, pues este proceso garantizaría la transparencia (evitaría el trapeo) y al mismo tiempo la privacidad de cada voto correspondiente a cada ciudadano. DESOUZA, K., *How blockchain could improve election transparency* <https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/> (párrafo 1º). Consulta válida a 24/3/2019.

<sup>54</sup> Government Office for Science, UK. *Distributed Ledger technology: beyond blockchain*, 2016 (p. 13). [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gs-16-1-distributed-ledger-technology.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf) Consulta válida a 23/3/2019.

<sup>55</sup> GRECH, A., y CAMILLERI, A., *Blockchain in Education*, 2017 (p.20).

<sup>56</sup> MARSHALL, S., SHELKOV, A., WELMANS, T., y WALSH, K., *Blockchain, democratised trust: Distributed Ledgers and the Future of Value*, 2016 (p. 86).

### **2.5.6 Desarrollo en software**

Como ya se ha reiterado anteriormente, en los contratos inteligentes los términos y condiciones se encuentran establecidos en líneas de código<sup>57</sup>. Ello permite atribuirles las siguientes características:

1. Los SC, por su propia naturaleza, quedan protegidos bajo por las leyes de propiedad intelectual<sup>58</sup>, al ser considerado como un programa informático<sup>5960</sup>.
2. Pese a que su base se desarrolla en lenguaje de programación, su elaboración puede ser muy sencilla gracias a dos factores:
  - a. Traducciones del código a lenguaje humano.
  - b. Uso de los denominados *templates* de SC (modelos disponibles para para la implementación de *smart contracts* específicos).
3. Al estar escrito en una lógica proposicional universal (if/then/else<sup>61</sup>), los SC operan sin la necesidad de interpretación humana: no es necesario interpretar el sentido de las palabras. No obstante, como se pondrá de manifiesto en el siguiente apartado (3. *Limitaciones en la aplicación de los SC*), esta característica puede suponer un arma de doble filo: las partes pueden desear emplear la ambigüedad del lenguaje natural para expresar y formalizar acuerdos que quieran dejar abiertos a posterior interpretación. Por lo tanto, la naturaleza programática es al mismo tiempo una ventaja en cuanto a su precisión y determinación, pero una desventaja en cuanto a su cualidad para expresar conceptos abstractos del lenguaje

---

<sup>57</sup> Lo cual, como también se ha mencionado *supra*, queda permitido por la libertad de forma expuesta en los arts. 1279 y 1280 CC.

<sup>58</sup> Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia (Boletín Oficial del Estado). Ver Título VII: Programas de ordenador.

<sup>59</sup> SAVELYEV, A., *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of the Classical Law*, 2016 (p.12).

<sup>60</sup> La protección no se da únicamente en el Estado Español. Analizando el Derecho comparado, podemos ver que aquélla se otorga en la inmensa mayoría de jurisdicciones. *Un ejemplo de ello es la legislación estadounidense con la Copyright Act, la cual brinda protección a los programas informáticos, definiéndolos de la siguiente manera: "A computer program" is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result*".

<sup>61</sup> LEGERÉN-MOLINA, A., *Los contratos Inteligentes en España: la disciplina de los smart contracts* publicado en la Revista de Derecho Civil (vol. V, núm. 2) en abril-junio de 2018 (p. 198). En este apartado el autor muestra las consecuencias de la lógica *booleana*.

humano. En caso de que las partes requieran ambas cualidades podrán recurrir a los denominados contratos híbridos anteriormente mencionados en este trabajo.

### **2.5.7 Seguridad e inmutabilidad**

Una vez que las transacciones o interacciones tienen lugar entre los nodos del sistema, éste genera un nuevo hash enviado a la cadena de bloques para que genere un *timestamp* (sello temporal) en el que se establece la fecha y hora la que se ha obtenido<sup>62</sup>. Este sello, junto con la firma electrónica generada automáticamente por la BC, se envían de vuelta para que pueda ser introducido en la cadena<sup>63</sup>. Gracias a este proceso, la BC adquiere características de seguridad e irreversibilidad debido a tres factores<sup>64</sup>:

- En primer lugar, habida cuenta que los datos originales no pueden ser calculados a partir del hash, (dado que la función del hash es unidireccional), los validadores de la BC sólo podrán verificar que tal interacción ha tenido lugar en ese momento (pero no se les mostrará la interacción en sí), lo que hace de este método un modelo seguro y confidencial.
- En segundo lugar, según se produce la validación o confirmación de la última versión de la cadena, cada bloque -y sus correspondientes conexiones entre los mismos- tendrán carácter irreversible, reduciendo a la mínima expresión la probabilidad de ataques individuales o consensuados en contra del registro distribuido y compartido.
- En tercer lugar, los datos incorporados al registro se encuentran íntegramente reproducidos en los ordenadores que operan en la red y validan la cadena siguiendo el consenso, garantizando así que si se produce una modificación de los registros de la base de datos que reside en uno o varios nodos, se detecte la inconsistencia y se rechace el registro de la transacción.

---

<sup>62</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 40).

<sup>63</sup> *What is a Timestamp?*: <https://www.globalsign.com/en/blog/what-is-timestamping-how-does-it-work/> (párrafo 7º). Consulta válida a 3/4/2019.

<sup>64</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 41).

### **2.5.8 Posible coordinación con Internet de las Cosas**

El denominado como Internet de las Cosas (IoT) supone la interconexión a través de Internet de todo tipo de objetos al que se les haya conectado un dispositivo emisor y/o receptor de información por radiofrecuencia.

Los SC, gracias a su base -lenguaje de programación- tienen la cualidad de la posible coordinación con estructuras de Internet de las Cosas mediante los siguientes elementos<sup>65</sup>:

- a) Dispositivo externo: con una capacidad tecnológica suficiente para permitir la comunicación bidireccional. Éste llevará a cabo el envío de información capaz de ser programada por el SC, pudiendo detectar eventos que supongan consecuencias desencadenantes de condiciones de autoejecución dispuestas en el contrato.
- b) Red de comunicaciones mediante la que se comuniquen los dispositivos y la BC (internet).
- c) SC conectado a la BC. Ésta, al verificar la concurrencia de un determinado evento que cumpla con condiciones de ejecución automática enviará de vuelta la llamada a los dispositivos IoT para llevar a cabo la ejecución.

Esta estructura aumenta de forma destacable la operatividad de los contratos inteligentes mediante dos vías:

- A través del input: podrá recibir una cantidad inmensa de información, por lo que los datos que manejará serán mucho más detallados y precisos. *Por ejemplo, supongamos un dispositivo IoT conectado a la red de suministro de una casa que transmite directamente los datos al SC contratado entre la compañía de gas y la familia de ese hogar. Otro ejemplo podría ser una empresa de envío de paquetes que introduce un dispositivo que lleva el tracking de los envíos, confirmando el tiempo, el lugar y si son correctamente entregadas al destinatario.*
- A través del output: podrá ejecutar materialmente el contrato de forma directa sin necesidad de acudir a una autoridad judicial. *Por ejemplo, supongamos un contrato de arrendamiento de un piso reflejado en un SC entre un casero y un inquilino. En caso*

---

<sup>65</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 117).

*de impago, el casero podría bloquear el bombín de la puerta (suponiendo que éste sea digital y IoT) en cualquier momento, impidiendo problemas como la ocupación (sin perjuicio de la posible calificación del ilícito que pudiera comportar esta última conducta del arrendatario).*



### **3. LIMITACIONES EN LA APLICACIÓN DE LOS SC: ANÁLISIS JURÍDICO**

A pesar de las numerosas ventajas antes mencionadas, la solución de los SC no es perfecta, pues existe un conjunto de inconvenientes que dificultan, y en muchas ocasiones directamente impiden, la aplicación de los SC a la contratación privada. Antes de comenzar a analizarlos, cabe mencionar que, en lo que a España se refiere, no existe una legislación específica relativa a los SC. Esto hace necesario acudir a la normativa general de los negocios jurídicos, así como a otras normas que la desarrollan, como la de contratación electrónica -que en parte se recoge en la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico<sup>66</sup>- y a la Ley General para la Defensa de los consumidores y Usuarios<sup>67</sup> (reformada en 2014 para incorporar modificaciones dispuestas en la Directiva 2011/83 sobre los derechos de los consumidores<sup>68</sup>) para estudiar la adaptación de los contratos inteligentes al derecho privado.

#### **3.1 Sobre los elementos esenciales para la validez del contrato**

Según reza el art. 1261 CC, *no hay contrato sino cuando concurren los requisitos siguientes: 1) consentimiento de los contratantes, 2) objeto cierto que sea materia del contrato y 3) causa de la obligación que se establezca*. Estos tres son los requisitos esenciales del contrato (su concurrencia es precisa para que el contrato exista<sup>69</sup>), los cuales se analizan a continuación:

##### **3.1.1 Consentimiento de los contratantes**

El contrato es un negocio jurídico y, como tal, está compuesto por declaraciones de voluntad procedentes de cada una de las partes contractuales. La concurrencia de aquéllas para la formación del contrato tiene lugar en el momento de su perfeccionamiento, y a partir del mismo las partes quedan obligadas al cumplimiento de las prestaciones. Como se ha reiterado en múltiples ocasiones en este trabajo, en los SC, la realización de las prestaciones -y, como consecuencia, la consumación del contrato mismo- es llevada a cabo por aquéllos de forma

---

<sup>66</sup> Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (Boletín Oficial del Estado).

<sup>67</sup> Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (Boletín Oficial del Estado).

<sup>68</sup> Directiva 2011/83/UE del Parlamento Europeo y del Consejo de 25 de octubre de 2011 sobre los derechos de los consumidores (Boletín Oficial de la Unión Europea).

<sup>69</sup> PUIG BRUTAU, J., *Fundamentos de Derecho Civil II*, vol. II, Boch, Barcelona, 1986 (p.141).

automática sin requerir el consentimiento de las partes en la fase de ejecución. Es por este motivo que, en el perfeccionamiento de los SC se requiere la concurrencia de un doble consentimiento simultáneo<sup>70</sup>:

- Por un lado, el consentimiento que determina que las partes se *obligan a obligarse*.
- Por otro, el consentimiento preconstituido sobre que la consumación del contrato se llevará a cabo de forma automática (en las condiciones pactadas y sin recabar para ello su autorización cuando fuera a tener lugar).

La disposición general que regula el consentimiento es el art. 1262 CC, el cual estipula que en los contratos celebrados mediante dispositivos automáticos el consentimiento existe desde que se manifiesta la aceptación. Para que tal consentimiento sea invalidado por error, éste deberá *recaer sobre la sustancia de la cosa que fuere objeto del contrato, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo* (art. 1266 CC). Matizando lo anterior, el TS se manifiesta afirmando que tal error surge cuando la voluntad del contratante se forma a partir de una creencia inexacta. *Es decir, cuando la representación mental que sirve de presupuesto para la realización del contrato es equivocada o errónea*<sup>71</sup>. De lo anterior podemos concluir que el consentimiento de las partes debe recaer sobre tres elementos del SC:

1. Las prestaciones concretas que van a llevarse a cabo.
2. La forma, el momento y la razón en y por las que se van a realizar.
3. Las consecuencias que derivan de no realizar tales prestaciones (aunque anteriormente se ha afirmado que la ejecución es automática, existe la posibilidad de que el deudor provoque el incumplimiento de ella *-i.e. dejando la cuenta acreedora con un valor nulo en el saldo-*. *Se realizará un estudio más detallado de este aspecto en el apartado 3.5.2 siguiente*).

Podemos incluir de lo hasta ahora expuesto la necesidad de recepción, previa al perfeccionamiento de los SC, de información clara, precisa, exhaustiva y comprensible sobre dos aspectos: 1) prestaciones del contrato y 2) procedimiento automático mediante el que se llevarán a cabo. Es por ello que debemos plantearnos cómo asegurar la comprensión del conjunto de cláusulas dispuestas, así como la emisión consciente del consentimiento respecto

---

<sup>70</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 81).

<sup>71</sup> Sentencia del Tribunal Supremo de 20 de enero 354/2014, fundamento jurídico decimoprimero (CENDOJ).

a las prestaciones que deban llevarse a cabo<sup>72</sup>. Para tal cometido en ocasiones será necesaria la transcripción a lenguaje humano (como se explicó anteriormente, esto no siempre deberá ser así *-i.e. entornos expertos o automatizados-*).

El error<sup>73</sup>, como vicio del consentimiento, permite a la parte que lo sufre anular el contrato bajo varios presupuestos establecidos en la ley. La anulación de dicho contrato puede ser difícil, debido a las características de automatismo e irreversibilidad del SC. Por este motivo, deberán establecerse en el contrato cláusulas que permitan detener y revertir los efectos de la ejecución si un juez o tribunal (o institución arbitral si así se ha pactado en el marco de la relación jurídica) adopta medidas cautelares o definitivas que impidan o retrocedan los efectos, ya sea en el entorno on-chain (sobre activos virtuales) como off-chain (sobre activos físicos.)<sup>74</sup>.

### **3.1.1.1 Sobre la redacción de los SC**

En la “redacción” de los SC, al contrario que en los contratos privados convencionales, intervienen tanto juristas como programadores. Por ello, las dificultades en el análisis del error aumentan: conocimiento inadecuado de la realidad jurídica por parte de los programadores, instrucciones mal trasladadas por los juristas, cláusulas no expresadas correctamente en el código, etc. Ante estas divergencias entre lo acordado y el código pueden darse tres posibles escenarios<sup>75</sup>:

- a) Que la diferencia entre la prestación querida y la realmente obtenida sea poco significativa: en este supuesto, en atención a las expectativas de las partes podemos concluir que el contrato sí se habría cumplido.
- b) La diferencia es apreciable: nos encontramos ante una situación de posible cumplimiento parcial de la prestación.
- c) La diferencia es total: el contrato se entendería incumplido.

---

<sup>72</sup> FELIU REY, J., *Autonomía privada y autotutela: oportunidades y riesgos de los Smart Contracts*. Publicado en *Sociedad Digital y Derecho*, 2018 (p. 811).

<sup>73</sup> Según dispone el art. 1265 CC, *será nulo el consentimiento prestado por error, violencia, intimidación o dolo*.

<sup>74</sup> *Ver medidas comentadas en el apartado 3.6.1: Sobre la ejecución de los SC*.

<sup>75</sup> FELIU REY, J., *Autonomía privada y autotutela: oportunidades y riesgos de los Smart Contracts*. Publicado en *Sociedad Digital y Derecho*, 2018 (p. 823).

### **3.1.1.2 Sobre los contratos estandarizados y contratos de consumo**

Además de lo anteriormente mencionado sobre la prestación del consentimiento en los SC, cabe realizar un especial estudio sobre tres tipos de contrato en los que el error de consentimiento posee características singulares adicionales:

1) Contratos en masa o estandarizados, respecto a sus condiciones generales de contratación, activando los controles de *incorporación, interpretación y contenido*<sup>76</sup> (conjugación de los arts. 5, 6 y 7 de la Ley sobre condiciones generales de contratación). Para que los SC que contengan aquel tipo de cláusulas puedan cumplir con estos requisitos puede ser necesario que se transforme su contenido en un formato legible para el usuario de tal forma que pueda adherirse a ellos con plenitud de conocimiento sobre su contenido y voluntad de su cumplimiento (ver *supra*).

2) Cuando sean contratos de consumo. En caso de que una de las partes tenga la condición de consumidor, y la otra de comerciante (según la definición dispuesta en la Directiva 2011/83 sobre los Derechos de los consumidores<sup>77</sup>), le serán aplicables los preceptos expuestos en tal normativa europea, especialmente los relativos a la tutela respecto a la abusividad de cláusulas y las reglas de *inclusión, incorporación y transparencia* (arts. 5 a 10 LCGC<sup>78</sup>). Además de ello, al tratarse de cláusulas no negociadas individualmente, se verán afectados por la TRLGDCU<sup>79</sup>, en especial, en lo relativo a la obligatoriedad de la entrega del contrato celebrado en formato escrito, ante la eventualidad de divergencia entre el código del SC y lo presentado al usuario (ex. arts. 61, 63, 65, 80, 98, y 99 de la mencionada Ley). Los problemas que puede conllevar un SC en contratación de consumidores pueden referirse a dos aspectos:

1. Falta de comprensión de las condiciones contractuales que suscribe el consumidor.
2. Operativa automatizada del SC, la cual se manifiesta en dos vertientes:

---

<sup>76</sup> FELIU REY, J., *Autonomía privada y autotutela: oportunidades y riesgos de los Smart Contracts*. Publicado en *Sociedad Digital y Derecho*, 2018 (p. 823).

<sup>77</sup> Directiva 2011/83/UE del Parlamento Europeo y del Consejo de 25 de octubre de 2011 sobre los derechos de los consumidores.

<sup>78</sup> Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación.

<sup>79</sup> Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (Boletín Oficial del Estado).

- a. Su integración: verificación del cumplimiento de condiciones con recurso a oráculos que pueden estar “sesgados” en favor del predisponente empresario o por la dependencia de condiciones puramente potestativas o consideradas abusivas.
- b. Su ejecución, que puede impedir que el consumidor sea protegido por los derechos que le atribuye la normativa imperativa de defensa de consumidores: *i.e. derecho de desistimiento sin causa en ventas a distancia*<sup>80</sup> (art. 72 TRLDCU) o el cargo automático de importes que conforme a la ley no se pueden imponer al consumidor.

3) Los SC que corresponden enteramente a acuerdos suscritos por máquinas: el consentimiento, al ser una exteriorización de voluntad interna del sujeto, únicamente puede ser formulado por personas. Las posibles formas de dar tratamiento legal a este fenómeno son mediante el uso de dos figuras:

- c. El precontrato<sup>81</sup>: emisión del consentimiento de manera anticipada, subordinando el contenido del contrato definitivo al cumplimiento de determinadas condiciones preestablecidas.
- d. Contrato marco<sup>82</sup>: en el que las partes humanas establecen una serie de condiciones o términos que serán la base a partir de la cual se formen todos los contratos por los agentes de software.

*A pesar de lo futurista que nos pudiera parecer esta modalidad de contratación, en mayo de 2018 Google ya presentó su nuevo asistente virtual capaz de llamar automáticamente a negocios, interactuar con ellos de forma idéntica a la humana (en cuanto a voz y contenido) y suscribir contratos según condiciones previamente configuradas por el usuario*<sup>83</sup>.

---

<sup>80</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 77). El autor afirma que “en contratos legales inteligentes, el derecho de desistimiento debe ser tomado en consideración por el desarrollador del programa (“contract”) que se integra en la cadena de bloques e incluir en el mismo las instrucciones necesarias para que se haga efectivo”.

<sup>81</sup> LEGEREN-MOLINA, A., *Los contratos Inteligentes en España: la disciplina de los smart contracts* publicado en la Revista de Derecho Civil, vol. V, núm. 2, en abril-junio de 2018 (p. 216).

<sup>82</sup> LÓPEZ CABIA, D., *Acuerdo marco*: <https://economipedia.com/definiciones/acuerdo-marco.html> (párrafo 1º). Consulta válida a 2/4/2019.

<sup>83</sup> <https://www.youtube.com/watch?v=D5VN56jQMWM> Consulta válida a 28/3/2019.

### **3.1.2 El objeto cierto que sea materia del contrato**

El concepto de objeto responde a la propia obligación que se constituye entre las partes, debiendo ser lícito, posible y determinado. Cabe mencionar al respecto del mismo: 1) que no es necesario que exista en el momento de perfeccionarse el contrato (art. 1271 CC) y 2) que, independientemente de cuál fuera, debe quedar perfectamente determinado en el propio cuerpo del mismo o ser fácilmente determinable a través de criterios establecidos (arts. 1273, 1447 y 1448 CC). El SC puede cumplir este elemento a la perfección, siendo incluso más preciso que un contrato convencional en lo referente a condicionantes que dependan de circunstancias futuras.

#### **3.1.2.1 Imposibilidad de incumplimiento**

El Derecho continental ha adoptado el concepto de obligación que ya existía en el Derecho Romano. Por aquel entonces, el elemento “obligatio” respondía a un vínculo con base legal que permitía a una persona compeler a la obligada a la realización de una determinada conducta, generalmente la entrega de una cosa<sup>84</sup>. Podemos deducir en una primera instancia que las obligaciones contenidas en contratos son dos caras de una misma moneda<sup>85</sup>: por una, la conducta que una parte debe llevar a cabo, y, por otra, el derecho a exigir aquella conducta que le corresponde a la otra parte. De este modo, podemos concluir dos características propias de ambas magnitudes: 1) orientación a un escenario futuro y 2) el componente de la “voluntad”. Habida cuenta lo anterior, es posible concluir que tal vínculo existe hasta el momento en el que tal acción o inacción deba ser llevada a cabo y el deudor decida realizarla<sup>86</sup>.

Con todo, si en los SC el resultado realmente no depende de la voluntad del deudor, sino de su propia configuración misma, entonces no existe una obligación real que pueda ser incumplida (aunque una parte decidiera apagar su ordenador a mitad del proceso de cumplimiento, el SC seguiría su curso normal).

---

<sup>84</sup> LONDON. N., *An Introduction to Roman Law*, Oxford, Glasgow, 1963 (p. 158).

<sup>85</sup> SAVELYEV, A., *Contract Law 2.0: “Smart” Contracts as the Beginning of the End of the Classical Law*, 2016 (p.17).

<sup>86</sup> Es posible afirmar que el espíritu del concepto de obligación del Derecho Continental al que se está haciendo alusión tendría su equivalente en el Common Law en los contratos ejecutorios.

A pesar de lo anteriormente expuesto, el SC puede ser considerado un contrato por dos motivos: 1) las partes expresan su voluntad de vincularse al resultado de la ejecución del contrato cuando firman (virtualmente) ser partes del mismo y 2) porque la ley contempla la vinculación a contratos de ejecución inmediata<sup>87</sup>.

### ***3.1.2.2 Análisis jurídico de las condiciones de ejecución de un SC***

Como se mostró en el apartado 2.3.1 (*Naturaleza Condicional del SC*), los contratos inteligentes se presentan como un agregado de condiciones que, dependiendo del modo en el que sean satisfechas, suponen la ejecución automática de un resultado, o no. Esto hace que, como se ha señalado, debamos encajar jurídicamente los SC dentro de los contratos con obligaciones sujetas a condición (entendida como el sometimiento a la contingencia de un hecho de la existencia o desaparición de los efectos de un negocio) expresadas en los arts. 1113 a 1124 CC. La relación jurídica condicional es una relación de eficacia incierta<sup>88</sup>, dado que sus efectos pueden no llegar a cumplirse nunca si las condiciones requeridas para ello nunca se llegan a dar. La clasificación jurídica de las condiciones que puede reunir un SC es la siguiente:

1. Suspensivas o resolutorias: si de ellas depende el nacimiento o cese de las obligaciones del contrato.
2. Potestativas, causales o mixtas: si la contingencia depende de la voluntad de las partes o de un suceso ajeno.
3. Positivas o negativas: dependiendo se si la incertidumbre depende de que un hecho tenga o no lugar.

---

<sup>87</sup> Ejemplos de ello pueden ser los actos jurídicos recogidos en los arts. 1529 CC (compraventa), 1621 CC (donación), 1602 CC (permuta) o 1604 CC (contrato de suministro).

<sup>88</sup> *Obligaciones condicionales*:

[http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUjYwtztlUouLM\\_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAxx3YxjUAAAA=WKE](http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUjYwtztlUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAxx3YxjUAAAA=WKE) (párrafo 3º). Consulta válida a 2/4/2019.

### **3.1.3 Causa válida que se establezca**

Sin entrar en el análisis de las diferentes posiciones doctrinales en relación a la causa del contrato (objetiva, subjetiva y unitaria<sup>89</sup>), el Tribunal Supremo ha señalado<sup>90</sup> que es la función económico-social del contrato como resultado práctico que las partes del mismo quieren conseguir o alcanzar, coincidiendo con el fin último perseguido y protegido por el ordenamiento jurídico<sup>91</sup>. Sobre la causa del SC cabe realizar dos apreciaciones:

- 1) La causa del contrato formulado dentro SC varía en función del negocio jurídico que se trate, como en cualquier otro contrato (este apartado no genera mayor problemática o análisis).
- 2) La causa específica del SC podría complementarse como la consecución de todas las ventajas expuestas en este trabajo: seguridad, eficiencia, rapidez, etc.

### **3.2 Sobre la forma de los contratos**

La forma de los contratos hace referencia al modo en el que se manifiesta o declara la voluntad de las partes<sup>92</sup> y, por lo tanto, cómo se perfecciona. Para analizar la forma de los contratos inteligentes cabe reconocer, en un primer lugar, la condicionalidad su lenguaje. Ello quiere decir que, dada la naturaleza de los SC (están programados en código informático) su forma debe seguir una lógica proposicional determinada (la anteriormente mencionada *if/then/else*) así como estar redactado en el lenguaje de programación que corresponda. Ello nos lleva a realizar dos apreciaciones:

---

<sup>89</sup> ARNAU MOYA, F., *Lecciones de Derecho Civil II: obligaciones y contratos*, Universitat Jaume I, Castellón de la Plana, 2009 (p. 147).

<sup>90</sup> Sentencia del Tribunal Supremo de 30 del junio 2823/2014, fundamento jurídico segundo, apartado sexto (CENDOJ).

<sup>91</sup> Sentencia del Tribunal Supremo de 24 de noviembre 5235/2016, fundamento jurídico quinto, apartado tercero (CENDOJ). En dicha sentencia el propio Tribunal afirmó que *el propósito perseguido por las partes del contrato ha de ser confrontado con la función económica y social en que consiste la causa de cada negocio, de modo que, si hay coincidencia, el negocio es protegido y reconocido por el ordenamiento jurídico, pero si no la hay [...] tal protección no se otorgará.*

<sup>92</sup> *Forma de los contratos*: <http://www.encyclopedia-juridica.biz14.com/d/forma-de-los-contratos/forma-de-los-contratos.htm> (párrafo 1<sup>a</sup>). Consulta válida a 17/03/19.



### **3.3.1 La forma y el lenguaje de los SC**

Frente al lenguaje humano, que es indeterminado y contiene ambigüedades, el lenguaje de programación debe ser determinado, objetivo y correctamente estructurado. Ello tendrá tres implicaciones fundamentales:

- En primer lugar, toda la información que manejen deberá ser objetivable y definible mediante 1s y 0s. (Este punto será tratado en el apartado siguiente: 3.3 *Necesidad de objetivación de la realidad*).
- En segundo lugar, la forma en los SC no tiene una mera función de soporte o documentación, sino que son las líneas de código el propio mecanismo que hace que funcionen<sup>93</sup>.
- Aunque la concurrencia del soporte digital podría facilitarnos determinar los SC como *contratos electrónicos*, su significado no sería suficiente para definir las cualidades de automatismo ni autoejecución: por lo que los SC tienen, en este sentido, una naturaleza distinta.

### **3.3.2 Requisitos de forma del contrato**

Según afirma el art. 1278 CC: *los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez*. Este precepto estipula la libertad de forma de las partes del contrato como norma general en su formalización: un contrato podrá ser materializado en cualquier forma que acuerden sus partes. Por ello podemos afirmar que los SC, como norma general, no tienen por qué no ser válidos por razón de forma.

Lo anterior queda matizado por los dos arts. siguientes:

- a) art. 1279 CC: *Si la ley exigiere el otorgamiento de escritura u otra forma especial para hacer efectivas las obligaciones propias de un contrato, los contratantes podrán compelerse recíprocamente a llenar aquella forma desde que hubiese intervenido el consentimiento y demás requisitos necesarios para su validez*. Aquí ya encontramos una primera laguna: al no establecer si el legislador acepta como válido la escritura en lenguaje

---

<sup>93</sup> FELIU REY. J., *Autonomía privada y autotutela: oportunidades y riesgos de los Smart Contracts*. Publicado en *Sociedad Digital y Derecho*, 2018 (p. 818).

de programación que utilizan los SC. Para matizar este punto recurrimos al régimen de reconocimiento de la validez y prueba de los contratos celebrados en soporte electrónico; más concretamente en los siguientes preceptos:

- a. art. 23.3 LSSI<sup>94</sup>: *siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.*
- b. art. 24.2 LSSI: *en todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.*

Como conclusión de lo anterior extraemos que, en tanto en cuanto el lenguaje de programación fuera aceptado como medio válido equiparable al soporte electrónico, podemos afirmar que la forma de los SC es válida para la celebración de un contrato.

- b) art. 1280 CC: establece la lista de actos jurídicos que deben constar en documento público (*i.e. cesión de derechos hereditarios o capitulaciones matrimoniales*). En tales casos sería imposible, en estos momentos y dada la ley vigente, la introducción de los SC.

### **3.3 Necesidad de objetivación de la realidad**

Los SC necesitan dos elementos clave para que su funcionamiento sea posible: un input (acción de entrada: datos de la realidad), y un output (acción de salida: ejecución de resultado).

Sobre el output, nada reseñable cabe decir más que para que los contratos inteligentes sean ejecutables, necesitan dispositivos u otros programas conectados a ellos que lleven a cabo las operaciones reflejadas en el código del contrato. *Un ejemplo de ellos sería, en un SC de compraventa, el envío de un determinado bien una vez que se ha recibido el pago.*

El input, por el contrario, genera una problemática mayor, pues su característica básica es la necesidad de ser objetivo. Este elemento es determinante en cuanto a sus diferencias con los contratos convencionales ya que impide que su ejecución pueda depender de un ente externo que valore el resultado y determine cómo debe llevarse a cabo la ejecución (juez o tribunal).

---

<sup>94</sup> Ley 34/2002 de 11 de julio se Servicios de la Sociedad de la Información y de Comercio Electrónico (Boletín Oficial del Estado).

La tarea de la objetivación resulta sencilla en aquellas condiciones del contrato que sean perfectamente determinables: *i.e. si (A) entrega X€ a (B), entonces (B) entrega el ítem de la compraventa*. No obstante, la tarea se complica en aquellos casos que requieran algún tipo de apreciación valoración de la realidad: *i.e. (A) realiza una contratación de un trabajo de limpieza a (B) y sólo pagará cuando se haya realizado satisfactoriamente el servicio*. En estos casos, ¿cuándo se ejecuta el contrato? (*i.e. ¿Quién introduce el input de realización de servicio para ejecutar el pago?*) y, ¿cómo se sabe que es el momento de ejecutar? (*i.e. ¿Cómo se puede llegar a tener certeza de que el servicio se ha realizado satisfactoriamente?*).

Sobre la naturaleza de input en un SC caben 2 posibles opciones:

***a) Los datos requieren de una valoración subjetiva***

Siempre que se dependa el resultado de una valoración humana (juez o tribunal) la introducción va a ser, en la práctica, imposible<sup>95</sup>. Diferente es el caso en el que tal valoración pueda realizarse en un futuro por inteligencia artificial: *i.e. en el ejemplo de la limpieza, pueda determinarse por un sofisticado software de análisis de fotos si el lugar ha quedado limpio o no*. De todas formas, este escenario dista aún de la realidad existente.

***b) Los datos pueden ser fácilmente objetivables por dispositivos: oráculos***

La capacidad de los contratos inteligentes es limitada<sup>96</sup>: solamente están diseñados para validar información procedente del interior de la propia cadena (no disponen de recursos suficientes para determinar qué información del mundo exterior real es necesaria y cuál cierta y cuál no). Por lo tanto, en infinidad de ocasiones tampoco serán capaces de discernir por sí mismos si las condiciones resolutorias y suspensivas (expuestas en el apartado 2.3.1) dependientes de eventos ajenos a la cadena han sido cumplidas o no.

---

<sup>95</sup> WERBACH, K., *Contracts ex machina*. Revista *Duke Law Journal*, vol 67, 2017 (p. 43). Se afirma: “*some contractual terms simply cannot be expressed through formal logic, because they imply human judgement*”.

<sup>96</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018. (p. 111).

En efecto, existen SC en los que se necesita trasladar información del mundo exterior al sistema, para saber si las prestaciones han sido ejecutadas. *Por ejemplo, un SC de compraventa en el que el precio final varía en función de la cotización de un determinado índice u otro SC en el que se compra un billete de avión que contiene indemnizaciones en caso de retrasos.* En ambos casos la realidad es fácilmente objetivable: puntos de cotización del índice o tiempo de retraso respecto a la hora esperada. Para tales condiciones de SC debe recurrirse a la colaboración de un ente ajeno y confiable que proporcione información no propia de la BC: los oráculos<sup>97</sup>. Éstos pueden ser definidos como instrumentos cuya cualidad es actualizar estados de condiciones de un SC a través de información del exterior<sup>98</sup> (en la mayoría de los casos obtenida a través de APIs). El desarrollador del SC deberá integrar en éste el código mediante el que pueda coordinarse con el oráculo a fin de que puedan implementarse las consultas de datos al mismo (denominadas *queries*).

La facilidad de conectar el SC con oráculos externos e integrar en su operativa la información de muy diversas fuentes (on-chain/off-chain, incluso del mundo físico) para que tenga consecuencias sobre la ejecución o inejecución de las prestaciones, puede ser de gran valor para cubrir las deficiencias que tradicionalmente presentan los contratos convencionales.

A pesar de su gran utilidad respecto de los SC, los oráculos presentan una gran limitación: pueden ser manipulados. Es por este motivo que resulta preciso que solamente sean integrados aquéllos que nos aporten garantías de ser entes imparciales y de reconocido prestigio<sup>99</sup>. No obstante, ante la posible eventualidad de que el oráculo transmita información falsa y que ésta desencadene una ejecución automática improcedente, nada impide que el perjudicado pueda llegar a ejercer acciones (ante el juez o tribunal) exigiendo el cumplimiento adecuado del contrato. Como es lógico, esta posibilidad sólo tendría cabida de encontrarnos ante un SC híbrido y no un SC puro; ya que, además del código ejecutable, sería preciso un contrato convencional privado adjunto al código (*ver apartado 3.5.2, en lo referente a las soluciones a los problemas en cuanto al automatismo y la irreversibilidad de los SC*), así como una acreditación fehaciente sobre la información verdadera correspondiente al evento que

---

<sup>97</sup> Actualmente sólo consta la existencia de dos plataformas que lleven a cabo tal funcionalidad de forma completa: SmartContract.com y ORACLIZE.

<sup>98</sup> Ésta puede ser de muy diversa índole: como se ha comentado, desde condiciones atmosféricas a la cotización bursátil de un índice.

<sup>99</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 113).

constituyese la condición. Por otro lado, la parte perjudicada por el faso cumplimiento de la condición podrá ejercer acciones resarcitorias frente al oráculo reclamando daños y perjuicios que le hubieran sido causados.

### **3.4 Sobre la legalidad del contenido de los SC**

Aunque sean numerosos los desarrolladores de la tecnología BC que proponen la creación de un sistema económico y legal al margen del regulado por los estados<sup>100</sup>, este escenario, además de ser difícilmente practicable, no gozaría en ningún momento de las garantías que ofrece la ley en un Estado de Derecho. Es por este motivo que los SC, al igual que así lo hacen los contratos convencionales, deberán pasar igualmente un filtro de legalidad sustantiva. Sobre ella cabe hacer dos menciones:

- a) La automatización de este juicio de legalidad será extremadamente difícil dada la necesidad de la intervención humana. Por lo tanto, será necesaria la transformación del SC a lenguaje comprensible por un juez y, una vez se haya confirmado la legalidad de sus elementos, automatizarlo.
- b) Podemos encontrar SC en los que su contenido es válido, pero es la legalidad de su ejecución la que se pone en duda<sup>101</sup> (*i.e. ejercicio de voto con abuso de minoría en un pacto parasocial con contenido lícito.*) Al igual que en el anterior caso, la automatización de la detección de ilegalidad es extremadamente compleja. Como máximo podría introducirse en la BC la traducción al código de todas aquellas normas legales que puedan objetivarse, de tal forma que sea el propio sistema quien detecte la ejecución ilegal.

---

<sup>100</sup> FELIU REY. J., *Autonomía privada y autotutela: oportunidades y riesgos de los Smart Contracts*. Publicado en *Sociedad Digital y Derecho*, 2018 (p. 826).

<sup>101</sup> FELIU REY. J., *Autonomía privada y autotutela: oportunidades y riesgos de los Smart Contracts*. Publicado en *Sociedad Digital y Derecho*, 2018 (p. 826).

### **3. 5 Sobre la ejecución de los SC**

#### ***3.5.1 Análisis de la ejecución de los SC***

Como hasta ahora hemos comentado, una de las principales ventajas de la *Blockchain* es el automatismo en la ejecución de las contraprestaciones programadas: la consumación del contrato no depende de la voluntad de las partes, sino que es la propia programación del SC la que, en función de si se dan determinadas circunstancias, la lleva a cabo de forma automática<sup>102</sup>. Esta autoejecución impide que podamos hablar de cumplimiento obligacional en cuanto a los SC, ya que -como vimos en el apartado 3.1.1- cuando las partes prestan consentimiento, lo hacen *ab initio* sobre todas las incidencias de la vida del contrato: función programada y autoejecutada futura.

No obstante la regla general anterior, cabe puntualizar la existencia de un reducido grupo de situaciones en las que el incumplimiento del deudor es posible. Se trata de aquellos casos en los que la ejecución automática depende de que el deudor haga que se mantengan las condiciones propicias para ello (*i.e. mantener el dinero necesario en la cuenta deudora para que el programa realice el cargo de la operación*). Solamente respecto a esta casuística cabrá apreciar incumplimiento desde una perspectiva tradicional.

La mencionada reducción de la posibilidad de que se produzca incumplimiento (evitando así la acudida a mecanismos de cumplimiento forzoso por vía judicial) supondría una eficiencia, así como una reducción en costes, considerables. No obstante, también esta ventaja tiene los inconvenientes que se muestran a continuación.

#### ***3.5.2 Problemas en cuanto al automatismo y la irreversibilidad***

La ejecución automática e irreversible de los SC, conlleva los siguientes inconvenientes:

- a) Resulta difícil, si no imposible, paralizar la ejecución o exigir el cumplimiento de las obligaciones por cuestiones de validez, eficacia o, simplemente, porque así lo deseen las partes.

---

<sup>102</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid 2018. (p. 108).

- b) En los supuestos de resolución o rescisión del contrato (*i.e. en caso de que las circunstancias que llevaron a contratar a las partes hayan cambiado por completo: cláusula rebus*), resulta extremadamente difícil conseguir los efectos legales y materiales de un contrato resuelto. Aunque se tratase de prever todas las circunstancias dentro de la programación de SC, la casuística puede ser infinita.

Dados estos problemas, en la actualidad existen diferentes soluciones tanto para detener la ejecución automática del contrato, como para poder introducir modificaciones en el código y poder así subsanar su irreversibilidad:

- a) Introducir un código en el SC que pueda inhabilitarlo o desactivarlo si se cumplen ciertas circunstancias: denominado código autodestructivo o suicida<sup>103</sup>.
- b) Crear modelos híbridos de la BC que permitan: 1) corregir errores del código o 2) mitigar los efectos de la reversibilidad de la operación realizada 3) forzar la ejecución en caso de inactividad improcedente.
- c) Crear un oráculo dependiente de la autoridad judicial, de manera que el SC, antes de ejecutar las prestaciones, pudiera informarse de si puede llevarlas a cabo o no.
- d) Establecer una condición resolutoria expresa en la BC que opere como resolución contractual (*i.e. vehículo en leasing conectado a dispositivo IoT - conectado con el SC- que impide su puesta en marcha en caso de no haberse pagado la cuota mensual correspondiente*).
- e) En los contratos legales inteligentes o SC híbridos se podrán prever canales alternativos para la efectiva realización de las contraprestaciones acordadas con los requisitos objetivos impuestos por la ley<sup>104</sup>:
  - a. Identidad entre la cosa pactada y la efectivamente entregada (art. 1166 CC).
  - b. Integridad de la deuda satisfecha (art. 1157 CC).
  - c. Indivisibilidad de la prestación (art. 1169 CC).

---

<sup>103</sup> LIVIO, P., *An empirical analysis of smart contracts: platforms, applications and design patterns*, 2017 (p.11).

<sup>104</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 110).

### **3.5.3 Problemas en cuanto a la ejecución de las consecuencias del incumplimiento**

Es preciso un análisis legal tanto de las consecuencias pactadas que deriven del incumplimiento (*i.e. cláusula penal*), como de los diferentes medios para su ejecución. Así, convendrá que a la hora de llevarse a cabo la redacción de un SC se tenga en cuenta la esfera jurídica de las partes, con especial atención a todo lo relacionado con sus derechos y libertades fundamentales (*ejemplo: empresa de alquiler de coches que apaga por control remoto el vehículo de un cliente que no ha realizado un pago, poniendo así en riesgo su integridad física*). Además de lo anterior, para que el SC sea válido, deberá incluir en su código la posibilidad de 1) parar aquellas medidas en caso de que un juez determine su ilegalidad y 2) incluir remedios económicos en caso de ser necesarios.

### **3.5.4 Mención sobre los remedios ante la ejecución defectuosa**

Partiendo de las características de automatización e irreversibilidad anteriormente mencionadas sobre los SC, podemos concluir que gracias a éstos perderá enormemente importancia la acción de cumplimiento en favor de la acción de restitución o indemnización<sup>105</sup>. Respecto a la *restitución*, no hay mayor problema que programar en el SC la devolución sobre propiedad de ítems o sobre pagos. Cuestión más difícil es la de la *indemnización*, ya que en primer lugar debería detectarse el sujeto causante y luego el nexo de causalidad, por lo que la aplicación de los SC en este campo puede resultar difícil.

## **3.6 Sobre la prueba de los *smart contracts* en el proceso**

Tal y como se ha reiterado en este trabajo, la BC garantiza la inmutabilidad de los datos que en ella se almacenan, lo que le otorga una alta fiabilidad probatoria frente a los órganos jurisdiccionales<sup>106</sup>. Habida cuenta que los SC no sólo almacenan de forma fiable estos datos,

---

<sup>105</sup> WERBACH, K., *Contracts ex machina*. Publicado en revista *Duke Law Journal*, vol 67, 2017 (p. 376).

<sup>106</sup> Es tal su fiabilidad que en numerosos países ya se están llevando a cabo iniciativas públicas para la creación de un registro de la propiedad basado en tal tecnología. A modo de ejemplo cabe mencionar la recientemente enmendada *Ley de Sociedades del Estado de Delaware*, en virtud de la cual se permite la contabilización, registro y transmisión de las participaciones sociales a través de la BC.



sino que además ejecutan los acuerdos de forma automática, la prueba de aquéllos ante los órganos jurisdiccionales exigirá la acreditación de los siguientes elementos<sup>107108</sup>:

1. Que las aplicaciones insertadas en el *front* han permitido adecuadamente a las partes la formación de su voluntad (respecto de las obligaciones contenidas en el SC) de forma consciente, informada y libre.
2. Que el SC almacenado en el *back end* lleva a cabo la ejecución prevista por las partes.
3. Todo dato de la BC relativo al mismo y que pueda haber tenido influencia en el resultado (*i.e. información recabada por el oráculo o todos los datos relativos al tiempo y modo de prestación de consentimiento de las partes*).
4. Traducción al lenguaje humano de toda prueba que se pretenda presentar en código<sup>109</sup>. Dicha traducción será únicamente relevante a efectos de comprensión (por el juez, los abogados y las partes) dado que el SC ya tiene valor probatorio (art. 24 LSSI).

El medio idóneo para llevar a cabo la acreditación de lo anteriormente expuesto es la prueba pericial. Para ello, según apunta TUR FAÚNDEZ, C. será precisa una nueva generación de peritos jurídico-informáticos que posean los conocimientos necesarios para interpretar de forma adecuada las interacciones que tienen lugar entre el software y la esfera jurídica y que al mismo tiempo puedan analizar y llevar a cabo traducciones como la anteriormente expuesta en el punto 4.

### **3.7 Sobre la función del abogado, juez, notario y registrador**

A pesar de lo que en muchos sectores del mundo de la BC se esté prediciendo la desaparición de estas figuras gracias a la introducción de los BC, la realidad actual y su porvenir parecen distar bastante de este escenario. Ello es debido a que los juristas no son meros autómatas, sino

---

<sup>107</sup> TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (p. 106).

<sup>108</sup> O'SHIELDS, R., *Smart Contracts: Legal Agreements for the Blockchain*, 2017 (p. 190).

<sup>109</sup> LEGERÉN-MOLINA, A., *Los contratos Inteligentes en España: la disciplina de los smart contracts* publicado en la Revista de Derecho Civil, vol. V, núm. 2, en abril-junio de 2018 (p. 230).

intérpretes del derecho, por lo que su intervención humana aún está muy lejos de ser innecesaria (la inteligencia artificial debería alcanzar un estadio de desarrollo mucho mayor al previsto). Lo que sí parece conveniente, a medio y largo plazo, es que adquieran los conocimientos de programación o de interpretación necesarios para analizar y redactar SC evitando la constante traducción a lenguaje humano.

### ***Especial mención al Derecho notarial y registral***

Existe un error ampliamente asentado entre la comunidad jurídica y de la BC acerca de la futura desaparición de los notarios y registradores como consecuencia de la implantación de la tecnología de la DLT. No obstante, este error proviene del Derecho del mundo anglosajón en el que tales figuras únicamente validan cuestiones de hecho y no de derecho<sup>110</sup>. En el Derecho Continental los notarios y registradores realizan controles de legalidad, lo cual no puede ser realizado por la propia BC. Es por este motivo que las principales aportaciones que puede realizar la BC al sistema notarial y registral de la actualidad son:

- Reducir los costes administrativos de transacción (*i.e. eliminando el coste del depósito notarial de documentos*).
- Dar soporte a los documentos enviados a través de las comunicaciones electrónicas: protegiendo y encriptando así la información enviada.
- Realizar todo lo que tenga que ver con el control de hecho (*i.e. cotejo material de documentos o comprobación de la presencia de las partes*).

Dadas estas ventajas y el desarrollo actual de la tecnología DLT, en Europa se han llevado a cabo innumerables iniciativas con el objetivo de adaptar la profesión notarial y registral al nuevo paradigma ofrecido por la cadena de bloques<sup>111</sup>, entre las que, a modo ejemplificativo mencionamos:

---

<sup>110</sup> IBÁÑEZ JIMÉNEZ, J., *Cuestiones jurídicas en torno a la cadena de bloques (Blockchain) y a los contratos inteligentes (smart contracts)*, publicado en Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales de ICADE, nº 101 (p. 5).

<sup>111</sup> Diario jurídico, *Notarios de toda Europa analizan el uso de nuevas tecnologías como el Blockchain*: <https://www.diariojuridico.com/notarios-toda-europa-analizan-uso-nuevas-tecnologias-blockchain/> Noticia ejemplificativa de tal fenómeno. Consulta válida a 6/4/2019.

1. *Proyecto EUFides*<sup>112</sup>: plataforma electrónica procesada en *cloud* que pretende la conexión telemática segura y eficaz de las notarías de toda Europa.
2. *Notarchain.es*<sup>113</sup>: base notarial digital que, mediante la implementación de una serie de protocolos *opensource*, permite la certificación, archivo y registro de actos y acuerdos contractuales.
3. *Stampery*<sup>114</sup>: plataforma española de certificación de documentos basada en *Blockchain* que demuestra de forma fehaciente la prueba sobre la integridad y existencia de documentos jurídicos.

---

<sup>112</sup> <http://www.notaries-of-europe.eu/index.php?pageID=8033> Página en la que se explica el proyecto EUFides. Consulta válida a 6/4/2019.

<sup>113</sup> <https://cdn.website-editor.net/58f6731a2aa84651bc30221ac2adeaf1/files/uploaded/FAQ%20ESP.pdf> Página en la que se explica el proyecto Notarchain.es. Consulta válida a 6/4/2019.

<sup>114</sup> <https://stampery.com/features> Página en la que se explica el proyecto Stampery. Consulta válida a 6/4/2019.

## **4. APLICACIONES MÁS PRÓXIMAS DE LOS SMART CONTRACTS AL DERECHO MERCANTIL**

### **4.1 Comercio electrónico**

La contratación electrónica a través de la cadena de bloques puede suponer una total revolución para el comercio electrónico en cuanto a los siguientes parámetros:

#### ***4.1.1. Generación de confianza entre los clientes***

Desde los inicios de internet, el desarrollo del e-commerce ha experimentado un crecimiento vertiginoso en cuanto a volumen de negocio<sup>115</sup> y una increíble mejora en cuanto a eficiencia y logística. No obstante, infinidad de marketplaces y su modalidad de contratación a distancia siguen arrastrando un gran inconveniente: la inseguridad<sup>116</sup>. Ésta ha venido determinada principalmente por la confianza transaccional y la falta de verificación de identidades. No obstante, como se ha explicado a lo largo de todo el trabajo, ambos problemas pueden ser satisfactoriamente superados por la tecnología DLT.

#### ***4.1.2 Minimización de los costes de transacción***

La BC tiene la capacidad de procesar pagos, gestionar inventarios y almacenar multimedia y descripciones. Todo ello significa una reducción de costes de mantenimiento del sistema y menos tareas administrativas que llevar a cabo. Si lo anterior se combina con el soporte de una eficiente y potente plataforma en la que poder anunciar correctamente los productos de venta, los empresarios podrían dedicar sus recursos a la gestión propia de su negocio y menos a mantener y controlar su tienda online<sup>117</sup>, lo cual supondría un inmenso ahorro de gastos operativos.

---

<sup>115</sup> <https://www.statista.com/statistics/281241/online-share-of-retail-trade-in-european-countries/> Gráfica en la que se explica la evolución del E-commerce. Consulta válida a 31/3/2109.

<sup>116</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 131).

<sup>117</sup> *How Blockchain is impacting Ecommerce?:* <https://igniteoutsourcing.com/blockchain/how-blockchain-is-impacting-ecommerce/> (ver apartado sobre reducción de costes). Consulta válida a 31/3/2019.

### **4.1.3 Control de ventas secundarias**

Gracias a la posibilidad de identificación de usuarios (dependiendo de la BC) y las transacciones asociadas a los mismos, es posible el seguimiento de activos (tanto on-chain como off-chain) y sus poseedores, permitiendo o impidiendo hechos como creación de activos asociados a un único usuario (*i.e. impidiendo reventa de entradas*) o controlar/limitar las condiciones en las que se realizan las transacciones (*i.e. estableciendo un múltiplo límite de precio de reventa a los proveedores*).

## **4.2 Propiedad Intelectual**

La tecnología *Blockchain* (junto con el carácter P2P de las redes no permissionadas y unida los avances en el campo del *Internet of Things*) permite la conexión directa entre los autores de la propiedad intelectual y a los consumidores de sus obras<sup>118</sup>, habilitando la consecución de tres fenómenos:

- a) Descentralización de la gestión de la identidad de los autores.
- b) Mejora de la tutela de los derechos de los autores en cuanto a sus derechos económicos y patrimoniales derivados de su condición de propietarios de tales creaciones.
- c) Correcta negociación de los derechos de autor: conociendo el uso o consumo exacto de tales obras por los usuarios.

*Ejemplo explicativo:*

*Supongamos una plataforma de servicio de reproducción streaming de música. En ella los autores suben la música y los usuarios la consumen a cambio de pagar una cuota mensual. La identidad de los autores sería verificada por la BC por lo que conseguimos un ahorro inmenso de personal que verifique la identidad de los autores y detecte y elimine las obras de falsa autoría. Por otro lado, se establecería de forma justa un reparto de los beneficios de la plataforma ya que: a) no existen costes de transacción (el 100% de lo recaudado sería para los productores) y b) el reparto de la recaudación sería totalmente justo (cada mes se reparte en función de las reproducciones de los usuarios).*

---

<sup>118</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 259).

### **4.3 Sector financiero**

La práctica totalidad de los servicios prestados por la banca puede ser reconducida y llevada a cabo mediante la aplicación de la tecnología DLT. Para llevar a cabo su análisis, dividiremos el estudio de la aplicabilidad de los SC y la BC en diferentes sectores:

#### **4.3.1 Banca comercial**

##### **4.3.1.1 Sistema de pagos y transferencias a distancia**

El principal sistema financiero de pagos y transferencias suele padecer los problemas de ser lento y caro. Ambos son solventados gracias a la tecnología *Blockchain* a través de dos procesos:

1. Eliminación de los intermediarios: reduciendo así comisiones de gestión e intermediación en transferencias, pagos y cobros y eliminando la litigiosidad asociada a disputas relacionadas con practicas bancarias abusivas o antijurídicas<sup>119</sup>.
2. Generación de inmediatez en envíos monetarios: las transferencias y pagos, tanto de criptomonedas o tokens, como en dinero fiat, pueden realizarse prácticamente de forma instantánea y segura a través de la BC, trasladando el dinero de una cartera a otra. El tiempo de validación de la transacción dependerá de las características de la BC<sup>120</sup>, así como de las teconologías asociadas a ellas (*i.e. lightning*<sup>121</sup>).

##### **4.3.1.2 Compensación de créditos**

Numerosas plataformas Fin Tech basadas en *Blockchain* y en SC permiten mejorar los servicios de tesorería de compensación de créditos a través de la liquidación automática de deudas que se encuentran en cadenas de compensación (*i.e. A debe a B, B debe a C y C a A*), sin existir conocimiento entre deudores (arts. 1195 a 1202 CC)<sup>122</sup>. El método que tienen estas

---

<sup>119</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 174).

<sup>120</sup> *The Fastest Cryptocurrency Transaction Speeds for 2018*: [https://medium.com/@johnhinkle\\_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-498c1baf87ef](https://medium.com/@johnhinkle_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-498c1baf87ef) Página en la que se analiza el tiempo de validación de diferentes criptomonedas. Consulta válida a 2/4/2019.

<sup>121</sup> *What Is Lightning Network And How It Works*: <https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works> Página en la que se explica las diferentes funcionalidades de la criptomoneda Litecoin. Consulta válida a 2/4/2019.

<sup>122</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 183).

plataformas de hallar créditos compensables es a través de complejos algoritmos de búsqueda de compatibilidad y conexión entre los mismos.

#### **4.3.1.3 Contabilidad y registro**

Por su propia naturaleza, y como ya se ha reiterado en este trabajo, la cadena de bloques puede llevar a cabo un rol de registro de operaciones similar al que desempeñan hoy los archivos, registros y repositorios privados de las empresas (e incluso más versátil y potente). En el sector financiero, la correcta, eficiente y transparente consecución de estas actividades, tanto desde el punto de vista legal como funcional, es indispensable. La introducción de la tecnología DLT, así como de los SC en el sector bancario mejorará tanto la contabilidad como el registro de estas operaciones financieras en cuanto a los siguientes aspectos:

1. Mejora de la gestión financiera a través de la automatización integral de los procesos de toma de decisiones. Una estructura combinada de BS y SC que prevea árboles de toma de decisiones óptimas para una variedad de escenarios contables y patrimoniales puede suponer una clave diferencial en cuanto al desarrollo de las instituciones financieras.
2. Eliminación del posible fraude contable, a través del tracto registral de la BC, tanto por quien lleva a cabo el registro como por quien lo audita. Ello elimina infinidad de costes operativos asociados a los mecanismos de control bancario por parte de las instituciones.

#### **4.3.2 Banca de inversión**

La introducción de los SC y la BC producirá importantes mejoras en la banca de inversión en los siguientes aspectos:

1. Ejecución inmediata y segura<sup>123</sup> de las transferencias de dinero e intercambios de divisas (con la añadidura de una gran reducción en cuanto a costes) entre cualesquiera mercados y jurisdicciones<sup>124</sup>.

---

<sup>123</sup> European Securities and Markets Authority: *The Distributed Ledger Technology Applied to Securities Markets*, 2017 (p. 5).

<sup>124</sup> IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (p. 187).

2. Mejora del sistema de las cámaras de compensación: el proceso de compensación de operaciones financieras actual es lento (puede llegar hasta las 48h de duración<sup>125</sup>) e ineficiente (debido a los numerosos intermediarios e instituciones de por medio<sup>126</sup>). Ambos problemas pueden ser resueltos por los SC y la tecnología DLT, sin perder la protección que precisa el cliente, a través de sus propiedades anteriormente reiteradas de descentralización (en las redes no permissionadas) y ejecución automática de transacciones.
3. Mejora de la vigilancia de las inversiones: gracias al tracking que la DLT y los SC proporcionan, será posible tener controlado en todo momento en qué están siendo destinados los fondos invertidos y si están cumpliendo las expectativas pactadas.
4. Mejora del control y auditoría pública en cuanto al cumplimiento de la legalidad por parte de las instituciones inversoras<sup>127</sup>.

### **4.3.3 Financiación de proyectos empresariales**

Una de las mayores utilidades de los SC en el sector financiero es lo referido al *levantamiento* de fondos para el desarrollo de proyectos a través de la *tokenización* de los mismos<sup>128</sup>. Los tokens (unidad de valor que representa una porción de una realidad presente o futura), generalmente utilizados en a modo de acciones o participaciones, son emitidos por las empresas en los denominados ITO (*Initial Token Offering*<sup>129</sup>) para conseguir dinero por parte de los inversores y así poder desarrollar sus proyectos. Aquéllos, dependiendo de la naturaleza que posean tendrán un tratamiento legal u otro, con sus correspondientes controles por parte de las administraciones<sup>130</sup>. La tokenización de los proyectos ha ofrecido una solución eficaz, económica y accesible a pequeños negocios o iniciativas que no cuentan con los medios necesarios para tener una proyección amplia a la hora de buscar financiación a gran escala.

---

<sup>125</sup> *Modernizing Clearing Through Blockchain*: [https://medium.com/@jd\\_32421/modernizing-clearing-through-blockchain-f16397ddee51](https://medium.com/@jd_32421/modernizing-clearing-through-blockchain-f16397ddee51) (párrafo 4º). Consulta válida a 3/4/2019.

<sup>126</sup> CMNV: *Reform of the Registry, Clearing and Settlement System*, 2013 (p. 92).

<sup>127</sup> <https://blog.bankofhodlers.com/how-blockchain-technology-improves-the-banking-industry/> (apartado referido a la banca de inversión). Consulta válida a 3/4/2019.

<sup>128</sup> *How blockchain technology can improve the banking industry*: <https://www.bbva.com/en/what-is-a-token-and-what-is-it-for/> Artículo en el que se realiza una explicación del proceso de tokenización. Consulta válida a 3/4/2019

<sup>129</sup> *Initial Token Offerings - Five Things That You Need To Know About Them*: <https://www.walkersglobal.com/index.php/publications/100-article/987-initial-token-offerings-five-things-that-you-need-to-know-about-them> (párrafo 4º). Consulta válida a 3/4/2019.

<sup>130</sup> *Por ejemplo, cabe destacar el debate entre la consideración diferencial de utility y security token.*



#### **4.3.4 Contrato Escrow desintermediado**

El contrato escrow está basado en la retención de fondos (por un tercero) que financian una transacción hasta que el bien es entregado o el servicio provisto satisfactoriamente. Gracias a la tecnología DLT este tercero, y sus costes asociados, pueden desaparecer de la operación. *Un ejemplo de esta aplicación sería una plataforma de crowdfunding en la que se recaudan fondos para llevar a cabo proyectos y que, en caso de no alcanzarse la cifra necesitada, las aportaciones son devueltas a los inversores en su total integridad.*

#### **4.3.5 Sistema monetario**

Aunque la aplicación monetaria de las criptomonedas sea quizá la mayor aplicación de la tecnología *Blockchain*, por motivos de espacio (y por no ser la materia para cubrir) en este trabajo no se explicarán exhaustivamente. Simplemente, a modo de resumen, cabe resumir que desde la invención del Bitcoin, numerosas criptomonedas han sido creadas con la intención de crear un sistema monetario supraestatal pretendiendo limitar el control de oferta monetaria por parte de la banca central, evitando así los ciclos financieros y económicos causados por los fenómenos de expansión crediticia descontrolada.

### **4.4 Sector asegurador**

Las principales aplicaciones de los SC en el sector asegurador vienen determinadas por dos elementos explicados anteriormente en este trabajo:

- a) Autogobierno sobre la identidad: este factor, unido a una red DLT con identidades reconocidas por instituciones acreditadas (ver apartado 3.1.1.2 *Sobre la identidad y los SC*) permite mostrar de forma fehaciente información verificada útil para las aseguradoras, de forma sencilla y segura, y siempre bajo el consentimiento del usuario<sup>131</sup>. *Ejemplos de ello serían el historial médico, historial delictivo o informes previos de otras aseguradoras.*
- b) Coordinación con *Internet of Things* e Inteligencia Artificial: gracias a la posible coordinación de los SC con tales tecnologías es posible conocer una información

---

<sup>131</sup> LAMBERTI, F., GATTESCHI, V., DEMARTINI, C., PRANTEDA, C., SANTAMARÍA, V., *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?*, 2018 (p. 7).

ingente del usuario asegurado. Estos datos poseen una gran relevancia tanto antes del cálculo de las primas (*i.e. una aseguradora médica que predice mediante Inteligencia Artificial y minado masivo de datos cuáles son las enfermedades que potencialmente va a tener el cliente en los próximos años*), como a la hora de pagar por ellas (sistema de peritaje automático de una aseguradora de vehículos que analiza la velocidad a la que conduce el piloto antes de tener el accidente). Otra de las aportaciones del IoT en combinación con los SC al mundo de las aseguradoras es la denominada modalidad *pay-per-use*, en la que el precio a pagar por los usuarios se adapta según ciertas variables sobre aquello que cubre la póliza (*i.e. aseguradora de coches que cobra sólo cuando se está conduciendo*)<sup>132</sup>.

#### 4.5 Logística y trazabilidad

La logística es una de las ramas empresariales en las que más impacto puede tener la introducción del SC en los próximos años, el cual se verá reflejado sobre los siguientes aspectos:

- a) Aumento de eficiencia de los procesos, gracias a los motivos extensamente explicados a lo largo del trabajo, a saber: 1) eliminación de intermediarios (con la reducción de costes que ello supone); 2) coordinación con IA y IoT (tracking de los ítems provistos, almacenados y comercializados); y 3) transparencia y precisión en cuanto a la información contenida en los documentos involucrados (se estima que un 10% del coste de la factura final en el comercio logístico es debido a disputas sobre las imprecisiones en las facturas<sup>133</sup>).
- b) Transporte masivo de información de los ítems y confidencialidad de la misa: debido a la capacidad de los SC de almacenamiento de información, los SC asociados a productos de la cadena pueden almacenar y tratar todos los datos relativos a los mismos, con las ventajas que en ello pueda derivar (*i.e. incorporación de minado de datos o eliminación del papeleo asociado al proceso*). Además de lo anterior, gracias a la característica de transparencia multinivel (explicada en el apartado 2.5.4) los SC tienen la capacidad de transportar información privada a lo largo de la cadena productiva de

---

<sup>132</sup> LAMBERTI, F., GATTESCHI, V., DEMARTINI, C., PRANTEDA, C., SANTAMARÍA, V., *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?*, 2018 (p. 7).

<sup>133</sup> KÜCKELHAUS, M., *Blockchain in logistics*, 2018 (p. 17).

forma oculta, y siendo únicamente mostrada en aquellos apartados que sea necesaria (a conveniencia del empresario) a los agentes que sea preciso.

## 5. CONCLUSIONES

1º) Actualmente, los contratos privados convencionales padecen múltiples limitaciones. Entre ellas podemos destacar las siguientes: su cumplimiento no está garantizado, son costosos, pueden contener fallos, no son inmutables y no están preparados para coordinarse con las nuevas tecnologías.

2º) La conjugación de los *smart contracts* con tecnología DLT supone una gran oportunidad para la contratación privada en cuanto a su modernización y actualización digital. Ello es así debido a las múltiples ventajas que son capaces de ofrecernos, entre las cuales podemos destacar: autoejecución, inmutabilidad, eficiencia, autogobierno de la identidad personal y posible coordinación con otras tecnologías (como IoT o IA).

2º) Es por tal motivo que una parte relevante de los problemas que actualmente padecen los contratos convencionales podrán ser resueltos en un futuro gracias a la implementación de los SC: se reducirán los casos de incumplimiento, se hará más rápida y eficiente la ejecución de las contraprestaciones y aumentará la transparencia o la confidencialidad de la información allá donde proceda.

3º) No obstante, tal implementación no está libre de obstáculos, pues el encaje jurídico de los contratos inteligentes no es del todo sencillo:

3.1) En primer lugar, es posible que en ocasiones puedan no reunir alguno de los elementos esenciales del contrato. De todos ellos el más problemático será el del consentimiento, pues a la hora de prestarlo las partes deberán no sólo ser conscientes de que sus prestaciones se van a ejecutar de forma automática, sino ser conocedoras de las propias prestaciones en sí y de todas las condiciones que las afectan (tarea compleja que precisará trasladar el código al lenguaje humano satisfactoriamente).

Sobre este respecto, cabe realizar una especial mención acerca de la adaptación a los contratos afectados por la normativa de consumo, la cual genera infinidad de limitaciones a los SC de difícil implementación, entre las que podemos destacar los derechos especiales que le asisten al consumidor (*i.e. derecho de desistimiento sin*

*motivo alguno en contratos a distancia*) o los contratos convenidos por un asistente virtual (contrato entre máquinas).

3.2) En segundo lugar, deberá seguir los requisitos de forma dispuestos en el Código Civil. A saber: aquella será libre, excepto cuando la ley imponga que sea de forma escrita (caso en el que deberá acompañarse de un formato convencional privado) o elevada a documento público (en cuyo caso no podrá tener lugar el SC).

3.3) En tercer lugar, respecto al procesamiento de información por los SC cabe realizar las siguientes apreciaciones:

3.3.1) Sólo con capaces, por sí mismos, de procesar datos objetivos de la propia BC (por lo que nunca podrán trabajar con condiciones que requieran valoración humana *-i.e. apreciación de un juez-*)

3.3.2 Gracias a unos dispositivos conectados a la BC denominados *oráculos*, los SC son capaces de procesar información que provenga del mundo externo a la BC (*i.e. condiciones meteorológicas*) y que pueda transformarse en datos objetivables.

3.4) Finalmente, la característica de ejecución automática que los define puede presentar inconvenientes en aquellos casos en los que haya sido mal programado el código o la BC haya recibido información falsa del exterior. En tales escenarios deberá diseñarse casos a través de una doble vía: mediante programación en el código (que permita detener y revertir la ejecución) y mediante mecanismos legales (en caso de que sea un SC híbrido serán los mismos que en contrato privado convencional).

4º) De poder solventarse los problemas anteriormente planteados, los SC supondrán innumerables mejoras de ciertos campos de la actividad mercantil. Entre las principales actividades que podrían beneficiarse a corto plazo, se pueden citar los siguientes:

4.1 El comercio electrónico: reducción los costes involucrados a través de la desintermediación y aumentando la confianza entre los clientes.

4.2 Propiedad intelectual: descentralizando la gestión, mejorando la tutela de los derechos económicos y patrimoniales de los autores y haciendo más eficiente su proceso de negociación.

4.3 Sector financiero: haciendo más baratos e inmediatos los pagos y las compensaciones de créditos, aumentando la seguridad en la contabilidad o tokenizando iniciativas empresariales.

4.4 Sector asegurador: obteniendo información mucho más precisa a través de la coordinación con IoT y mejorando la protección de datos privados de los usuarios.

4.5 Logística y trazabilidad: transformando masivamente información y gestionándola a través de IoT e IA.

5º) Con todo, podemos afirmar que la aplicación de los contratos inteligentes puede suponer una considerable mejora respecto a las limitaciones que ahora plantean los contratos convencionales. Es por ello que será preciso que en un futuro el legislador permita una implementación que sea lo más cómoda y sencilla para la sociedad del mañana.

## **Bibliografía**

### **1. Legislación**

#### ***Europea:***

- 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 (Diario Oficial de la Unión Europea).
- Directiva 2011/83/UE del Parlamento Europeo y del Consejo de 25 de octubre de 2011 sobre los derechos de los consumidores (Diario Oficial de la Unión Europea).

#### ***Nacional:***

- Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil (Boletín Oficial del Estado).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia (Boletín Oficial del Estado).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (Boletín Oficial del Estado).
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (Boletín Oficial del Estado).
- Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación (Boletín Oficial del Estado).

### **2. Jurisprudencia**

- Sentencia del Tribunal Supremo de 20 de enero 354/2014, fundamento jurídico decimoprimer (CENDOJ).

- Sentencia del Tribunal Supremo de 30 del junio 2823/2014, fundamento jurídico segundo, apartado sexto (CENDOJ).
- Sentencia del Tribunal Supremo de 24 de noviembre 5235/2016, fundamento jurídico quinto, apartado tercero (CENDOJ).

### 3. Obras doctrinales

- ANKALKOTI, P., *A relative Study on Bitcoin Mining*, 2017 (p.2).
- ARIJA SOUTULLO, C., *La condición en el contrato. Inscripción en el Registro de la Propiedad*, publicado en la Revista de Derecho Civil (vol. V, núm. 2) en abril-junio de 2018 (p. 282).
- ARNAU MOYA, F., *Lecciones de Derecho Civil II: obligaciones y contratos*, Universitat Jaume I, Castellón de la Plana, 2009 (p. 147).
- BUTERIN, V., *Ethereum White Paper: A next generation smart contract & decentralized application platform*, 2013. (p. 2 y ss.). Disponible en: [http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf) Consulta válida a 21/3/2019.
- BUTERIN, V., *Ethereum White Paper: A next generation smart contract & decentralized application platform*, 2013. (p. 2 y ss.). Disponible en: [http://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf) Consulta válida a 21/3/2019.
- CIAIAN, P., *Blockchain Technology and Market Transparency*, 2018 (p. 11).
- FELIU REY, J., *Autonomía privada y autotutela: oportunidades y riesgos de los Smart Contracts*. Publicado en Sociedad Digital y Derecho (pp.811-834), 2018 (p. 811).
- GAYLE HYMAN, M. y DIGESTI MATTHEW P., *New Nevada legislation recognizes Blockchain and Smart Contract technologies*, junio de 2017 (p.1).
- GOMEZ POMAR, F., *El incumplimiento contractual en el Derecho español*. Publicado en Revista para el Análisis del Derecho, vol. 3, 2007 (pp. 4-38).
- GRECH, A. y CAMILLERI, A., *Blockchain in Education*, 2017 (p.19).



- GRECH, A., y CAMILLERI, A., *Blockchain in Education*, 2017 (p.20).
- GROSSMAN SANFORD, J. y OLIVER, H., *The costs and benefits of ownership: A theory of vertical and lateral integration*, *Journal of Political Economy*, 1986 (p. 698).
- IBÁÑEZ JIMÉNEZ, J., *Cuestiones jurídicas en torno a la cadena de bloques (Blockchain) y a los contratos inteligentes (smart contracts)*, publicado en *Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales de ICADE*, nº 101 (quinto artículo).
- IBÁÑEZ JIMÉNEZ, J., *Derecho de Blockchain*, Aranzadi, Navarra, 2018 (págs. 31, 40, 41, 43, 56, 131, 174, 183, 259).
- KOSBA, A., MILLER, A., SHI, E., WEN, Z. y PAPAMANTHOU. C., *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*, 2016 (p. 3).
- KRITIKOS, M., *What if Blockchain offered a way to reconcile privacy with transparency?*, 2018 (p. 1).
- KÜCKELHAUS, M., *Blockchain in logistics*, 2018 (p. 17).
- LAMBERTI, F., GATTESCHI, V., DEMARTINI, C., PRANTEDA, C., SANTAMARÍA, V., *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?*, 2018 (p. 7).
- LEGERÉN-MOLINA, A., *Los contratos Inteligentes en España: la disciplina de los smart contracts* publicado en la *Revista de Derecho Civil* (vol. V, núm. 2) en abril-junio de 2018 (pp. 193-241).
- LIVIO, P., *An empirical analysis of smart contracts: platforms, applications and design patterns*, 2017 (p.11).
- LONDON. N., *An Introduction to Roman Law*, Oxford, Glasgow, 1963 (p. 158).
- MARSHALL, S., SHELKOV, A., WELMANS, T., y WALSH, K., *Blockchain, democratised trust: Distributed Ledgers and the Future of Value*, 2016 (p. 86).
- MATTILA, J. y SEPPÄLÄ, T., *Smart Contracts: How will Blockchain Technology Affect Contractual Practices*. Publicado por The Research Institute of the Finnish Economy (vol. 68) en enero de 2017 (págs. 1-27).
- NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009 (p. 1). Disponible en: <https://bitcoin.org/bitcoin.pdf> Consulta válida a 21/3/2019.

- NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009. Disponible en: <https://bitcoin.org/bitcoin.pdf> Consulta válida a 21/3/2019.
- NAKAMOTO, S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2009 (p. 3). Disponible en: <https://bitcoin.org/bitcoin.pdf> Consulta válida a 21/3/2019.
- O'SHIELDS, R., *Smart Contracts: Legal Agreements for the Blockchain*, 2017 (p. 190).
- PANISI, F., *Blockchain and Smart Contracts: Fintech Innovation to Reduce the cost of Trust*, 2017 (p. 8).
- PUIG BRUTAU, J., *Fundamentos de Derecho Civil II, vol. II*, Boch, Barcelona, 1986 (p.141).
- SAVELYEV, A., *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of the Classical Law*, 2016 (p.12).
- SAVELYEV, A., *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of the Classical Law*, 2016 (p.17).
- SEANG, S. y TORRE, D., *Proof of Work and Proof of Stake consensus protocols: a Blockchain application for local complementary currencies*, 2018. Disponible en: <https://gdre-scpo-aix.sciencesconf.org/195470/document>
- SEGURA ORTEGA, M., *Problemas interpretativos e indeterminación del Derecho*. Publicado en revista *Dereito* (vol 22) en noviembre de 2013 (p. 677).
- SZABO, N., *Smart Contracts: Building Blocks for Digital Markets*, 1996. Disponible en: [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html) Consulta válida a 21/3/2019.
- TUR FAÚNDEZ, C., *Smart Contracts: Análisis jurídico*, Reus, Madrid, 2018 (págs. 77, 81, 88, 106, 108, 110, 111, 113, 117).
- WERBACH, K., *Contracts ex machina*. *Revista Duke Law Journal*, vol 67, 2017 (pp. 314-381).