InDret
2.2020

Smart contracts o *Code is Law*: soluciones legales para la robotización contractual

Cristina Argelich Comelles
Universidad de Cádiz
-

Sumario

-

El presente trabajo ofrece soluciones a los problemas jurídicos que plantean los smart contracts, *por tratarse de cláusulas contractuales autoimplementadas en un código informático que autoejecuta su contenido. Estos versan sobre su discutida naturaleza jurídica, la adhesión del consumidor 2.0 mediante* Blockchain, *su personalización con* Ethereum, *los errores de programación y la responsabilidad civil, la protección y encriptación de datos de carácter personal, y la formación y ejecución del contrato. Las dificultades que plantean los* smart contracts *requieren de una regulación europea, inspirada en las legislaciones existentes en algunos territorios de los Estados Unidos y Francia, así como en los estudios formulados en el ámbito de UNIDROIT y la CNUDMI.*

Abstract

-

This paper suggests legal remedies for smart contracts, based on a code that self-implement contractual clauses to self-execute its content. These problems refer to its legal nature, the adhesion of adprosumer through Blockchain, the personalization of smart contracts with Ethereum, programming errors and civil liability, protection and encryption of personal data, and contract formation and execution. All these difficulties need an EU Law inspired in US Law, French Law and in studies in the field of UNIDROIT and UNCITRAL.

Title: *Smart contracts or Code is Law: legal remedies for contractual robotization*

-

Palabras clave: contratos inteligentes, tecnología *blockchain*, Derecho de contratos, autoimplementación, responsabilidad civil, Internet de las cosas.
Keywords: *smart contracts, blockchain technology, Contract Law, self-implementation, civil liability, Internet of Things.*

-

DOI: 10.31009/InDret.2020.i2.01

InDret

2.2020

Recepción
27/11/2019
-
Aceptación
10/2/2020
-

Índice

-

1. Consideraciones previas sobre los* smart contracts *y su desregulación
2. La conceptuación de los* smart contracts*: acerca de su naturaleza jurídica
2.1. *Smart contracts in the books:* aplicación acrítica del código informático a un contrato vs. ámbito material de aplicación
2.2. Críticas al concepto de *smart contract* y reafirmación de su naturaleza contractual
2.3. *Smart contracts in action* y *M2M contracts*
***3. Tecnología* blockchain*: la adhesión contractual mediante* Blockchain *y la personalización con* Ethereum**
3.1. El *adprosumer* o consumidor 2.0 y los *smart contracts*
3.2. La plataforma *Blockchain* y el papel del registro distribuido en la adhesión contractual
3.3. La plataforma *Ethereum* o la *blockchain* de los *smart contracts* personalizados: un *"Smart Contract Inventor"* y la iconificación de las prestaciones
4. Errores de programación, responsabilidad civil objetiva y protección de datos de carácter personal
***5. La formación y la ejecución de los* smart contracts: autoimplementación y autoejecución**
5.1. La formación y la ejecución del contrato: tratamiento de la invalidez y la ineficacia en sentido estricto
5.2. La automatización de los remedios: algunas limitaciones por razón del objeto, y el papel del *Internet of Things* y la Tokenización
6. Conclusiones
7. Bibliografía

-

Este trabajo se publica con una licencia Creative Commons Reconocimiento-No Comercial 4.0 Internacional

1. Consideraciones previas sobre los smart contracts y su desregulación*

"Lex ex machina" o el "Derecho desde la máquina" sería la expresión metafórica de lo que entrañan los *smart contracts* o contratos inteligentes: la "robotización" de la formación y ejecución del contrato en un contexto de digitalización. Los *smart contracts* van más allá de la informatización del contrato producida por el comercio electrónico porque, una vez perfeccionado el contrato, automatizan la fase de ejecución. Este nuevo paradigma reserva al Derecho un papel que le es impropio, si consideramos la necesaria tarea interpretativa para aplicarlo al caso concreto. Asimismo, se alteran las bases de la contratación tradicional, porque se sustituye la confianza en la contraparte y su solvencia en favor de un código informático, que mecaniza las prestaciones y su *enforcement* al margen de la jurisdicción, reforzando el papel de la *self-help* o remedios privados para adaptar el contrato o desvincularse.

En este contexto, el legislador no tiene otra opción que afrontar las consecuencias de la digitalización que se está produciendo en la contratación, cuyos inconvenientes desarrollaremos a lo largo de este trabajo, pues lo contrario aboca a quienes utilicen los *smart contracts* a la inseguridad jurídica y los abusos, especialmente en la negociación con consumidores. Actualmente, algunos Estados[1] de los Estados Unidos –a la espera de una regulación federal[2] (DEWEY, 2019) y de otros Estados[3] que la han proyectado–, y algunos estados del ámbito europeo[4], como Francia, Malta y Mónaco, entre otros, han legislado sobre *blockchain* y *smart contracts*. Por

* Autor de contacto: *Cristina Argelich Comelles, cristina.argelich@uca.es*.

[1] Los Estados se refieren cronológicamente a Vermont, Nevada, Delaware y Arizona. El 6 de febrero de 2016, Vermont aprobó la *Bill Status H.868* (https://legislature.vermont.gov/statutes/section/12/081/01913), que en el § 1913 regula el uso de la tecnología *blockchain*. DEMCHENKO (2018, p. 47). GILCREST (2018, pp. 1-5). El 5 de junio de 2017, Nevada reguló el uso de la tecnología *blockchain* en la *Senate Bill Nº. 398: Establishes various provisions relating to the use of blockchain technology* (https://legiscan.com/NV/text/SB398/id/1626453), y que modificaba el *Uniform Electronic Transactions Act*. HYMAN (2017, pp. 13-17). El 21 de julio de 2017, Delaware aprobó la *Senate Bill 69: An Act To Amend Title 8 Of The Delaware Code Relating To The General Corporation Law* (https://legiscan.com/DE/text/SB69/2017). Finalmente, el 3 de abril de 2018, Arizona aprobó la *House Bill 2603: Corporations; blockchain technology* (https://legiscan.com/AZ/text/HB2603/id/1718691).

[2] Se ha planteado en la propuesta de *Blockchain Promotion Act of 2018* (https://www.congress.gov/bill/115th-congress/house-bill/6913/text?format=txt).

[3] Véanse cronológicamente Maine, con el Legislative Document No. 950, Senate, To Study Using Blockchain Technology in Conjunction with Paper Ballots in Maine Elections (http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0305&item=1&snum=128), Illinois, con la House Joint Resolution 25 (http://www.ilga.gov/legislation/100/HJR/PDF/10000HJ0025lv.pdf), Hawaii, con la Bill for an Act relating to economic development (https://www.capitol.hawaii.gov/session2017/bills/HB1481_HD1_.htm), y Arizona, con la House Bill 2216 an Act amending title 13, chapter 31, Arizona revised statutes, by adding section 13-3122; relating to firearms (https://apps.azleg.gov/BillStatus/GetDocumentPdf/453206).

[4] (PERCHET, 2019). Véase el Décret n° 2018-1226 du 24 décembre 2018 relatif à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons, JORF de 27.12.2018 (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037852460).

su parte, otros Estados como Canadá[5] (DRUZETA, 2019), Suiza[6] (HAEBERLI, 2019), Singapur[7] (CIAMBELLA, 2019), Gibraltar[8] (GARCIA, 2019), Rusia[9] (STRIZH, 2019), y Estonia[10] (LATT, 2019) están planteando regulaciones en materia de *blockchain*. Fundamentalmente, pretenden hacer frente al blanqueo de capitales que se produce a través de las criptomonedas[11] (BORG, 2019), en atención a los 22 millones de *traders*[12] que existen a nivel mundial, las transacciones que se realizan en cajeros[13] automáticos de criptomonedas, y una futura *criptotarjeta*[14] que van a lanzar al mercado *Visa* y *Coinbase* (FINANCIAL TIMES, 2019). Una regulación en este ámbito permitiría evitar un *"shadow contracting"* o una contratación al margen del Derecho, ejecutada por quienes no se encuentren bajo supervisión, como sucede con las *Fintech*, que operan al margen de la Comisión Nacional del Mercado de Valores (CNMV, 2019). En este sentido, ya señaló (CNMV, 2018) en relación con las *Initial Coin Offering* u oferta inicial de moneda que "no puede excluirse la posibilidad del registro de derechos que puedan tener la consideración de valor negociable a través de la tecnología DLT *(blockchain)*". Ello abrió la puerta a la emisión de obligaciones o acciones de una sociedad representadas en *Tokens*, con el carácter de *Security Token* y exentas de control, conforme al art. 35 apartados segundo y tercero del Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores (BOE nº 255, de 24.10.2015).

Si el uso de la tecnología *blockchain* y su desregulación está ocasionando estos desajustes, la pronta extensión de los *smart contracts* a la contratación en masa va a requerir de una regulación a nivel europeo adaptada al mercado de crédito (GRUNDMANN, 2017, pp. 255-293; MARSH, 2019), que creemos que debería abordarse mediante un Reglamento que garantice su uniformidad en todos los Estados de la Unión. En este sentido, el *EU Blockchain Observatory and Forum,* perteneciente a la Comisión Europea, emitió un Informe (EU BLOCKCHAIN OBSERVATORY AND FORUM, 2019) denominado *"Legal and Regulatory Framework of blockchains and smart contracts"*. En sus conclusiones, formuló una serie de recomendaciones que una regulación europea debería

---

[5] En este sentido, el pasado 15 de marzo de 2019, la *Canadian Securities Administrators* (CSA) y *the Investment Industry Regulatory Organization of Canada* propusieron una regulación para criptomonedas y blockchain conocida como *Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms* (https://www.osc.gov.on.ca/documents/en/Securities-Category2/csa_20190314_21-402_crypto-asset-trading-platforms.pdf).

[6] El Gobierno suizo ha abierto un periodo de consultas para mejorar la regulación de la tecnología *blockchain*. Véase la nota de prensa oficial (https://www.efd.admin.ch/efd/en/home/dokumentation/nsb-news_list.msg-id-74420.html).

[7] La *Monetary Authority of Singapore* está trabajando en una regulación sobre *blockchain* y criptomonedas (https://thetokenist.io/monetary-authority-of-singapore-to-introduce-a-regulatory-framework-for-cryptocurrency-exchanges/).

[8] La *Gibraltar Financial Services Commission's* está proyectando una regulación respecto de *blockchain* en relación con la normativa que ya tienen las DLT.

[9] Desde el 1 de marzo de 2019, el Ministerio de desarrollo económico está impulsando una regulación sobre *blockchain* (https://tass.ru/ekonomika/6175089).

[10] La *Estonian Financial Supervisory Authority* ha publicado una guía para los usuarios de ICOs para regular la venta de *Tokens*.

[11] Sobre el funcionamiento de la tecnología *blockchain* y las criptomonedas, atiéndanse GONZÁLEZ-MENESES (2019, pp. 12-219) y LEGERÉN (2019, pp. 177-237).

[12] Sobre el ranquin mundial, encabezado por Estados Unidos, Japón y Korea, véase la siguiente explicación (https://bitcoin.es/actualidad/japon-segundo-pais-con-mas-cripto-traders-en-el-mundo/).

[13] *Bitcoin* dispone de unos cajeros automáticos para realizar transacciones con esta criptomoneda, e incluso permite ingresar efectivo para convertir el saldo en la criptomoneda, lo que puede servir como vía para el blanqueo de capitales procedentes de actividades delictivas.

[14] *Visa* y *Coinbase* pretenden lanzar al mercado una *criptotarjeta,* es decir, una tarjeta de débito financiada con criptomonedas, con un límite de gasto de 10.000 libras mensuales, que puede aumentar hasta 20.000, sin que de momento hayan garantizado que se va a impedir el blanqueo de capitales con este medio de pago.

atender: crear definiciones simples y útiles de la tecnología *blockchain* en el seno de la Unión; comunicar las interpretaciones legales a los diferentes Estados Miembros; escoger la normativa adecuada en función de la aplicación material de la tecnología *blockchain*; armonizar la normativa y sus interpretaciones; ayudar a los legisladores y operadores jurídicos en la comprensión de la tecnología *blockchain;* centrar la regulación normativa en los casos de uso de la tecnología *blockchain* de alto impacto; alentar la autorregulación y monitorizar la evolución de los usos de *blockchain* minoritarios; y, finalmente, hacer uso de la tecnología *blockchain* como herramienta reguladora, al igual que las plataformas *peer-to-peer* o P2P realizan mediante los mecanismos reputacionales.

Por ahora, el marco normativo español aplicable a los *smart contracts* serán las disposiciones del Código Civil, la normativa relativa al comercio electrónico[15], firma electrónica[16] y dinero electrónico[17], así como la legislación de consumo[18], teniendo en cuenta que los contratos inteligentes parten de una igualdad formal (SAVELYEV, 2017, p. 16) que habrá que armonizar. En el ámbito internacional, debemos referirnos a la normativa sobre comercio internacional de mercancías, que ampara legalmente el uso de los *smart contracts*: en concreto, el art. 12 de la *United*[19] *Nations Convention on the Use of Electronic Communications in International Contracts 2005* dispone el uso de sistemas de mensajes automatizados para la formación de contratos; por otra parte, el art. 6 de la *UNCITRAL*[20] *Model Law on Electronic Transferable Records* reconoce la posibilidad de insertar en un registro electrónico transferible la información contractual, incluyendo los metadatos. Por todo ello, resulta especialmente relevante la actividad que se está desarrollando en el ámbito de UNIDROIT[21] y la CNUDMI[22] –conocida internacionalmente como UNCITRAL–, porque puede inspirar la actividad legislativa de la Unión en un futuro.

UNIDROIT materializó prospectivamente en el *Work*[23] *Programme for the triennial period 2017-2019* (UNIDROIT, 2017), a petición de Hungría[24] y Chequia[25], el estudio de un marco legislativo

[15] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE nº 166, de 12.7.2002).

[16] Ley 59/2003, de 19 de diciembre, de firma electrónica (BOE nº 304, de 20.12.2003).

[17] Ley 21/2011, de 26 de julio, de dinero electrónico (BOE nº 179, de 27.7.2011).

[18] Contenida en las sucesivas reformas del 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 (BOE nº 287, de 30.11.2007).

[19] *United Nations Convention on the Use of Electronic Communications in International Contracts 2005* (https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf).

[20] *UNCITRAL Model Law on Electronic Transferable Records* (https://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf).

[21] Acrónimo del Instituto Internacional para la Unificación del Derecho Privado.

[22] Acrónimo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

[23] Esta propuesta se sometió a la atención de la Asamblea General en su 75º período de sesiones (Roma, 1.12.2016) y posteriormente al Consejo de Administración en su 96º período de sesiones (Roma, 10.5.2016-12.5.2016), durante la cual el Consejo de Administración concluyó que la Secretaría debería continuar siguiendo los desarrollos a este respecto.

[24] En el año 2015, el Ministerio de Justicia de Hungría envió una propuesta a la Secretaría de UNIDROIT para que tomase en consideración el desarrollo de un marco legislativo para las plataformas de servicios, los servicios de software, los servicios de hardware, las bases de datos y la computación en la nube.

[25] En noviembre de 2016, el Ministerio de Industria y Comercio de la República Checa envió a la Secretaría de UNIDROIT una propuesta para incluir dos temas principales en el Programa de Trabajo: tecnología *blockchain* y la herencia de propiedades digitales. Al recibir la Nota verbal de la Secretaría del 18 de junio de 2018 en la que se solicitaban propuestas para el Programa de trabajo 2020-2022, la República Checa presentó una segunda propuesta a UNIDROIT, reiterando las propuestas anteriores y expresando la necesidad de evaluar lo que sería una distribución justa de los derechos y obligaciones en contratos relacionados con productos y servicios inteligentes, es decir, los *smart contracts* y el IoT, y para redactar normas marco al efecto.

para los *smart contracts,* la tecnología *blockchain* y las plataformas de servicios, así como los *digital assets* o bienes digitales. Igualmente, la CNUDMI recibió una Nota, denominada *Legal aspects of smart contracts and artificial intelligence* (UNCITRAL, 2018, pp. 1-4), por parte del Gobierno de Chequia[26]. En ella, se abordaban los aspectos legales de los *smart contracts* y la inteligencia artificial o IA, y se examinaba la conveniencia de controlar su regulación. A raíz de esta propuesta, la CNUDMI acordó[27] recabar información respecto de las cuestiones jurídicas de la economía digital mediante reuniones de expertos. Sin embargo, Chequia aludió que el conocimiento de estas disposiciones parece limitado, y que las prácticas comerciales emergentes requieren de la reformulación de las disposiciones vigentes. Estas modificaciones fueron consideradas académicamente en el *Congress of the United Nations Commission on International Trade Law 2017* (UNCITRAL, 2017). La propuesta elaborada por el Gobierno de Chequia, que tanto UNIDROIT como la CNUDMI recibieron, ha cristalizado en el *Draft Triennial Work Programme 2020-2022* (UNIDROIT, 2019, pp. 19-20) del *Governing Council* de UNIDROIT. En él, se prevé un *Joint Workshop*[28] sobre los aspectos legales de los *smart contracts,* la inteligencia artificial y la *Distributed Ledger Technology*[29] o DLT (CIEPLAK, 2017, pp. 417-427), como tecnología de registro distribuido donde se encuentra circunscrita la tecnología *blockchain*[30]. Sus conclusiones serán consideradas en el próximo *Governing Council* de mayo de 2020, para elaborar la versión definitiva del *Triennal Work Programme 2020-2022,* lo que puede servir de base para una regulación a nivel europeo. Asimismo, a nivel global, la Organización Mundial del Comercio (GANNE, 2018, pp. 127-129) también ha destacado la oportunidad para el tráfico mercantil internacional de la aplicación de la tecnología *blockchain*, por su eficiencia y seguridad, así como la reducción del fraude en las transacciones, la mejora de la gestión de los derechos de propiedad intelectual, el perfeccionamiento de la rastreabilidad y el aumento de la confianza en las cadenas de valor. Finalmente, el secretario general de Naciones Unidas, Antonio Guterres, ha afirmado en el mes de diciembre (FORBES, 2019) que dicha organización debe acoger el uso de la tecnología *blockchain* para acelerar el alcance de los Objetivos de Desarrollo Sostenible.

Para concluir con estas reflexiones iniciales, debemos indicar que la ausencia de una ordenación específica de los *smart contracts* ocasiona disfunciones, que derivan de tener que traducir al lenguaje informático cláusulas contractuales, o lo que es lo mismo, aplicar en la práctica el *"From Law to Code"*. El Derecho no siempre puede condensarse en un código informático, porque su automaticidad impide atender determinados elementos: los que requieran de una valoración

---

[26] La República Checa presentó una propuesta a la Secretaría de la CNUDMI solicitando que controlase la prospectiva regulación de los contratos inteligentes y la inteligencia artificial, y que informase a la Comisión sobre las áreas que podrían requerir un tratamiento legal uniforme.

[27] El acuerdo está contenido en las actas del 51º periodo de sesiones (Nueva York, 25.6.2018-13.07.2018) (http://www.uncitral.org/uncitral/es/commission/sessions/51st.html).

[28] Joint Workshop on the legal issues arising from the use of Smart Contracts, Artificial Intelligence and Distributed Ledger Technology (https://www.unidroit.org/89-news-and-events/2609-uncitral-unidroit-workshop-on-smart-contracts-artificial-intelligence-and-distributed-ledger-technology?fbclid=IwAR2JmVfX8snY12AdNKUhiGjXKpmr5-e7JUvs4LVm8XkhYHIxqOUPju0e5RI).

[29] Es un protocolo informático que puede tener carácter público, para que cualquier usuario pueda añadir bloques o leer lo registrado, carácter privado, para que solamente accedan sus miembros, o cadenas semipúblicas. Esta base de datos única guarda todos los nodos, que registran todas las modificaciones realizadas.

[30] En relación con la tecnología *blockchain*, véase *infra* apartado 3. En OCARIZ (2018, pp. 90-155) puede encontrarse una explicación técnica de esta tecnología, formulada a modo de aproximación técnica en el presente trabajo. ARRUÑADA (2018, pp. 55-105). BÖHME (2015, pp. 213-238). Para un examen de esta tecnología desde un análisis económico, véanse ALI (2018, pp. 1676-1717) y ABADI (2019, pp. 1-53). Sobre este extremo, ECHEBARRÍA (2017, pp. 70-79) expone que la identificación de los contratos inteligentes con la tecnología *blockchain* ha generalizado su uso, y que esta tecnología permite programar pagos sin intervención humana.

subjetiva[31]; los que atiendan a sujetos o conceptos[32] tasados en la normativa o en la jurisprudencia; y los supuestos que originen responsabilidad civil (JOHNSON, 2017, pp. 73-78) o su exoneración por caso fortuito o fuerza mayor (WERBACH, 2017, p. 367), conforme al art. 1105 CC. Hasta la llegada de una regulación completa de esta materia, la igualdad material de las partes deberá encomendarse a una adecuada programación. Por ello, una regulación clara evitaría problemas en la aplicación de los *smart contracts*, por su novedad y por la ausencia –al menos teórica, como veremos– de una jurisdicción que reequilibre la asimetría negocial y mitigue los resultados inadecuados, derivados del automatismo del código informático. Estos retos pendientes de abordar se refieren principalmente a la personalización del contrato, los errores de programación y la responsabilidad civil, la protección y encriptación de datos de carácter personal, así como la invalidez e ineficacia en sentido estricto, y examinaremos sus desajustes a lo largo de los siguientes apartados.

2. La conceptuación de los *smart contracts*: acerca de su naturaleza jurídica

2.1. *Smart contracts in the books: aplicación acrítica del código informático a un contrato vs. ámbito material de aplicación*

Con el surgimiento del ciberespacio, en un primer momento se acuñó (LESSIG, 1999, pp. 5-20) la expresión *"Code is Law"*, en el sentido que la tecnología puede operar sin una normativa que ampare dicha actuación. Esta es la idea subyacente al término *smart contract* (SZABO, 1996), que fue acuñado como el código o protocolo informático que expresa el conjunto de cláusulas contractuales o pactos que suscriben las partes[33]. Estos pactos se incorporan en el *hardware* y el *software* para automatizar las prestaciones de las partes, o en su caso los remedios de adaptación o desvinculación. Este contrato opera prescindiendo de la confianza (RASKIN, 2017, pp. 1-37; WERBACH, 2017, pp. 313-382; MIK, 2017, pp. 269-300) y de cualquier exigencia económica, en particular, la solvencia. En su concepción inicial, estos contratos estaban configurados para funcionar al margen del Derecho, e incluso se planteó su sustitución mediante un sistema alternativo y su propia criptomoneda, el *Bitcoin*. Por todo, y conforme a este concepto[34], podemos distinguir (STARK, 2016) entre los *smart code contracts,* que son jurídicamente irrelevantes por tratarse de una mera secuencia de código informático, y los *smart legal contracts*, que sirven para el intercambio de prestaciones y a los que en adelante denominaremos *smart contracts,* por economía lingüística.

No obstante, como es bien sabido, las utopías no suelen prosperar cuando se implementan. En un plano teórico, que un contrato funcione sin Derecho puede resultar atractivo, porque reduce tiempo y costes, pero los abusos quedan sin tratamiento legal. Ello conduciría a especie de

---

[31] PUTERBAUGH (2017, pp. 24-26). LEGERÉN (2018, pp. 201-205) dedica una extensa explicación a la imposibilidad de que los contratos inteligentes sean *omnicomprensivos,* aunque deberemos atender a la evolución del IoT para identificar el alcance de esta restricción material.

[32] Como sujetos podemos encontrar el parámetro de consumidor medio, el consumidor experto, el consumidor vulnerable, así como estándares de conducta como la diligencia debida o comportamientos informados por conceptos jurídicos indeterminados o poco concisos, como la buena fe o el interés superior del menor.

[33] Detalla que un *smart contract* es "a set of promises, specified in digital form, including protocols within which the parties perform on these promises. The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher".

[34] Atiéndanse también VILALTA (2019, pp. 126-152) y TUR (2018, pp. 55-56).

"anarquía contractual", inadecuada a todas luces, especialmente para el reequilibrio de la asimetría negocial. La pretensión inicial de crear un contrato que opere al margen del Derecho se desvanece cuando se aplica en la práctica pues, aunque el *smart contract* permita ahorrar los costes de transacción, abarate la contratación y el coste de las vicisitudes contractuales, requiere del Derecho para aplicarlo al caso concreto y subsanar los resultados inadecuados derivados de la programación. Por tanto, debemos precisar su orientación inicial, advirtiendo que la tarea del programador únicamente consiste en codificar las prestaciones del contrato, conforme al Derecho vigente, para su automatización.

Deus ex machina es la expresión latina por la cual en el teatro griego y romano se introducía el intérprete de una deidad para resolver una situación. El Derecho no ofrece soluciones milagrosas, y los *smart contracts* o también llamados *contracts ex machina* (WERBACH, 2017, pp. 313-382) tampoco, aunque pueda parecerlo por la automatización. El código informático no atiende a la adecuación material de los resultados programados, esto es, solamente podrá operar correctamente cuando hablemos de defectos intrínsecos al contrato, es decir, los supuestos de invalidez. Sin una programación muy exhaustiva, es difícil que los resultados automatizados sean igual de adecuados cuando estamos ante supuestos de ineficacia en sentido estricto, porque los elementos extrínsecos al contrato escapan a su control, y para que el código funcione correctamente deben estar previstas todas las eventualidades. En definitiva, podemos convenir que prescindir del Derecho se convertiría, por absurdo, en un *"In Code we trust"* (WALCH, 2018, pp. 4-27; CHENWEI, 2004, pp. 585-610) o una confianza ciega en los *coders* o programadores, lo que supondría aceptar acríticamente la ejecución del código informático. Sobre la inoperancia de esta ejecución acrítica del código volveremos más adelante, en relación con los errores de programación[35], adelantando la conveniencia de aplicar las instituciones jurídicas que nos permitan enmendar sus disfunciones. Entre estos instrumentos encontramos las soluciones frente la invalidez o ineficacia contractual, es decir, todo aquello que afecta a la formación y ejecución del contrato, así como la capacidad, legitimación, interpretación y afectación a terceros. Por todo ello, podemos afirmar que no es posible prescindir[36] de la intervención humana aun cuando se haya "robotizado" el contrato, especialmente en los *Machine to Machine contracts*[37].

Respecto del ámbito material de aplicación de los *smart contracts,* actualmente tienen una especial relevancia en el entorno financiero (TAPSCOTT, 2016, p. 103). Presentan una importancia creciente en las *Fintech* o servicios financieros complementarios adscritos a determinados sitios web, las herramientas de operación y medios de pago a través de Internet, el cruce de datos personales mediante el *Big Data,* los medios digitales para la identificación de personas como la firma digital, los medios de pago electrónico, así como el dinero electrónico. En el ámbito financiero, deberá prestarse una especial atención, por los motivos aludidos anteriormente, a la combinación[38] de instrumentos no financieros en forma de contratos bancarios celebrados con

[35] Véase *infra* apartado 4.

[36] SALVADOR (2018, p. 3) sostiene con acierto que prescindir de la intervención humana es un invento viejo, por el ahorro de los costes de transacción, el abaratamiento de la contratación y las vicisitudes contractuales, pero que las cuestiones inherentes a la contratación permanecen. LEGERÉN (2018, pp. 200-205) dedica una extensa explicación a señalar las dos consecuencias que tiene el automatismo en los contratos inteligentes: la innecesaridad de intervención humana en su ejecución, un aspecto que ya hemos matizado respecto de la ineficacia en sentido estricto, así como que el potencial ámbito de aplicación de este tipo de contratos no es omnicomprensivo.

[37] Véase *infra* apartado 2.3.

[38] ARGELICH (2019, p. 21): "en el caso de la comercialización de un instrumento no financiero, por ejemplo, un préstamo hipotecario, combinado con un instrumento financiero, como los *swaps*, deberán aplicarse igualmente estos controles

consumidores, con instrumentos financieros destinados a inversores, que ya prevén para los *smart contracts* algunas entidades financieras[39]. Así, encontramos las denominadas *equity swaps*[40] y otros instrumentos financieros comercializados indebidamente con consumidores[41], préstamos con claves de acceso a fondos que tienen eficacia revocatoria por la falta de pago del deudor[42], e incluso su aplicación a letras de cambio[43]. Respecto del tráfico mercantil, los *smart contracts* tienen un papel destacado en las Organizaciones Autónomas Descentralizadas o DAOs, que se refieren a nuevas modalidades empresariales en las que la relación entre los diferentes entes participantes se rige por un *smart contract* complejo, programado con la tecnología *blockchain*. De esta manera, la toma de decisiones en la sociedad se encuentra tan formalizada que se puede ejecutar automáticamente y *on-chain,* por tanto, en forma de registro distribuido para que las partes implicadas no puedan modificarlo. Su naturaleza jurídica empresarial se encuentra cuestionada (EU BLOCKCHAIN OBSERVATORY AND FORUM, 2019) porque las DAOs operan en una *blockchain* no permisionada, de manera que su número y los protocolos de Gobernanza cambian continuamente, y los nodos maestros no se encuentran identificados; estas características afectan al alcance de la responsabilidad por errores en la programación de la *blockchain* y a los contratos que la integran. Asimismo, los *smart contracts* también tienen un rol destacado en el comercio internacional, y en el comercio de bienes de consumo vinculados al *Internet of Things*[44] o IoT.

Otras instituciones (LEGERÉN, 2018, p. 207) de Derecho civil también pueden instrumentarse mediante la tecnología *blockchain* y los *smart contracts*, aunque con cautelas para evitar los abusos por su desregulación[45]. En este sentido, encontramos los depósitos en garantía, la

---

porque se comercializan a consumidores y, sobretodo, porque la conducta del empresario es calificable de práctica comercial desleal. Este último es uno de los elementos que, de conformidad con la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores, puede utilizarse para apreciar la abusividad en las cláusulas del contrato relativas al coste del crédito concedido al consumidor".

[39] Véase en este sentido el estudio realizado el 29 de marzo de 2016 por *BNP Paribas* sobre la aplicación de los *smart contracts* (https://news.bitcoin.com/bnp-paribas-smart-contracts-legal-code/).

[40] Se trata de un instrumento financiero derivado *Over the Coulter* u OTC, es decir, no compensado, conforme al cual se intercambian los rendimientos de una cartera por unos tipos de interés, es decir, se constituye una opción de compra futura de un valor a un precio determinado pactado por las partes fuera del mercado. En este sentido, véase el test realizado en noviembre de 2017 por las entidades financieras *JP Morgan* y *Credit Suisse* mediante un *smart contract* para realizar una *equity swap*, que comprendía servicios postventa, como por ejemplo la adquisición de acciones corporativas o transferencias de pago (https://www.businessinsider.com/jpmorgan-citi-credit-suisse-test-distributed-ledger-technology-solution-2017-11?IR=T).

[41] En este sentido, encontramos también la deuda subordinada y las participaciones preferentes. ARGELICH (2019, p. 15): "en junio de 2018 se presentaron en el Parlamento Europeo cuatro informes titulados *Mis-selling of Financial Products,* en los que se analiza la *Marketing Sale and Distribution* o comercialización de productos financieros, la *Subordinated Debt and Self-placement* o comercialización de productos híbridos por cuenta propia, y los informes relativos al *Consumer Credit* o crédito al consumo y a *Mortgage Credit* o crédito hipotecario. Estos estudios constatan varios fraudes en la contratación con consumidores, entre los que destacan la comercialización indebida de participaciones preferentes y los abusos en los préstamos hipotecarios, especialmente en las cláusulas suelo y las cláusulas relativas a los gastos hipotecarios".

[42] LEGERÉN (2018, p. 206) explica que el software permitirá incluso la solicitud de garantías adicionales en caso de disminución del valor de la garantía. En este sentido, consideramos que va a necesitar una adaptación en el caso de la contratación con consumidores, para evitar abusos.

[43] En agosto de 2016, el *Bank of America*, *Merrill Lynch, HSBC* e *Infocomm Development Authority* de Singapur aplicaron la tecnología *blockchain* a esta transacción (https://www.ida.gov.sg/About-Us/Newsroom/Media-Releases/2016/BofAML-HSBC-IDA-Singapore-Build-Pioneering-Blockchain-Trade-Finance-App). Véase SCHINDLER (2017, pp. 1-16).

[44] ALI (2018, pp. 1676-1717) examina eventuales vinculaciones entre la tecnología *blockchain* y los *smart contracts* al IoT. Véanse también ALI (2018, pp. 584-591) y CHRISTIDIS (2016, pp. 2292-2303).

[45] En este sentido, advierte PUTERBAUGH (2017, p. 52) que el código informático no es Derecho, en el sentido de que su validez todavía no está clara, y que la concepción del *smart contract* puede obedecer a un mecanismo para forzar el cumplimiento del contrato en lugar de denominar a un contrato en sí mismo.

distribución y pago de derechos de autor, y el reparto de la herencia. En este último caso, plantea dudas la aplicación de la tecnología *blockchain* a la automatización de la aceptación de la herencia y el papel del Notario. En nuestra opinión, solamente cabría en el caso de la aceptación pura y simple. Al tratarse de un acto de carácter voluntario, creemos que es difícilmente automatizable la repudiación e incluso, por su carácter restringido, la aceptación a beneficio de inventario. Asimismo, también suscita dudas la automatización del pago de la legítima porque, aunque se trate de una parte del patrimonio hereditario de la que el testador no puede disponer, inciden en ella eventos externos que requieren de una apreciación con posterioridad al fallecimiento del causante, a saber: la inoficiosidad de las donaciones realizadas con anterioridad a la sucesión, *ex* art. 819 CC; y la existencia de una causa de desheredación, conforme a los arts. 852-855. En suma, la tecnología *blockchain* puede servir para agilizar los trámites derivados del fallecimiento, con la tecnificación del Registro Civil y del Registro de Actos de Última Voluntad, pero no puede automatizar todo aquello que concierne a la distribución del patrimonio hereditario. En otras palabras, por las limitaciones señaladas, consideramos que no es posible codificar completamente la aceptación de la herencia ni su reparto, que en abstracto únicamente cabría respecto del tercio de libre disposición, porque la aplicación parcial de esta tecnología provocaría desajustes materiales.

En cuanto al Derecho del trabajo, por tratarse de Derecho privado, debemos señalar que se ha admitido la automatización mediante la tecnología *blockchain* de determinadas prestaciones[46]. Sin embargo, advertimos que cada nuevo cambio en las condiciones de trabajo requerirá de una actualización de los *smart terms,* a modo de cláusulas inteligentes que automaticen cambios en determinadas prestaciones con la confirmación por las partes. Esta constante adaptación o renegociación, que contradice materialmente el automatismo del código informático, hace que, si bien el uso de la tecnología *blockchain* puede facilitar la ejecución de determinadas prestaciones, dificulta su calificación de *smart contract de trabajo,* por diversas razones: por una parte, existen eventualidades en la fase de ejecución del contrato, como la indemnización por despido o las infracciones laborales, que por su componente subjetivo no son susceptibles de programación; y, por otra parte, las prestaciones del contrato no pueden estar sometidas parcialmente a un *smart contract,* de la misma manera que ocurre en el ámbito sucesorio, máxime cuando entre estas se encuentran aquellas referidas a normativa imperativa. Por lo que se refiere al Derecho de la seguridad social, por tratarse de Derecho público, únicamente puede ser objeto de automatización el abono de determinadas prestaciones, mediante la tecnología *blockchain.* Finalmente, en el Derecho administrativo, pueden operar los *smart contracts* en los contratos privados que formalice la Administración, conforme al art. 26 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (BOE nº 272, de 9.11.2017). De acuerdo con la regulación vigente, no es posible hablar de *smart contracts públicos,* por la existencia de un procedimiento administrativo de carácter imperativo, aunque para los contratos públicos y para la agilización de determinados trámites administrativos resulte de utilidad la aplicación de la tecnología *blockchain.*

2.2. *Críticas al concepto de* smart contract *y reafirmación de su naturaleza contractual*

[46] Por ejemplo, los *smart contracts* puede servir a la actividad sindical y a la renegociación de las condiciones de trabajo, como la jornada laboral, los salarios o el contenido de las tareas, como indica WORLD ECONOMIC FORUM (2016). Sin embargo, debemos señalar que en nuestra opinión ello no debe tener una total traslación al contrato de trabajo ni a las prestaciones de la Seguridad Social, pues además en este último caso se trata de Derecho Público. ROJAS (2017).

Las numerosas críticas[47] al término *smart contract* se refieren a lo que calificamos de una interpretación literal y reduccionista, como justificaremos. Conforme a esta, se niega que sea un *contrato,* por tratarse de un código informático[48] cuyo cumplimiento no es legalmente exigible, y se rechaza su carácter *inteligente* porque no utiliza IA, pues el *smart contract* no actúa de forma autónoma como un robot, sino que tiene un cierto componente de adaptación al entorno, por la comprobación de eventos externos y, por tanto, de imprevisibilidad. Sin embargo, todo ello no es cierto por varias razones. Por una parte, el código informático autoejecuta las prestaciones de un contrato, *ergo* la programación es instrumental al contrato y no al revés, y buena prueba de ello es la configuración de la *self-help* frente al incumplimiento. Además, el propio Szabo justificó (SZABO, 1996) la denominación de *"smart",* porque son más funcionales o dinámicos que los contratos tradicionales, referidos como *"inanimate paper-based ancestors"*. Por otra parte, aunque debemos precisar que una *blockchain* no requiere de una IA para su correcto funcionamiento, la IA tiene influencia en su arquitectura (ALMASOUD, 2018, pp. 1-6) por la intervención en su configuración, mediante los denominados *miners* o mineros, los datos de la cadena de bloques, la red de observadores, así como la integridad de la plataforma.

Si bien es cierto que el *software* no puede, desde una concepción formalista, calificarse *per se* de contrato, lo cierto es que el término s*mart contract* es suficientemente conciso para expresar lo que pretende: un contrato inteligente es aquel que se perfecciona por el consentimiento, y las partes quedan vinculadas por el conocimiento de su existencia. La perfección (TUR, 2018, pp. 74-75) del contrato se produce en el momento en el que las partes expresan su consentimiento en el *front-end*, o la parte visible para el usuario de la plataforma de que se trate, para que el *back-end*[49] procese el consentimiento y el resto de datos proporcionados para iniciar la ejecución del *smart contract.* El consentimiento puede expresarse oralmente, por escrito, o por medios informáticos, como la firma digital (CHENG, 2018, pp. 1046-1051) y los acuerdos *clickwrap* y *browsewrap,* destinados principalmente a que los consumidores tengan la *actual notice* de los términos del contrato, y cuya validez se supedita a su obtención documental antes de la celebración del contrato[50]. El consentimiento electrónico que reúna los requisitos de validez producirá los mismos efectos que el prestado presencialmente, pues lo permite para la contratación

[47] Por todas, véase WERBACH (2017, pp. 338-350). En particular, MCJOHN (2016, pp. 2-23) manifiestan que ni es inteligente ni es un contrato porque en realidad "is robotic not smart" y "it is not legally enforceable", y expresan que las partes no pueden quedar insatisfechas porque las prestaciones se han pactado con anterioridad. En el mismo sentido, O'SHIELDS (2017, p. 178). Respecto del carácter contractual de los *smart contracts*, SAVELYEV (2017, p. 14) ha negado que sean fuente de obligaciones porque no depende de la voluntad del deudor sino del código informático, lo que supone la aplicación del principio *pacta sunt servanda* de manera absoluta, y niega la responsabilidad del deudor por el incumplimiento de su prestación.

[48] Conforme a la plataforma *Ethereum,* un *smart contract* es un programa, entendido como código informático, que se registra y opera en la propia plataforma.

[49] El término *back-end* se refiere a la parte del desarrollo web encargada de procesar los datos proporcionados por los usuarios en el *front-end* o la plataforma mediante la cual interactúan.

[50] Los *clickwrap agreements* van referidos a contratos en los que las condiciones y términos de un sitio web se aceptan expresamente antes de completar una transacción, a modo de mecanismo reputacional. Por otra parte, los *browsewrap agreements* son un acuerdo de licencia relativo a los términos y condiciones de uso de un sitio web que cubre el acceso a los datos de un sitio web o producto descargable. Para una explicación más detallada sobre estos conceptos y la *actual notice* que exigen los tribunales estadounidenses como prueba del consentimiento mutuo o *mutual assent,* véase entre otras la Sentencia United States Court of Appeals for the Ninth Circuit, 18.8.2014 (763, F3.d 1171; MP: Roslyn O. Silver). Respecto del *clickwrap* de aceptación de las condiciones generales que atribuyen competencia judicial, véase la STJUE, 20.5.2015 (TJCE 196; MP: C. Toader), pues solamente serán válidas si permiten imprimir y guardar su contenido antes de la celebración del contrato. O'SHIELDS (2017, p. 186).

electrónica el art. 23.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE nº 166, de 12.7.2002).

Por tanto, aunque el contenido, objeto y función del *smart contract* pueda ser cualquiera, es decir, sirva para transacciones que no encajen en el concepto jurídico de contrato, y a pesar de que materialmente es un programa creado para operar en una plataforma *blockchain*, debemos afirmar que en última instancia ejecuta prestaciones, lo que refuerza esta calificación. Para ello, la plataforma *blockchain* correspondiente deberá activar los mecanismos para la comprobación de la identidad, capacidad de obrar y los requisitos[51] de validez inherentes al contrato. Una vez perfeccionado, el Derecho de contratos aplicado a la ejecución de los *smart contracts* operará en dos estadios: en el primero, las partes cumplirán con las prestaciones pactadas voluntariamente y controlarán su ejecución y la de la contraparte; y, en el segundo, el código informático arbitrará la *self-help* o los remedios privados frente al incumplimiento contractual, sin perjuicio de su reclamación judicial. Por la naturaleza mayoritariamente disponible del Derecho civil, debe entenderse que las normas dispositivas operarán en defecto de pacto si se han codificado, y la ejecución del contrato responderá a los distintos eventos previstos por las partes, sin más coerción que el automatismo informático.

En suma, afirmar que la naturaleza jurídica del *smart contract* se corresponde con un contrato, permite aplicar su teoría general y remedios, aunque deban adaptarse por sus particularidades materiales, en especial cuando el objeto del contrato se encuentre conectado a la red mediante el *Internet of Things* (ASHTON, 2009) o IoT[52]. En este sentido, debemos recordar que el art. 1258 CC vincula a las partes a las consecuencias derivadas del contrato y a las que deriven de la buena fe, la costumbre y la ley. Por ello, todo *smart contract* deberá incorporar códigos informáticos que automaticen remedios como la moderación equitativa en caso de incumplimiento parcial, la cláusula *rebus sic stantibus* y la excesiva onerosidad del contrato, entre otros. Además, quienes operen en el tráfico jurídico con los *smart contracts* van a beneficiarse de sus ventajas materiales, fundamentalmente la rapidez y seguridad, y sus ventajas jurídicas porque, aunque inicialmente Szabo lo configuró (SZABO, 1996) como un mecanismo al margen de la jurisdicción, el Derecho y sus remedios van a estar presentes ante la imprevisión o imperfección del código informático. Es más, el Derecho no puede ser ajeno a las transacciones comerciales, con independencia del instrumento utilizado, porque eso llevaría a una desregulación que no se debe potenciar sino aislar. En última instancia, respecto de los contratos sin acuerdo previo con consumidores, provocaría un efecto parecido al del *shadow banking,* es decir, una actividad de financiación al margen del crédito bancario tradicional, operada por instituciones financieras no bancarias que no se encuentran sometidas a un ente regulador.

En definitiva, tener que reinterpretar la teoría general del contrato, los remedios del consumidor y la protección de datos, como los principales elementos que necesitan una revisión en sede de *smart contracts,* no le niega su naturaleza contractual. Su naturaleza contractual se afirma desde una interpretación finalista: nace el contrato por el acuerdo de las partes y les vincula desde su perfección, con independencia del medio utilizado para formalizarlo y ejecutarlo. Negar dicha naturaleza por razón del instrumento es interpretarla de manera superficial y sin atender a su trascendencia material, esto es, servir de instrumento para el intercambio de bienes y servicios; es como negar la existencia de un bosque por atender solamente a las copas de los árboles, en

[51] Véase *infra* apartado 5.1.

[52] Véase *infra* apartado 5.2.

este caso la terminología, desoyendo su ecosistema, es decir, su función. Es por tanto que debería preguntarse a quienes le han negado y le siguen negando esta naturaleza qué otra podría tener, qué remedios frente al incumplimiento deberían arbitrarse, distintos de los existentes por no corresponderse con un contrato, y qué contratos se considerarían inteligentes o cuáles no. Por el momento, más allá de las críticas al término, ampliamente extendidas a pesar de su reduccionismo, no hemos encontrado ninguna respuesta a estos interrogantes.

2.3. *Smart contracts in action y M2M contracts*

Los *smart contracts* sustituyen el tradicional clausulado del contrato por un código informático de tipo condicional, o de lógica *booleana.* Este código debe tener una estructura *if/then/else*, es decir, si se cumple una premisa o supuesto de hecho *"if",* se automatiza la consecuencia jurídica o una prestación *"then";* si no se cumple, se ejecuta una acción prevista como *"else",* a la que denominaremos jurídicamente remedio. De esta manera, y partiendo del concepto adaptado a la realidad contractual actual, podemos definir el *smart contract* como el código informático que contiene el conjunto de pactos o cláusulas contractuales, programado mediante un módulo, que está formado por un código virtual –como por ejemplo es el lenguaje *Solidity* (BHARGAVAN, 2016, pp. 91-96) que opera en *Ethereum*, aunque existen otros como *Serpent* y *LLL*– y que, una vez incorporado a la tecnología *blockchain* (ALHARBY, 2017, pp. 125-140) o cadena de bloques, forma una unidad autónoma que procesa la información, es decir, autoejecuta las prestaciones del contrato. Por tanto, es posible programar el concepto jurídico de condición del art. 1113 CC, con los límites del art. 1116 y por ende del art. 1255, sometiendo la eficacia o ineficacia futura a un evento externo al contrato, pero previsto en el código informático. En el trasfondo de esta programación, en realidad es donde está la clave de la tarea del programador: prever en el código informático las distintas eventualidades que puedan manifestarse en la fase de ejecución.

Como puede observarse, la eliminación del factor humano, salvo cuando sea necesario corregir el acuerdo que representa el código informático, suprime al menos dos defectos consustanciales: por una parte, el error humano, sin perjuicio de la correspondiente responsabilidad civil por una programación inadecuada; y, por otra parte, las conductas que persigan demorar la ejecución de un contrato, así como la *Verwirkung* o el retraso desleal en la reclamación judicial de un derecho subjetivo. Sin embargo, pensando fundamentalmente en contratos B2B de tracto sucesivo, como por ejemplo un contrato de suministro, dicho retraso incide materialmente en la ejecución del contrato. Para este supuesto, y especialmente en el tráfico mercantil internacional, debe permitirse la desvinculación del contrato, pues el automatismo del código no puede generar esta consecuencia por un retraso. Si es necesario, se puede optar por la aplicación de una cláusula de excepción –como contiene, por ejemplo, el art. 4.3 del Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (DOUE nº 177, de 4.7.2008)–, entendida como la regla legal que permite aplicar una norma más vinculada con el litigio que la designada por la norma de conflicto, para que pueda proceder la desvinculación contractual.

Todos los *smart contracts* presentan una serie de características[53] comunes: en primer lugar, se trata de un conjunto de pactos arbitrados mediante un código informático; en segundo lugar, su materialización se contiene en el *digital form* del contrato, como ya sucede en la contratación

[53] SAVELYEV (2017, pp. 3-24) indica que su naturaleza es electrónica, se implementan en el software, aumentan la certeza, el código es de tipo condicional, son autoejecutables y autosuficientes. CLACK (2017, pp. 1-15).

electrónica, y además la programación de su ejecución, que constituye su novedad; y, finalmente, los protocolos[54] informáticos que se incluyen en el *smart contract* automatizan las prestaciones. Del concepto y características de los *smart contracts*, destacamos que son contratos autoejecutables, por el código informático, autosuficientes, por no requerir de acción humana, y autoejecutables o *enforceables* mediante el código informático. Como observamos, la confianza en la contraparte[55] se coloca en un algoritmo que automatiza las consecuencias jurídicas del contrato. En un contrato autoejecutado, la confianza de las partes pierde relevancia a favor del cumplimiento de las prestaciones, pues su incumplimiento resulta antieconómico y sus consecuencias negativas son automáticas, porque la identidad (AL-BASSAM, 2017, pp. 1-6) de la contraparte queda registrada de forma externa. Por ejemplo, SCPKI es el sistema vinculado a la plataforma *Ethereum* para comprobar la identidad, y se compone del nombre, la identificación, el código informático, el *hash* y el sistema de encriptación. Ello permite que la exigencia de la confianza, sobretodo basada en la solvencia, se desvanezca, pues el riesgo desaparece porque el *smart contract* registra el incumplimiento y automatiza sus consecuencias. Esta identificación presenta ventajas sobre todo en la contratación electrónica con grandes plataformas, tan extendida en la actualidad, y en la contratación entre ausentes. Además, para los incumplimientos previstos por el *smart contract,* ni siquiera es necesario acudir a la jurisdicción, que quedará reservada para aquellos casos que presenten una complejidad que supere al código informático.

Respecto del cumplimiento de lo pactado, este se comprueba mediante un ordenador que verifica los eventos externos para automatizar las prestaciones del contrato, y prescindiendo de una autoridad central[56] o un mecanismo de ejecución externo. Ante la producción de un determinado evento o el vencimiento del plazo para el cumplimiento de una obligación, el protocolo automatiza la ejecución contractual, programada con un código informático que arbitra el cumplimiento. La principal manifestación de esta autoejecución del contrato son las consecuencias frente al impago: la imposibilidad de utilizar el objeto del contrato. Sin embargo, esta automatización contractual requerirá de un examen más profundo cuando el objeto del contrato recaiga sobre un bien que afecte a las necesidades básicas o a la seguridad[57] del deudor. En última instancia, una adecuada programación permite prescindir de la jurisdicción, salvo para los casos de imposibilidad sobrevenida, en las prestaciones específicas, y los casos en los que proceda la aplicación de la cláusula –implícita– *rebus sic stantibus* y sus expresiones[58], contenidas en la regulación de diversos Estados europeos y los Principios UNIDROIT.

---

[54] Se refiere a un programa o conjunto de instrucciones, conforme a las cuales los cambios de estado en la información que contiene se registra en una base de datos digital, lo que vincula estos protocolos con la efectividad práctica del contenido contractual.

[55] SAVELYEV (2017, p. 8) explica que, en contraste con la contratación tradicional, la confianza en los *smart contracts* "is put in the computer algorithm standing behind the agreement", lo que califica de "trustless trust" o confianza sin confianza.

[56] En su configuración tradicional, se prescindió de una autoridad central, e incluso como el propio SZABO afirmaba sobre la jurisdicción, aunque esta última afirmación tiene los matices expresados en el artículo. Véanse SZABO (1996) y HYMAN (2017, pp. 13-17). Atiéndase también respecto del Proyecto de Ley de reforma de la *Nevada's Uniform Electronic Transactions Act,* en el Estado americano de Nevada, mediante la *Senate Bill no. 195* (https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6337/Text). Esta propuesta ha proyectado la regulación del uso de la tecnología *blockchain* y la exigibilidad de los *smart contracts*.

[57] Véase *infra* apartado 5.2.

[58] Estas se refieren a: la teoría italiana de la *eccessiva onerosità* o excesiva onerosidad del contrato, conforme a la regla de la *eccessiva onerosità* del art. 1467 del Código Civil italiano de 1942, que ha sido incorporada en el art. 6.2 de los Principios UNIDROIT y que implica la posterior renegociación del contrato; la teoría francesa de la *imprévision* o imprevisión; y, finalmente, la teoría alemana (LARENZ, 1963, pp. 10-201) *Geschäftsgrundlage* o de la base del negocio, dispuesta en el §

Una vez explicado el concepto de *smart contract,* debemos señalar que también comprenden los denominados *Machine to Machine contracts*, en adelante *M2M contracts*: la perfección y ejecución automática de un nuevo contrato derivado de la ejecución, también automática, de las cláusulas establecidas en un *smart contract* originario. O lo que es lo mismo, de un *smart contract,* personalizado o fruto de la adhesión, surge automáticamente un *M2M contract*. Ello puede plantear dificultades especialmente en el ámbito del Derecho del consumo, pues un consumidor puede adherirse a un contrato que le sea beneficioso, pero el acreedor debe prestar correctamente el deber de información precontractual para evitar que la conclusión automática de un *M2M contract* le sea perjudicial, especialmente por la combinación de instrumentos financieros y no financieros. Existen voces[59] que consideran que en realidad el *smart contract* primigenio se trata de un *precontrato,* sometido a la condición de que el contrato definitivo cumpla determinadas exigencias, e incluso lo han calificado de *precontrato imperfecto* –para conseguir su encaje–, respecto del que las partes se obligan a negociar las prestaciones y concluir el contrato proyectado. El precontrato, por su naturaleza, debe estar sometido a un plazo de caducidad, como término esencial para concluir el segundo contrato; en ausencia de este, se establecerá por los Tribunales, conforme al art. 1128 CC. Este término esencial, pensado para evitar la vinculación indefinida, impide que pueda calificarse al *smart contract* originario como precontrato, por una razón: el término esencial no encaja en la ejecución automática del *M2M contract,* que depende de la producción de un evento externo, elemento que resulta totalmente incompatible con la fijación de un término inicial para el cómputo del plazo de caducidad requerido.

Por el contrario, consideramos que este impedimento no se produce si el *smart contract* y el *M2M contract* se configuran como dos contratos autónomos, pero con relación de dependencia; no deja de ser una obligación principal y otra accesoria. Por ello, en este caso las partes perfeccionan un *smart contract* como obligación principal, y el código informático obtiene de ese consentimiento[60] la base para la perfección automática de un *M2M contract* accesorio. Esta calificación que se propone soluciona, además, el problema que presenta el precontrato respecto del consentimiento como base de un negocio posterior: las partes no tienen como finalidad en el *smart contract* originario asegurar la celebración de un *M2M contract*, y su intervención en este contrato es mediata. La finalidad del *smart contract* no es la conclusión del *M2M contract,* mientras que este último contrato podría existir o lo contrario, pero en ningún caso puede subsistir y tener sentido sin el *smart contract* originario, que sirve de fundamento al consentimiento mediato, pues no puede extraerse[61] un nuevo consentimiento de un código

313 BGB, para el caso de desaparición de la base subjetiva u objetiva del contrato, y que fue elaborada partiendo de la teoría de la presuposición o *Voraussetzung* de Windshceid. Al respecto y en profundidad, atiéndanse PARRA (2015, pp. 1-54) y SALVADOR (2009, pp. 1-60). La excesiva onerosidad del contrato, aunque carezca de una regulación sustantiva, encuentra su fundamento en el art. 7 CC, donde se contienen los límites al ejercicio de los derechos subjetivos: el abuso de derecho y la buena fe. La Propuesta de Modernización del Código Civil pretende incluir como límite la excesiva onerosidad del contrato en el art. 1192.2.2, como ya se contiene en el art. 7.2.2 de los Principios UNIDROIT, en el art. 9:102 (2) PECL y en el art. III.-3:302 (3) DCFR. Para la apreciación de la excesiva onerosidad del contrato, se exige que la parte perjudicada no haya asumido este riesgo, del mismo modo que se requiere para la procedencia de la cláusula *rebus sic stantibus*. El fundamento de la excesiva onerosidad atiende a que el riesgo del contrato recae exclusivamente en el deudor por falta de información, un riesgo que en lo que se refiere al precio y su reembolso puede comprometer su capacidad económica para hacer frente al pago de la deuda.

[59] LEGERÉN (2018, pp. 216, 222-224) quien, después de una larga argumentación y profusa doctrina académica y jurisprudencial, concluye que se trata de un "precontrato imperfecto", porque "se dejan abiertos los términos del precontrato". Sobre el precontrato imperfecto, véase GONZÁLEZ (2013, pp. 822-823).

[60] Véase *infra* apartado 5.2.

[61] Véase *infra* apartado 5.1.

informático. En otras palabras y respecto del consentimiento, sin este no acaece el contrato accesorio. Un ejemplo práctico de lo expuesto sería un instrumento financiero, como un *swap,* aparejado a un préstamo hipotecario como instrumento no financiero y obligación principal, en cuyo caso tienen una relación de dependencia como obligación principal y accesoria.

3. Tecnología *blockchain:* la adhesión contractual mediante *Blockchain* y la personalización con *Ethereum*

Una vez expuesta la naturaleza jurídica de los *smart contracts* y los *M2M contracts*, debemos referirnos a la tecnología *blockchain* que los hace posible. En una primera aproximación que desarrollaremos en los siguientes subapartados, la tecnología *blockchain* consiste en un código en cadena que emite registros descentralizados para subvenir a las dificultades que planteaban los contratos electrónicos (BELLAMY, 2016, pp. 6-12; LUU, 2016, pp. 254-269), relativos a la manipulación del contenido y la prueba de su emisión y recepción. Sus principios (TAPSCOTT, 2016, pp. 56-92) se basan en determinados parámetros: integridad en red, poder distribuido, valor como incentivo, seguridad, privacidad (CHATZOPOULOS, 2018, pp. 442-450), derechos preservados e inclusión. La tecnología *blockchain* está basada en una red P2P en la que los nodos, como terceros ajenos que comprueban la veracidad de los eventos, son iguales entre sí, aunque cumplen distintas funciones según se trate de nodos mineros, nodos simples o nodos maestros[62]. Ello permite articular un registro distribuido que los hace menos vulnerables a ataques informáticos, por existir otros nodos que suplirían su actividad.

Este mecanismo opera a través de tres elementos (ABADI, 2019, pp. 2-6) relacionados entre sí: la exactitud se vincula con la eficiencia de costes, mediante un libro mayor centralizado, y a su vez la exactitud se vincula con la descentralización por el *PoW-blockchain* o su prueba de trabajo, aunque existen otros protocolos de consenso que lo posibilitan sin coste energético, como la prueba de participación. La tecnología *blockchain* se relaciona con su entorno mediante los *Oracles* u oráculos, que es una red de observadores externos que comprueban los eventos producidos durante la ejecución del contrato, responden a las instrucciones de las partes en el sistema o a eventos externos cuya existencia queda registrada, y producen automáticamente las consecuencias jurídicas programadas. Por otra parte, debemos señalar que existen otras plataformas como *Logalty,* que emite registros de tipo centralizado, aunque por ello menos seguros y vulnerables a ataques informáticos, pues carecen de esta red de observadores imparciales.

Las principales[63] plataformas de tecnología *blockchain* son *Blockchain* y *Ethereum,* aunque existen otras como Quorum. *Blockchain*[64]*,* utilizada por más de 38 millones de usuarios, permite adherirse a un *smart contract* predispuesto y comprar criptomonedas, la propia de la plataforma que es *Bitcoin*, así como *Ether* y *Stellar*. *Ethereum*[65]*,* utilizada por 12 millones de usuarios, es una *blockchain* programable por la que se pueden crear *smart contracts* personalizados y comprar la

[62] Los nodos mineros emiten y propagan transacciones, ponen en funcionamiento el software necesario como BTCMiner o CGMiner y crean una copia disponible para los mineros en la *blockchain*. Por su parte, los nodos *broadcast* o simples solamente emiten transacciones y reciben información de la *blockchain*. Finalmente, los nodos maestros o completos permiten la descarga de una copia de la *blockchain* para pasar a ser un nodo más de la *blockchain*.

[63] Existen otras plataformas como Chainspace. Véase AL-BASSAM (2018, pp. 1-16).

[64] *Blockchain* (https://www.blockchain.com/).

[65] *Ethereum* (https://www.ethereum.org/).

criptomoneda de la plataforma, que es *Ether*. Mediante esta plataforma, en lugar de operar con un *smart contract* predispuesto, se incorporan los datos a la plataforma en forma de *input,* que genera nuevas transacciones u *outputs*. Por tanto, a este *smart contract* lo podemos calificar de "personalizado", por su configuración mediante *Ethereum*, en contraposición a la adhesión contractual que posibilita *Blockchain*.

Ethereum, sin embargo, tiene un coste económico: los usuarios deben pagar unas *fees* o tasas en *Ethers* por cada operación que activan. Ello permite evitar actuaciones maliciosas y sostener el coste de mantenimiento de la plataforma, denominado *gas*[66]*,* que es el coste de la computación sobre esta *blockchain.* Este coste se determina libremente por los mineros, conforme a las reglas del libre mercado, y quien ejecuta una transacción puede delimitar la cantidad máxima de *gas* que está dispuesto a gastar. Por el momento, este coste está desincentivando su extensión, a diferencia de la expansión que está experimentando *Blockchain*, así como por la inversión[67] que las partes necesitan realizar para la adquisición de equipos informáticos y la formación para operar en la plataforma *Ethereum*. Sin embargo, esta inversión tendrá sus externalidades positivas cuando los contratos tradicionales incorporen progresivamente (PUTERBAUGH, 2017, pp. 24-26) algunas cláusulas que se autoejecuten, para pasar a un segundo estadio de programas ayudados de IA que elaboren por sí mismos *smart contracts*. Por el contrario, la plataforma *Blockchain* permite la obtención de criptomonedas, convertibles a saldo canjeable en *PayPal,* por la fidelización de nuevos usuarios y contactos de usuarios ya registrados; no obstante, el coste material de la gratuidad es la cesión de datos de carácter personal.

De acuerdo con las plataformas de tecnología *blockchain* y sus posibilidades, podríamos distinguir entre dos clases de *smart contract*. Por una parte, aquel en el que existe un acuerdo previo y que, por tanto, su contenido se pacta o personaliza, mediante la plataforma *Ethereum.* Por otra parte, aquel en el que no existe un acuerdo previo y que, al no estar personalizado, es suficiente con el uso de la plataforma *Blockchain* para comprobar los requisitos de validez y adherirse. En el primer caso, por la existencia del acuerdo *off-chain,* la tecnología *blockchain* se utiliza para garantizar la eficacia del pacto, donde se habrán previsto las prestaciones y la activación y desactivación del código informático. En el segundo caso, por la ausencia de un acuerdo previo, el acreedor predispone el contenido contractual, el deudor solicita la adhesión, y la plataforma *Blockchain* comprueba los requisitos de validez y la identidad del deudor para activar el código informático.

3.1. *El adprosumer o consumidor 2.0 y los smart contracts*

El Derecho del consumo se encuentra en una encrucijada la que debe dar respuesta a nuevas realidades surgidas de la era digital, que son fruto directo de la evolución que ha experimentado el comercio electrónico: los *smart contracts* y los *adprosumers* o consumidores 2.0, como protagonistas de esta revolución contractual. Los *adprosumers* no se limitan a adquirir un bien o servicio, sino que requieren una experiencia positiva de compra. Esta se concreta, en primer lugar, en reclamar información y transparencia, elemento que deriva de los controles de incorporación, contenido y transparencia que le asisten como consumidor. Asimismo, el consumidor 2.0 busca asesoramiento, atención personalizada y una determinada relación

[66] OCARIZ (2018, pp. 111-112) concreta que este concepto alude al término "gasolina", porque pone en funcionamiento el *smart contract* de que se trate.

[67] PUTERBAUGH (2017, pp. 24-26) señala claramente que este desincentivo obedece a que las empresas todavía operan en contratos escritos o *paper-based.*

calidad-precio. Este último elemento, sin embargo, queda excluido del control de abusividad, pues solamente admite un control indirecto mediante un test circunstancial, relativo a la equivalencia de las prestaciones.

El *adprosumer* genera contenidos a través de las redes sociales, interactúa con una marca, y anuncia su experiencia con la finalidad de informar a otros consumidores. Ello permite conseguir el *customer engagement* o la adhesión del consumidor a una determinada firma, mediante la evaluación de las relaciones comerciales entre una empresa y un consumidor a largo plazo. En suma, tiene un papel de imagen de una marca y de su promoción, porque dirige indirectamente las acciones de marketing y publicidad, especialmente ante opiniones negativas, y crea una comunidad de seguidores en torno a un producto y su experiencia particular. El *adprosumer* sería el usuario que genera el contenido, sus seguidores quienes lo comentan, y los usuarios silenciosos quienes lo siguen, en un esquema que se correspondería respectivamente con 1-9-99, es decir, un usuario genera nueve seguidores, y estos a su vez noventa y nueve usuarios silenciosos.

Este consumidor 2.0, como destinatario principal de los *smart contracts,* se inserta en una protección del consumidor organizada en torno al concepto de *average consumer* o consumidor medio (HUALDE, 2016, pp. 12-31), como estándar que adopta la Directiva 2005/29/CE, de 11 de mayo, del Parlamento Europeo y del Consejo relativa a las prácticas comerciales desleales de las sociedades en sus relaciones con los consumidores en el mercado interior (DOUE nº 149, de 11.6.2005). Este concepto fue creado por la jurisprudencia[68] del Tribunal de Justicia para identificar al consumidor normalmente informado y razonablemente atento y perspicaz (WILHELMSSON, 2004, pp. 317-337). En un sentido contrario a la jurisprudencia del Tribunal de Justicia, nuestro Tribunal Supremo efectúa otra distinción: por un lado, el consumidor medio, conforme a los estándares expuestos; y, por otro lado, el consumidor experto, quien se ve privado de su protección en atención a sus conocimientos financieros, a pesar de la asimetría negocial. La supresión de esta distinción, que no se encuentra armonizada a nivel europeo, permitiría proteger a los consumidores de *smart contracts,* por centrarse en el desequilibrio contractual.

A modo de reflexión prospectiva, los retos que plantean los *smart contracts* en relación con los *adprosumers* afectan principalmente a la protección de datos de carácter personal, referidos al control de identidad y los ficheros de solvencia, así como a los controles de abusividad que les asisten como consumidores. Estos controles deben revisarse porque únicamente podrá subsistir en su configuración tradicional el control de incorporación, relativo a las Condiciones Generales de la Contratación, por tratarse de un control formal y, por tanto, programable. Su cumplimiento podría comprobarse en dos estadios: en primer lugar, mediante la incorporación de las Condiciones Generales de la Contratación; y, en segundo lugar, durante su formación, a través la tecnología *blockchain*, por el cruce automático de información entre distintas instituciones para comprobar si las Condiciones Generales han sido incorporadas al contrato de una forma transparente.

[68] En particular, véase la STJCE, 16.7.1998 (TJCE 174; MP: Jean-Pierre Puissochet), que condensa la jurisprudencia anterior y acuña el concepto de *average consumer* o consumidor medio, así como la STJCE, 13.1.2000 (TJCE 4; MP: José Carlos de Carvalho Moitinho de Almeida), que introduce el concepto de la proporcionalidad en la consideración de la expectativa que se presume en un consumidor medio.

Todo este panorama permite indicar que en un futuro los operadores jurídicos (FRIES, 2018, pp. 86-90) deberán especializarse en este ámbito para poder ofrecer *smart contracts* personalizados, sin depender de servicios externos. En este sentido, en el XII Congreso Nacional (CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA, 2019) se presentó el Informe "Abogacía Futura 2020: áreas de negocio emergentes". En este informe se detallan como profesiones jurídicas del futuro la de programador de *smart contracts*, asesor de criptomonedas, o experto en derechos de autor de objetos impresos en 3D. Por lo que aquí interesa, el Informe revela que los abogados deberán elaborar modelos de *smart contracts*, y los colegios profesionales tendrán que ofrecer como servicio la certificación de *smart contracts* ajustados a Derecho, otorgando "sellos de calidad". Sin embargo, el Informe no considera las consecuencias de una eventual responsabilidad patrimonial de la Administración por una certificación inadecuada, especialmente cuando el destinatario final sea un consumidor y el contrato contenga cláusulas abusivas o no supere el control de transparencia. Finalmente, y de conformidad con la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional (BOE nº 103, de 30.4.2019), resultará clave la figura del *ciberabogado*, aunque la propia norma no lo describa así, pues se refiere en el Objetivo II a la importancia de formar a los profesionales del Derecho para que sean expertos en ciberseguridad.

3.2. *La plataforma Blockchain y el papel del registro distribuido en la adhesión contractual*

La plataforma *Blockchain* y la irrupción de su criptomoneda *Bitcoin,* tras otros intentos fallidos[69] y a la espera del lanzamiento en 2020 de la criptomoneda *Libra*[70]*,* perteneciente a *Facebook*, han supuesto un revulsivo (TAPSCOTT, 2016, p. 102; O'SHIELDS, 2017, p. 179; OCARIZ, 2018, pp. 135-158) para los *smart contracts.* Respecto de *Bitcoin,* el Tribunal Supremo[71] se pronunció por primera vez en un supuesto de estafa el 20 de junio de 2019. Estableció que se trata de "un activo patrimonial inmaterial, en forma de unidad de cuenta", usado como "activo de contraprestación o de intercambio en cualquier transacción", pero que "en modo alguno es dinero, o puede tener tal consideración legal". Por otra parte, el surgimiento de *Libra* provocó que el Senado[72] de los Estados Unidos requiriese información sobre la denominada originalmente *Facebook Coin,* el 9 de mayo de 2019. El Senado identificaba como principales problemas que debía aclarar la plataforma la garantía de la privacidad, la protección e información financiera al consumidor, y el uso de la información proporcionada por el consumidor, en particular sus datos personales, lo que alude a los problemas[73] que presentan las criptomonedas en general.

---

[69] Entre ellos debemos mencionar *DigiCash*, *B-money* y *BitGold*. Esta última era la criptomoneda más tecnificada, pues se basaba en un sistema descentralizado a modo de clave público-privada para firmas digitales mediante una prueba de trabajo o *hashcash*. Sin embargo, no triunfó porque requería un quorum para las direcciones de red, lo que lo hacía vulnerable a los ataques informáticos. Para más detalle, véase OCARIZ (2018, pp. 57-58).

[70] *Libra* (https://libra.org/en-US/).

[71] STS, 2ª, 20.6.2019 (CL 28079120012019100389; MP: Pablo Llarena Conde).

[72] La carta del Senado pide al fundador de *Facebook* que aclare los siguientes extremos: el funcionamiento del sistema de pago; la privacidad y la protección que se otorgará al consumidor; la información financiera que se tenga de los consumidores; los usos que se van a dar, en su caso, a esa información financiera; si *Facebook* pretende compartir o vender esa información o aquella que derive de los usos que realice el consumidor; la información que *Facebook* pueda tener relativa a la solvencia, capacidad crediticia, reputación, características personales o modos de vida sobre los usuarios; y las garantías que ofrezca *Facebook* para la protección de esa información. Puede consultarse la carta del Senado a Mark ZUCKERBERG en este enlace: (https://www.banking.senate.gov/imo/media/doc/5.9.19%20Facebook%20Letter.pdf).

[73] Véase *supra* apartado 1.

Una vez contextualizada la irrupción de *Blockchain,* debemos atender a los elementos que han favorecido su extensión. La plataforma *Blockchain* permite emitir un código en cadena, es decir, un registro inmodificable, que procede de una fuente fiable y segura, y arbitra lo programado por las partes. La ventaja de esta tecnología es que un conjunto de terceros ajenos al contrato, denominados *nodos*, actúan en la plataforma P2P como fedatarios de las actuaciones de los intervinientes. Una vez que la red ha validado una conducta, le atribuye un *hash,* un código incorporado al registro que lo hace inalterable. Este código, como representación del contrato, queda incorporado en un registro distribuido. Desde ese momento, se esperan los datos que integran las variables establecidas, es decir, aquellas vicisitudes que afectan a la fase de ejecución del contrato, que proceden de unas fuentes fiables u *oráculos.* Cuando estas fuentes coinciden con el evento esperado y previsto por las partes en el contrato, generan el resultado previsto, dejando una constancia irreversible y permanente en el registro. Un ejemplo sería la recepción de la mercancía objeto del contrato, en este caso como tradición real o modo que aparejado al título transmite la propiedad (ARRUÑADA, 2018, pp. 55-105). Su ejecución se correspondería con el oráculo de geolocalización de la mercancía y su recepción, mediante un sistema de firma digital del destinatario para comprobar su identidad, generaría la orden de pago, para cuya facilitación es recomendable la conexión del objeto[74] del contrato con el IoT a la red. Asimismo, *Blockchain* proporciona la posibilidad de convertir el objeto de determinadas transacciones al método de pago *PayPal* y, por tanto, lo hace apto para el tráfico comercial en un entorno digital, por lo que resulta especialmente útil en la contratación con consumidores.

La utilización de registros de tipo descentralizado o distribuido como *Blockchain* permite que el *smart contract* esté programado en forma de código autoejecutable, incorporado a un registro que reside en miles de ordenadores, y que tiene carácter inmodificable, irreversible, inmune a manipulaciones o alteraciones y, por tanto, transparente. Ello dota a estos contratos de una seguridad y autenticidad (BELLAMY, 2016, pp. 6-12) que no puede proporcionar la contratación tradicional, aunque también resultan inflexibles[75] y poco adaptables a nuevos eventos sin una programación adecuada, por lo que incluso se les ha calificado de *dumb* (CAWREY, 2016), en el sentido que no atienden a elementos extrínsecos. Asimismo, también proporcionan una mayor eficiencia y agilidad por su objetividad y automatismo, pues no hay margen a la ambigüedad y no se requiere de acciones que materialmente puedan demorar la fase de ejecución del contrato.

Sin embargo, la implementación generalizada de *Blockchain* requeriría de una modificación en la admisión de las pruebas documentales, porque los certificados no presentan problemas de admisibilidad y esta plataforma no puede emitirlos por su naturaleza descentralizada. Para subvenir a este problema, debemos plantear dos alternativas para aportar un *smart contract* a un proceso judicial: por una parte, mediante el uso de la plataforma *Logalty,* que emite registros de tipo centralizado que sirven como prueba documental conforme al art. 265 LEC, pues son relativos al fondo del asunto; o, por otra parte, optar por la transformación de la codificación informática al lenguaje escrito. De acuerdo con lo establecido en sede de presentación de documentos públicos en el art. 267 LEC, puede aportarse mediante escritura pública e incluso soporte electrónico, como permite el art. 24 de la Ley 34/2002, para que sirva como prueba documental según lo contenido en el art. 265 LEC. Esta conversión (DWIVEDI, 2018, pp. 1-4) del lenguaje informático al ordinario, para el caso de que el contenido contractual no se haya

[74] Véase *infra* apartado 5.2.

[75] Sin embargo, ello puede ser percibido por las partes como una limitación, por tratarse de contratos demasiado rígidos y con poca adaptación a nuevas circunstancias. En este sentido, se expresa SKALAROFF (2017, pp. 263-303).

personalizado, está contenido en las Condiciones Generales de la Contratación o en el propio contrato de adhesión, mediante la aceptación de los términos y condiciones a través del *"I agree button"*, lo que constituye la autorregulación de la plataforma en forma de mecanismo reputacional.

3.3. *La plataforma Ethereum o la blockchain de los smart contracts personalizados: un "Smart Contract Inventor"* y *la iconificación de las prestaciones*

Una vez precisado el funcionamiento de la tecnología *blockchain* y la principal plataforma que permite la adhesión contractual, es momento de prestar una especial atención a *Ethereum*. Esta plataforma es una *blockchain* programable, mediante la *Ethereum Virtual Machine*[76] o EVM, y posibilita la creación de *smart contracts* personalizados. Este contrato se ejecuta mediante un código completamente aislado, porque no tiene acceso a la red, al sistema de archivos, ni a otros procesos, e incluso tiene acceso limitado a otros *smart contracts*. En la actualidad, y por la garantía de su privacidad, constituye la plataforma mayoritaria[77] para el desarrollo y creación de *smart contracts*. *Ethereum* permite la creación de un *smart contract* desde el inicio, lógicamente con nociones de programación, por lo que, si se extiende su uso al público en general, deberá simplificarse el mecanismo. En cuanto a su configuración, *Ethereum* opera mediante una *account*[78] o cuenta con un seguimiento del estado, sus transacciones y las trasferencias de valor o información entre cuentas. En contraste, *Blockchain* se configura como una lista de transacciones, de modo que el beneficiario de una transferencia anterior remite todo o parte de lo que ha recibido a otra dirección. Algunos ejemplos de la aplicación de *Ethereum* serían la formalización de un contrato de sociedad multiparte, y los contratos aleatorios como el de apuesta, en el que las partes remiten criptomonedas a una cuenta que las libera a favor del ganador.

En este sentido, debemos señalar una experiencia que puede trasladarse a los *smart contracts* personalizados para extender su uso: *App Inventor*[79], una aplicación de desarrollo de *software* creada por *Google Labs* y desarrollada por el *MIT Media Lab* y el Instituto Tecnológico de Massachusetts. Esta plataforma sirve para la elaboración de aplicaciones destinadas al sistema operativo Android[80]. Existen dos perspectivas para poder crear la aplicación de que se trate: la pantalla *designer,* consistente en el diseño visual que va a tener la aplicación, y la pantalla *blocks,* correspondiente a la programación que contiene la pantalla *designer*. Un icono, en realidad, consiste en una imagen que se incrusta en la pantalla *designer,* que contiene la programación y

[76] Para una explicación más detallada, atiéndase la guía que *Solidity*, por tratarse del código mediante el que opera *Ethereum*, ha elaborado al respecto (https://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html#index-6).

[77] Como hemos mencionado al inicio de estas líneas, *Ethereum* tiene más de 12 millones de usuarios registrados.

[78] En el caso de *Ethereum*, las cuentas pueden ser de dos clases: las *Externally Owned Accounts* o EOA, que se controlan mediante claves privadas por seres humanos; y las *Contract Accounts*, cuyo mecanismo de funcionamiento es su código interno y su control se efectúa por el código de contrato, que solamente se activa mediante una EOA. En consecuencia, el *smart contract* configurado desde *Ethereum* es un código incorporado a una cuenta de contrato, que ha sido programada para ser controlada por una EOA, y que tiene una clave privada para restringir su acceso a quien no disponga de esa clave. Este *smart contract* se ejecutará cuando se active una operación desde una EOA y se envíe una transacción a esta cuenta.

[79] *App Inventor* (http://appinventor.mit.edu/explore/index-2.html).

[80] El usuario, que no requiere de conocimientos de programación, puede enlazar una cadena de bloques para crear la aplicación mediante unas herramientas básicas, pues además la plataforma ofrece una guía de inicio, tutoriales y un foro de usuarios. Para que un destinatario final pueda descargarse la aplicación creada, debe generarse un archivo en formato *".apk",* y en la medida de lo posible que dicha aplicación acceda a las plataformas de distribución digital para dispositivos móviles, con la finalidad de generalizar su uso.

cuya pulsación la activa. En una misma aplicación, cada función se automatiza en pantallas superpuestas, lo que el usuario medio identifica como iconos sobre los que clicar. Mediante los bloques *"set"* y *"get"* se pueden atribuir unos determinados valores que, automatizados por la pulsación del usuario, emiten una orden. Los distintos eventos van incluidos en cada bloque, y se articulan de una manera visual a modo de "puzle", por tanto, resulta más fácil de utilizar que el lenguaje de programación, aunque con una formación inicial a nivel de usuario, pues sin ella no es suficiente. Asimismo, también pueden programarse en lenguaje condicional *if/then* y añadir tantos *else* como sea necesario, porque pueden ampliarse las entradas de cada "puzle" para que encajen los distintos remedios. Para una adaptación de los *smart contracts* al usuario medio, lo que extendería su uso como ha sucedido con las criptomonedas, debería articularse un sistema a modo de *"Smart Contract Inventor"*. Ello posibilitaría su creación sin necesidad de ser un programador, pues la informática es accesoria al Derecho, como la garantía del correcto desarrollo del código informático. Actualmente, las guías de programación de *smart contracts,* proporcionadas por *Github*[81] y *Medium*[82]*,* tienen un alto contenido técnico dirigido solamente a programadores[83].

Junto con la propuesta de crear un *Smart Contract Inventor,* en lugar de utilizar lenguaje de programación como *Solidity*, e incluso algunos proyectos existentes de programación de *smart contracts* mediante C# o *Javascript,* debería articularse una herramienta de composición visual o icono para facilitar que cualquier usuario sin ser programador pudiese incorporar cláusulas representadas en un icono y personalizar un *smart contract.* Esta simplificación fue la que permitió el uso de los ordenadores a usuarios no expertos, pues inicialmente estaban destinados únicamente a programadores informáticos. Estos utilizaban una línea de comandos para dar órdenes en forma de código informático, mediante el *Microsoft Disk Operating System*[84] –más conocido como MS-DOS–, hasta la creación de *Windows.* Este sistema operativo popularizó su uso mediante los iconos con su distribución inicial[85] –originada en 1985 y desarrollada posteriormente como *Windows New Tecnhology*[86] o *Windows NT* en 1993–, y cuya primera versión exitosa para el gran público fue Windows 95. Su composición interna como núcleo de tipo híbrido permitió a usuarios inexpertos ordenar una función clicando un icono, mediante la *Graphical*

[81] *Github* (https://github.com).

[82] *Medium* (https://medium.com).

[83] Por ejemplo, *EtherScripter* permite arrastrar bloques que, una vez ensamblados unos con otros, crean una cadena a modo de código condicional lógico, e incluso pueden programarse repeticiones para configurar un *smart contract* básico. Otra experiencia posible, como idea prospectiva sujeta a su materialización, seria *ShadowEth* (Yuan, 2018, pp. 542-556), una plataforma cuyo *hardware* permite crear y almacenar *smart contracts* privados y garantizar su confidencialidad en una *blockchain* pública, como es *Ethereum* en este caso. Sin embargo, estas posibilidades son todavía desconocidas por el público en general, y para promover su utilización debería simplificarse todavía más, pues este último ejemplo resulta de difícil manejo para quien no tenga unas mínimas nociones de programación. OCARIZ (2018, pp. 98-99) reconoce que la mejora de los compositores como *EtherScripter* será clave en la difusión de esta tecnología más allá de la comunidad informática.

[84] Sus versiones eran PC DOS 1.0 (lanzado en 1981), PC DOS 1.1, MS-DOS 2.0, PC DOS 2.1, MS-DOS 2.11, MS-DOS 3.2, PC DOS 3.3, MS-DOS, 3.3, MS-DOS 4.0, PC DOS 4.0, MS-DOS 4.01, MS-DOS 5.0, MS-DOS 6.22, MS-DOS 6.0, MS-DOS 6.2, MS-DOS 6.21, PC DOS 6.3, MS-DOS 6.22, PC DOS 7.0, MS-DOS 7.0, MS-DOS 7.1, y MS-DOS 8.0.

[85] Sus versiones fueron el Windows 1.00 (lanzado en noviembre de 1985), Windows 2.00 (lanzado en noviembre de 1987), y Windows 3.00 (lanzado en mayo de 1990).

[86] Sus versiones fueron Windows NT 3.1 (lanzado en abril de 1992), Windows NT 3.5 (lanzado en septiembre de 1994), Windows NT 3.51 (lanzado en mayo de 1995), Windows 95 (lanzado en agosto de 1995), Windows NT 4.0 (lanzado en julio de 1996), y las versiones sucesivas de Windows 98, Windows 2000, Windows Me, Windows XP, Windows Vista, Windows 7, Windows 8, Windows, 8.1, y Windows 10.

User Interface[87] o GUI, es decir, la interfaz gráfica de usuario. Como vemos, la clave del éxito fue la simplificación mediante iconos de las órdenes y la ocultación de la línea de comandos, solo disponible para programadores. Actualmente, la creación de nuevos iconos es posible en determinadas páginas web[88], que lo ofrecen partiendo de una imagen. Por ello, de lo que se trata es de que la plataforma en la que se cree el *smart contract* contenga una herramienta que permita transformar un código informático, que resulte frecuente en la contratación, en un icono que lo represente. En este sentido, la línea de comandos sería parecida a la codificación en los *smart contracts*, pues en la línea de comandos el ordenador recibe las órdenes del usuario y las procesa, mientras que en la codificación del *smart contract,* el programador debe prever todas las eventualidades del contrato y codificarlas para que la autoejecución futura sea adecuada. En definitiva, consideramos por todo ello que evolucionar hacia la *iconification* u iconificación de las prestaciones contractuales de los *smart contracts* haría posible su acceso a usuarios no expertos.

4. Errores de programación, responsabilidad civil objetiva y protección de datos de carácter personal

Llegados a este punto, y habida cuenta de la importancia de la programación para la correcta ejecución del *smart contract,* debemos contextualizar la trascendencia económica de los ataques informáticos y los defectos de programación. El *MIT Media Lab* (ORCUTT, 2019) señala que, desde principios de 2017, los *hackers* se han apropiado del equivalente a 1.800 millones de dólares en criptomonedas. Ello se debe a los *bugs* o errores en el programa informático de las plataformas correspondientes, cuyo tratamiento legal veremos a lo largo de este apartado. En particular, atenderemos a los fallos en la plataforma *Ethereum,* conocidos como el ataque a *The DAO* de 2016 (ATZEI, 2017, pp. 1-23) y el ataque a *Parity*, a los que por su importancia nos referiremos a continuación, junto con otros casos[89] a los que nos remitimos.

The DAO fue la denominación de un proyecto impulsado por la sociedad alemana *Slock.it UG*. Consistía en un fondo de capital riesgo operado mediante un *smart contract* sobre la plataforma *Ethereum*, cuyo objetivo era la financiación de *startups* y que fue hasta su fecha la operación de *crowdfunding* más exitosa de la historia[90]. El 17 de junio de 2016 un *hacker,* conocido como *The Attacker,* aprovechó un *bug* en las *recursive calls* o retiradas repetidas de fondos. Al producirse antes de actualizar el balance, logró transferir en *Ethers* el equivalente a 40 millones de dólares a una cuenta de su control, y anunció acciones legales contra quieres pretendiesen privarle de los *Ethers* adquiridos. La *Ethereum Foundation*, formada por los inversores, desarrolladores y mineros de *Ethereum,* llegó al acuerdo de que el mal denominado "robo", pues en realidad se trata de una apropiación indebida, debía dejarse sin efecto mediante un *hard fork* de emergencia, ejecutado el 20 de julio de 2016. Este *hard fork* consistió en una alteración de la cadena de bloques para generar una nueva línea que iniciase desde el bloque anterior a la transferencia fraudulenta,

[87] Se trata de un programa informático que utiliza un conjunto de imágenes u objetos gráficos para representar la información y acciones disponibles en la interfaz, y su principal función es proporcionar un entorno visual sencillo para que un usuario sin conocimientos de programación pueda comunicar instrucciones al sistema operativo del ordenador.

[88] *Iconifier,* por ejemplo, mediante el uso de imágenes en los formatos ".jpg", ".png", o ".gif" permite crear en el momento un icono que lo represente (https://iconifier.net/).

[89] Estos casos se refieren a *CoinDash ICO*, con una pérdida en criptomonedas de 10 millones de dólares, la Estafa del Proyecto Enigma, consistente en una preventa falsificada de Tokens que supuso una pérdida de 1.500 *Ethers*, el robo de *Tether,* que perdió el equivalente a 31 millones en Tokens, y la Estafa de *Bitcoin Gold*, que conllevó una pérdida del equivalente a 3 millones de dólares.

[90] Consiguió recaudar en *Ethers* el equivalente a 150 millones de dólares por parte de 11.000 inversores desde el 30 de abril al 28 de mayo de 2016.

porque el sistema impide modificar el contenido de cada uno de los sucesivos bloques por el encadenamiento de los *hashs.* Esta nueva cadena de bloques tiene una longitud que supera a la anterior, de modo que, aunque coexistan, acaba prevaleciendo la segunda porque los nodos tienen como referencia la cadena más larga. En consecuencia, todos los *Ethers* transferidos, incluyendo los fraudulentos, se traspasaron a una *recovery address* a través de una transferencia incluida en un bloque enlazado con el *hash* del bloque anterior al *bug*. Ello permitió la autocomposición del conflicto mediante la manipulación de la cadena de bloques, sin acudir a la jurisdicción ni exigir responsabilidad alguna al *Attacker*. A pesar de haber logrado el objetivo final, que era evitar las consecuencias del ataque a la plataforma, como los inversores eran partidarios de mitigar sus consecuencias, y los desarrolladores y mineros consideraban que debían asumir ese fallo como riesgo del sistema, los nodos partidarios de asumirlas se escindieron en la plataforma *Ethereum Classic*[91], con su criptomoneda *Ethereum Classic* o ETC. Por su parte, quienes promovieron el *hard fork* mantuvieron el nombre de *Ethereum*[92] y su criptomoneda *Ether,* que es la única de las dos criptomonedas que se puede adquirir en la actualidad. Esta escisión, más allá de manifestar un descontento por la falta de asunción de los riesgos de la programación, carece de sentido práctico por lo que a continuación explicaremos.

Existen auténticos ríos de tinta –referidos a lo largo de este apartado y a los que nos remitimos– que describen con mucho más detalle lo acontecido, pues la pretensión de estas líneas es acercar el error de programación del *smart contract* a un lenguaje divulgativo para analizar sus consecuencias jurídicas. Sin embargo, todos desatienden lo que realmente sucedió, porque de nuevo necesitamos al Derecho. El *hard fork* o reprogramación consideramos que en realidad consiste en la aplicación de un viejo remedio jurídico: el enriquecimiento injusto. Descartamos el cobro de lo indebido porque la transmisión patrimonial en sí misma no era legítima, puesto que *the Attacker* se aprovechó de la falta de actualización del balance para efectuar las retiradas repetidas de fondos. La codificación informática no puede con todo, y buena muestra de ello son los "hackeos", por lo que resulta positivo y necesario que existan soluciones legales para mitigar y revertir sus efectos. El Derecho se presta a unas valoraciones subjetivas que impide la objetividad u ortodoxia de la programación, pues no todo es reducible a un código informático. Sin embargo, haber permitido las consecuencias de la apropiación, además de haber hundido la plataforma, solamente habría servido para amparar el uso fraudulento de esta tecnología, o lo que es lo mismo: que el Derecho diese cobertura a que una programación maliciosa posibilite un acrecimiento patrimonial injustificado a costa de la plataforma. En este caso, lo podemos calificar de enriquecimiento injusto *sui generis,* porque en lugar de que *The Attacker* restituyese lo obtenido, se optó por una reprogramación que permitió el reintegro del contenido económico a la plataforma. Por todo ello, debemos señalar que la aplicación de la codificación informática sin moderar sus desequilibrios llevaría a la imposibilidad de mitigar sus consecuencias negativas. La subsistencia del código informático necesita del Derecho. De lo contrario, no pueden evitarse las consecuencias de llevar al extremo o, mejor dicho, al absurdo, la expresión *Code is Law.* El Derecho instrumenta alternativas ante la rigidez normativa; de igual manera, la programación debe plantearlas, como en definitiva lo fue el *hard fork,* aunque ello haga visible la vulnerabilidad del código, pues necesita adaptarse a nuevas realidades como el Derecho. En definitiva, por encima de las ventajas objetivas que ofrece la programación, deben existir remedios externos para subsanar sus defectos, pues lo opuesto sería la aplicación del Derecho sin atender al caso concreto ni a la justicia material.

---

[91] *Ethereum Classic* (https://ethereumclassic.org/).

[92] *Ethereum* (https://www.ethereum.org/).

Por otra parte, otro ataque al que nos hemos referido inicialmente es el de la billetera virtual *Parity,* que arbitraba un mecanismo de firmas múltiples en *Ethereum.* Un *hacker* introdujo una serie de errores en el código fuente de la billetera digital, bloqueando el equivalente en *Ethers* a 300 millones de dólares. Los programadores de *Parity* sabían que existía este riesgo, pero no lo programaron por considerarlo improbable, lo que demuestra la conveniencia de codificar tantos "*else"* como sea necesario. De los errores se aprende, y de este suceso surgió la creación de *Mythril*, una herramienta de exploración *blockchain* e intercepción de errores que permite buscar, desensamblar y analizar *smart contracts* en *Ethereum,* mediante el lenguaje de programación *Python,* con la finalidad de dificultar futuros ataques.

Estos errores en la programación derivan del automatismo de estos contratos y, en consecuencia, de su irreversibilidad, porque no se puede detener su ejecución sino solamente revertir sus efectos mediante la reprogramación. Ningún código informático está exento de *bugs,* lo que requiere su comprobación previa en aras de evitar resultados inadecuados y garantizar su ejecución sin intervención humana o reprogramación. Estos errores conllevan el incremento (BELLAMY, 2016, pp. 6-12) de la inversión para evitarlos y de los costes de indemnización por una programación defectuosa. Por ello, apuntamos que una extensión a la contratación en masa de los *smart contracts* debería llevar aparejada una responsabilidad de carácter objetivo de la plataforma que ofreciese la adhesión a un *smart contract* predispuesto, mediante la formalización de un contrato de seguro que cubriese los daños generados al adherente, sin tener que demostrar nada más que el perjuicio económico. La justificación de dicha responsabilidad objetiva de la plataforma predisponente la encontramos en la calificación del usuario de esa plataforma como *consumidor,* y por el hecho de la *adhesión,* sin posibilidad de modificación, que hace necesaria la imputación de la responsabilidad a quien ofrezca un servicio defectuoso por un error de programación, de conformidad con el art. 128 del 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 (BOE nº 287, de 30.11.2007). Debemos advertir que la exigencia legal de responsabilidad objetiva que proponemos puede conllevar que plataformas como *Blockchain* dejen de ser gratuitas, pues de algún modo complementario a la publicidad y la cesión de datos de carácter personal debe sufragarse el coste por el aseguramiento de esta responsabilidad. Por el contrario, en el caso de la personalización de un *smart contract,* la responsabilidad debería tener carácter subjetivo, conforme al art. 1902 CC, para individualizar la conducta del programador, consistente en codificar las prestaciones indicadas por las partes, así como la de los contratantes en la indicación del contenido contractual, en aras de determinar una compensación proporcional a la responsabilidad de los intervinientes.

Otro aspecto que plantea desajustes en este ámbito es la protección de datos de carácter personal y su encriptación. Con el surgimiento de los *smart contracts,* el Derecho tuvo que dar respuesta a dos problemas: por una parte, la ocultación de la identidad personal, pues la IP del dispositivo identifica a los equipos informáticos; y, por otra parte, la protección de datos de carácter personal, fruto de nuestro volcado a los sitios web que posteriormente los intercambian. Estos problemas han sido parcialmente resueltos con la encriptación de datos y una normativa europea de protección de datos. La encriptación de datos, tan frecuente en el uso de aplicaciones de mensajería, se basa en la denominada *criptografía asimétrica*, concebida por Whitfield Diffie, Martin Hellman y Ralph Merkle en 1976, y desarrollada mediante el algoritmo *RSA* por Ron Rivest, Adi Shamir y Leonard Adleman en 1977. Esta criptografía efectúa una encriptación de doble clave o clave pública: proporciona confidencialidad mediante la encriptación del mensaje

con la clave pública del destinatario; y garantiza su autenticidad o garantía de origen, es decir, la firma electrónica o la encriptación del mensaje con la clave privada del emisor.

Por lo que se refiere a la protección de datos de carácter personal, el Reglamento 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 (DOUE nº 119, de 4.5.2016), regula esta materia. En particular, el art. 22 prohíbe el procesamiento automático de datos, salvo en tres casos, referidos en el apartado segundo: que la decisión sea necesaria para la celebración o la ejecución de un contrato entre el interesado y el responsable del tratamiento; que esté autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, y que establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o que se base en el consentimiento explícito del interesado, opción habilitada en la mayoría de plataformas mediante el *"I agree button"*. Por tanto, los *smart contracts* solamente podrán procesarse automáticamente (FINCK, 2019, pp. 1-17) si cumplen estos requisitos, que deberán matizarse. Al tratarse de un código informático, los *smart contracts* se ejecutarán si cumplen los requisitos del apartado segundo, que en realidad constituye una fuga respecto de la efectiva protección de datos. En cuanto a las medidas que el responsable del tratamiento debe adoptar, creemos que es necesario el establecimiento en el *smart contract* de una cláusula que publicite las acciones que lleva a cabo la empresa para garantizar la protección de datos, a modo de *Corporate Compliance* (FRIES, 2018, pp. 11-18). Sin embargo, plantea contrariedades la última causa relativa al consentimiento, por falta de concreción, pues en realidad la cesión de datos se encuentra sujeta a la correcta prestación del consentimiento informado sobre el tratamiento de los mismos, especialmente cuando el uso de la plataforma es gratuito. La automatización de la ejecución del contrato impide que se pueda hacer efectivo en la práctica el tercer requisito, porque no existe la posibilidad de revocar el consentimiento, máxime en un contrato de adhesión, una revocación que por el contrario permite la contratación electrónica.

5. La formación y la ejecución de los *smart contracts:* autoimplementación y autoejecución

5.1. La formación y la ejecución del contrato: tratamiento de la invalidez y la ineficacia en sentido estricto

A la luz de lo expuesto hasta el momento, podemos afirmar que los *smart contracts* constituyen una revolución en la contratación y la confianza de las partes. La programación sustituye la valoración subjetiva humana, para la apreciación de determinadas vicisitudes en la fase de ejecución, por unos datos de carácter objetivo que van a automatizar los remedios y evitar la simulación contractual. Esta codificación permite reducir los costes de intermediación o gestión, así como la eventual litigiosidad, reservada para aquellos asuntos más complejos. Sin embargo, presenta algunos desajustes que examinaremos a continuación, referidos a la autoimplementación del contenido obligacional –realtivo a la fase de formación– y la autoejecución del contrato, en particular, respecto de los remedios privados frente al incumplimiento.

Los *smart contracts* reúnen los elementos esenciales del contrato contenidos en el art. 1261 CC, pues que la formación y ejecución sea automática, o al menos que una vez expresada la voluntad

de perfeccionar un contrato se ejecute automáticamente, no impide categorizarlos como verdaderos contratos. En relación con el consentimiento, debemos considerar que en el *smart contract* se presta de manera inmediata, es decir, directa en la personalización de un contrato o en la adhesión a uno predispuesto. En el *M2M contract,* las partes prestan su consentimiento de manera mediata, pues, por ahora, solamente tiene capacidad para ello una persona, representada por una clave criptográfica (WERBACH, 2017, p. 371) o por un tercero mediante una *proof of identity*, pero no un código informático *per se*, que únicamente constituye una forma electrónica (MORENO, 1999, pp. 34-36) de emitir el consentimiento. En el *smart contract* originario, el consentimiento se presta de manera inmediata, y en el *M2M contract* por remisión al consentimiento previo del que deriva este segundo contrato. Eso puede dar lugar a la existencia de vicios del consentimiento –en particular, el error– en el consentimiento inmediato que, al no emitirse un nuevo consentimiento, se extiendan al *M2M contract*. La validez del *M2M contract* queda sujeta, lógicamente, a la prestación de una adecuada información a la contraparte del acaecimiento de este segundo contrato, por lo que resulta especialmente importante en materia de consumo el deber de información precontractual y el control de transparencia de la cláusula que disponga la ejecución automática de este segundo contrato.

Respecto del objeto, la prestación es previa y conocida por las partes, de manera que está determinada con anterioridad a su ejecución, y debe tratarse de un objeto lícito, posible y determinado o determinable, conforme a los límites de los arts. 1271, 1272, 1273 y 1255 CC. Los problemas que plantea el objeto del contrato serán analizados con mayor profundidad en el siguiente subapartado, porque no se refieren a los requisitos de la prestación sino a los resultados inadecuados provocados por el automatismo del código. En relación con la causa, y teniendo en cuenta la falta de armonización de este elemento en el Derecho comparado, recordamos que viene determinada por la propia naturaleza de la prestación. Por la automatización de las prestaciones, una adecuada codificación va a evitar que la causa no se corresponda con la finalidad económica que dimane de la naturaleza del contrato, esto es, el código informático evita o reduce en la práctica la simulación contractual. En este sentido, los *smart contracts* deberán atender para su correcta formación a determinados datos externos al contrato, de carácter administrativo, bancario, tributario y judicial, por lo que resulta imprescindible que la Administración incorpore la tecnología *blockchain* para permitir su incorporación. En particular, sería conveniente que la Administración Tributaria habilite la autoliquidación de determinados impuestos desde el propio *smart contract*, para dificultar todavía más la simulación contractual y reducir los costes de inspección.

En cuanto a la forma, si bien es cierto que rige el principio de libertad de forma, *ex* art. 1278 CC, no es menos cierto que, por exigencia legal y por seguridad jurídica, existe un amplio sector de contratación en la que será necesaria la formalización del *smart contract* mediante escritura pública, conforme al art. 1280 CC y al art. 23.4 de la Ley 34/2002. En consecuencia, en lugar de negar[93] el ámbito material de aplicación a los *smart contracts* por la forma, consideramos que es más adecuado articular un mecanismo conforme al cual, una vez celebrado el contrato, el código informático suspenda la autoejecución hasta que las partes procedan a elevar el contrato a escritura pública. Una vez examinados los elementos esenciales del contrato, respecto de la invalidez del contrato, el principal vicio que puede tener incidencia en el *smart contract* es el error, *ex* art. 1265 CC, derivándose la anulabilidad del contrato si cumple con los requisitos del

[93] LEGERÉN (2018, p. 218) afirma que el ámbito de aplicación de los contratos inteligentes se limita cuando se exige escritura pública, y que no cabe realizar contratos inteligentes que sustituyan a los que requieren de documento público.

art. 1266. Sin embargo, por el automatismo de la ejecución del contrato, será difícil mitigar los efectos del error en la codificación[94] del contrato, porque una eventual reprogramación supondría una adaptación del contrato que no se corresponde con la anulabilidad que procede.

Respecto de las fases del contrato aplicadas a los *smart contracts,* en la fase de formación (DUROVIC, 2018, pp. 753-771), la voluntad de las partes interviene de manera inmediata, y de manera mediata en la fase de ejecución. Desde esta perspectiva, el *smart contract* se asemeja a dos tipos de contratos que reinterpretan la autonomía de la voluntad: los contratos dictados y los contratos de adhesión. En los contratos dictados, la celebración proviene del libre pacto entre las partes y los efectos vienen determinados *ex lege,* lo que se correspondería con la automatización de la ejecución en los *smart contracts*. Por su parte, en los contratos de adhesión, el consumidor decide voluntariamente adherirse y los efectos vienen predispuestos por el acreedor; esto mismo sucede cuando un consumidor se adhiere a un *smart contract* que no puede negociar. Debemos recordar aquí que, en el caso de relaciones de tracto sucesivo, mediante un único acuerdo de voluntades que afecta a la fase de formación, se automatiza la ejecución de las prestaciones. Ello no supone una automatización de la formación, sino una continuación de lo acordado por las partes por economía contractual. Sin embargo, también es posible una remisión a esa formación voluntaria del contrato para la ejecución de prestaciones accesorias que permitan cumplir con lo pactado, sin deducir de ello la automatización de su formación. Esta consideración tiene una especial relevancia en las DAOs, por ejemplo, cuando contratan con otros entes determinados servicios, como el repuesto de una sustancia para el funcionamiento del objeto del contrato sin requerir un nuevo consentimiento de la contraparte, es decir, remitiendo dicho consentimiento a la formación del contrato matriz.

Por lo que respecta a la fase de ejecución, las prestaciones autoimplementadas en fase de formación del contrato desencadenan las consecuencias jurídicas previstas por las partes, para cuya comprobación y cumplimiento el código informático va a verificar la existencia de los eventos externos al contrato que sirven de premisa. Los ordenadores ejecutan lo establecido en el código mediante unos algoritmos prefijados por las partes en atención a la producción de unos determinados resultados, o el arbitrio de los correspondientes remedios. En la ejecución del *smart contract*, no hay margen para la interpretación jurídica, por lo que Szabo lo denominó *wet code,* en contraposición al *dry code* interpretado por ordenadores (SZABO, 1996). De esta manera, deben introducirse en el código informático las cláusulas que puedan automatizar la adaptación del contrato, en particular ante el cambio de circunstancias y la excesiva onerosidad, la moderación equitativa de las cláusulas pactadas, así como la desvinculación por incumplimiento, e incluso ante el enriquecimiento injusto, por mencionar algunos ejemplos. Asimismo, el código informático debe habilitar un mecanismo que materialice la retroactividad o la mitigación de los daños derivados de la ejecución del contrato, por una mala programación o porque esta no ha atendido posibles efectos adversos. En definitiva, estos contratos deben satisfacer por sí mismos, o mediante su impugnación judicial, las expectativas jurídicas de las partes.

Los *smart contracts* siempre están condicionados a la producción de los eventos futuros que desencadenan la ejecución de las prestaciones del contrato. Por ello, resulta fácilmente programable el cumplimiento de los requisitos de validez, pero difícilmente, por tratarse de eventos futuros e imprevisibles, la ineficacia en sentido estricto. Por la importancia que tiene en

[94] BELLAMY (2016, pp. 6-12) vinculan la modificación o anulación de un *smart contract* con el error, una vinculación que creemos que pasa por alto las consecuencias de ambos remedios.

la ejecución del contrato la comprobación de los eventos externos, debería articularse la presencia de los oráculos también en esta fase, y no únicamente en la de formación como hasta ahora. De esta manera, estos terceros imparciales ajenos al contrato podrían reintroducir en la codificación elementos externos, una vez comprobados. Una adecuada codificación posibilita la atención *a posteriori* de las consecuencias de la falta de conformidad, pues la calidad en el cumplimiento de una determinada prestación es un juicio de apreciación no codificable. Incluso en los contratos aleatorios, la programación del contrato deberá tener acceso a determinada información externa al contrato, que no puede autoimplementarse durante su formación, para comprobar si el evento que desencadena la prestación principal se ha cumplido o no. Por tanto, la automatización contractual va a ser completamente útil respecto de prestaciones cuyo cumplimiento se pueda encomendar en exclusiva a un programa informático.

Finalmente, una vez examinada la invalidez y la ineficacia en sentido estricto, debemos atender al tratamiento de la tutela judicial del *smart contract*. Este contrato es un título autoejecutivo y, por tanto, *enforceable* al margen de la jurisdicción, mediante remedios privados que no permiten la defensa u oposición de la parte ejecutada. Ello constituye una importante diferencia con el título ejecutivo *ex* art. 517 LEC, que habilita el acceso directo al procedimiento judicial de ejecución mediante, por ejemplo, una escritura pública e intervención notarial como garantía del consentimiento informado. En esta autoejecución no interviene un intermediario de confianza, como una de las partes, porque su intervención es mediata en la fase de formación, y ello implica que debamos matizar sus consecuencias. En atención al importante papel que tiene la programación, si esta es adecuada debería permitir, sin acudir al control notarial, la correcta prestación del consentimiento informado y la incorporación de los eventos externos y sus consecuencias al contrato. En los casos en los que sea necesario este control, si no se reforma el art. 267 LEC, que exige escritura pública en determinados supuestos[95], la tarea informativa del Notario podría quedar automatizada, especialmente respecto del deber de información precontractual y la eventual conclusión de un *M2M contract*. En este sentido, debería reformarse la legislación aludida al inicio de este trabajo para que, en particular, cuando se trate de un consumidor, no sea posible autoejecutar el contrato, es decir, que se incluya una cláusula de desvinculación en distintos casos: cuando ello conlleve consecuencias irreversibles, por ejemplo, la pérdida del objeto del contrato cuando afecte a necesidades básicas, como la vivienda; en el caso de que la ejecución sea excesivamente gravosa para el consumidor, para evitar la excesiva onerosidad del contrato[96]; y los supuestos de la cláusula *rebus sic stantibus*[97].

5.2. La automatización de los remedios: algunas limitaciones por razón del objeto, y el papel del *Internet of Things* y la Tokenización

La automatización propia de los *smart contracts* debe limitarse cuando impida mitigar las consecuencias materiales de los resultados inadecuados, especialmente cuando tengan carácter irreversible. Estas consecuencias pueden evitarse con la conexión del objeto del contrato mediante el IoT a la red. El IoT permite integrar el objeto en el *smart contract*, como puede ser un vehículo en un contrato de seguro[98] o en un préstamo para su adquisición. Esta conexión hace

[95] Véase *supra* apartado 3.2.

[96] Por ejemplo, este fue el fundamento del pronunciamiento del TJUE respecto de la conocida como hipoteca multidivisa en la STJUE, 20.9.2017 (TJCE 171; MP: A. Prechal).

[97] Véase *supra* apartado 2.3.

[98] La plataforma *Etherisc* es objeto de estudio por parte del *European Law Institute's project team on block chain & smart contracts* (https://www.etherisc.com/). *Etherisc* dispone de una plataforma para formalizar *smart contracts* de seguro,

posible su control[99] porque el *smart contract* no puede *per se* adaptar la codificación sin la vinculación del objeto mediante el IoT, pues este instrumento posibilita la recepción de los eventos externos que le afecten y la incorporación de sus consecuencias jurídicas al contrato.

Respecto de la ejecución del contrato, este instrumento automatiza las consecuencias del incumplimiento con el bloqueo del objeto del contrato, o la transmisión de información en caso de un evento imprevisto. En caso de accidente de circulación, por ejemplo, la aplicación de esta tecnología permite que los datos recogidos por los sensores de un automóvil inteligente, conectado a un *smart contract* de seguro mediante el IoT, puedan remitir los datos para su incorporación al parte de accidente y así proceder a depurar las responsabilidades civiles correspondientes, reduciendo eventuales errores o fraudes (JOHNSON, 2017, pp. 73-78) en los resultados del siniestro. Incluso puede servir para la emisión permanente de información conforme a la cual proceda la renovación automática de la póliza del seguro, de cumplirse con las condiciones pactadas previamente, mediante los algoritmos conectados con el *Big Data* que miden los eventos externos. Sin embargo, deben preverse excepciones a dicho automatismo cuando la seguridad de la parte que ha incumplido se vea comprometida, por ejemplo, por circular con un automóvil a alta velocidad, o cuando se vean afectadas sus necesidades básicas, como en el caso de que el objeto recaiga sobre la vivienda habitual. Las ventajas que plantea la aplicación del IoT a los *smart contracts* son diversas. Por una parte, facilita la ejecución real del contrato sin necesidad de un ordenador central en quien confiar la ejecución o de un acuerdo posterior de las partes. Por otra parte, la conexión del objeto contractual mediante el IoT desincentiva el incumplimiento, pues la principal prerrogativa para la contraparte es la posibilidad de inutilizar el objeto del contrato o impedir su acceso. Si nos encontramos ante una relación contractual de hecho, por tratarse de contratación en masa, el incumplimiento directamente impide la ejecución del contrato y arbitra el remedio de la desvinculación.

En la actualidad, todavía son escasos los objetos cotidianos que pueden vincularse a la red, de los cuales los más llamativos son los altavoces inteligentes. Con un mayor desarrollo del IoT, además de vincular un objeto a un *smart contract*, se podrá controlar su propiedad y uso mediante la *Tokenización*. Un *Token* es un metadato o referencia criptográfica sobre un registro de tipo descentralizado, a modo de unidad de valor. Este metadato lo crea una organización para basar su modelo de negocio, y que sus clientes utilicen los *Tokens* para interactuar con sus productos. Algunos ejemplos los encontramos en las acciones, bonos, derechos de propiedad intelectual, divisas, derechos sobre bienes muebles como obras de arte, automóviles e incluso derechos sobre bienes inmuebles. Estas fichas digitales tienen propiedad intelectual[100], y se someten a una programación informática que los hace susceptibles de ser objeto de *smart contracts*. FINMA[101], que es el regulador financiero de Suiza, ha distinguido tres clases de tokens, según su función: los *payment tokens,* destinados a utilizarse como criptomonedas; los *utility tokens,* que proporcionan acceso digital a una aplicación o servicio; y los *asset tokens,* que representan activos

---

personalizados o prototípicos, por retrasos en vuelos, protección contra huracanes, seguros para tarjetas *cryptowallet*, seguros para la contratación de préstamos, seguros para la cosecha, seguros de vida y salud, así como la posibilidad de solicitar la creación de nuevos productos o construir, es decir, personalizar el propio producto.

[99] STARK (2016) quien alude como problema la inexistencia de un control físico sobre los activos reales por parte del *smart contract*, pero no es necesaria esta codificación porque mediante la vinculación del objeto contractual al IoT ya es posible dicho control: "First, smart contracts require a way for computer code to control real assets. By enabling fully digitized assets, blockchains make it possible for code to exercise control over property. On a blockchain, control over an asset means controlling a cryptographic key that corresponds to the asset in question, rather than any physical object".

[100] Sobre los problemas de la propiedad intelectual en el ámbito de los *Tokens*, véase KRUMHOLZ (2019).

[101] FINMA (https://www.finma.ch/en).

como acciones, participaciones e incluso el derecho al pago de dividendos o de intereses. FINMA advierte (FINMA, 2018, pp. 1-11) que pueden crearse *tokens híbridos;* ello sucederá, por ejemplo, en la criptomoneda *Ether*. En este caso, el *payment token* es utilizado como *utility token* a modo de *gas*, que es el coste de computación en la plataforma *Ethereum* para ejecutar *smart contracts*, a diferencia de la plataforma *Blockchain* que no repercute el coste del *gas* al usuario.

Las empresas u otras organizaciones crean tokens para basar su modelo de negocio y que sus clientes los utilicen para interactuar con sus productos. La Tokenización posibilita la digitalización de la propiedad, de modo que su administración y disposición es programable, permitiendo su control mediato a tiempo real mediante la tecnología *blockchain*. En la actualidad, *Blockchain* y *Ethereum* permiten entre tres y seis transacciones por segundo, una cifra que *Ethereum* prevé incrementar hasta 1 millón por segundo, lo que facilitaría la Tokenización de inmuebles. La principal ventaja de la Tokenización es que permite transformar activos poco líquidos en instrumentos para obtener financiación, lo que proporciona liquidez inmediata al mercado inmobiliario en caso de transmisión, de forma similar al proceso de titulización hipotecaria. Por ejemplo, las plataformas P2P dedicadas al *crowdfunding inmobiliario* adquieren las propiedades y generan los tokens que se negocian en la plataforma *blockchain* correspondiente. Los tokens son divisibles y universales, de modo que si aumenta su demanda se va a reducir el denominado *descuento de iliquidez*.

Tanto en la Tokenización de bienes inmuebles como muebles, resulta esencial que el token permanezca vinculado al objeto del derecho real, es decir, que el activo digital tenga correspondencia posesoria con el activo real. Ello permite comprobar la existencia de los elementos de la adquisición derivativa y la extinción por pérdida o destrucción de la cosa. La comprobación material de la tradición en la adquisición derivativa realizada mediante la Tokenización se concreta en las siguientes clases de tradición: en primer lugar, mediante la representación de la propiedad en el token correspondiente, lo que se correspondería con la *traditio ficta;* en segundo lugar, puede articularse con la comprobación mediante Oráculos o terceros de confianza para un correcto traspaso posesorio como *tradición real;* finalmente, el cambio del título posesorio en caso de constitución de un derecho real limitado puede realizarse mediante el *constitutum possessorium* que, aunque el art. 1463 CC lo refiera a bienes muebles, también se aplica a bienes inmuebles, con la finalidad de ejecutar las prestaciones mediante la *blockchain* en el *smart contract* de que se trate. Otras opciones alternativas al uso de un tercero intermediario en una *blockchain* son las siguientes: *fábrica* y *harbor*. El concepto de *fábrica* consiste en introducir una capa intermedia entre la plataforma P2P que ofrece inmuebles y sus potenciales clientes para que esta capa actúe de tercero a modo de fideicomitente. La encomienda de *fábrica* es ser el receptor temporal de la propiedad para incluirla en un contrato operado en una *blockchain* y mediante unas APIS, que son unos protocolos informáticos para que las webs intercambien la información necesaria para formalizar un *smart contract*. Por su parte, *harbor* introduce la capa intermedia antes referida a modo de *Regulated token,* para comprobar el cumplimiento normativo de la transacción correspondiente. El *Regulated token* es un protocolo que comprueba la información de los inversores que pretendan participar en la transacción, así como la dirección y aprobación comercial de la transacción.

La Tokenización plantea dos retos (SAVELYEV, 2018, pp. 863-869) para el Derecho civil. En primer lugar, la sustitución del objeto contractual del Derecho civil y su regulación legal, por la regulación del token: en forma de mecanismo reputacional, a modo de aceptación de los términos y condiciones de uso (BYGRAVE, 2015, pp. 30-39) de la plataforma correspondiente; o en

el caso de tratarse de un modelo de acceso abierto, en forma de *core team* (PHILLIPS, 2009, pp. 147-173) o personas que controlan y desarrollan centralizadamente la plataforma. En segundo lugar, la determinación de la naturaleza real o personal de los derechos derivados de los *tokens*. Ello dependerá de si representan una criptomoneda, en cuyo caso deberá configurarse como un derecho de crédito sin la figura del deudor. Asimismo, puede existir un token como derecho de crédito que obligue al deudor, por representar el derecho de un inversor a participar en los beneficios sobre la explotación de un derecho real.

Por ello, debemos distinguir (SAVELYEV, 2018, p. 867) entre *the right to a token* o el derecho a un token, como en las criptomonedas, de *the rights certified by a token* o los derechos que represente, como el derecho de propiedad, pues ello hace que podamos diferenciar dos relaciones jurídicas: la del propietario del token respecto de terceros, y la del propietario del token y el emisor del token, como sucede en las criptomonedas. El *asset token* o token de activos tiene un emisor, que se convierte en deudor respecto del propietario del token en relación con las obligaciones que certifica para proveer un servicio online. La relación entre el emisor del token y el propietario es un derecho de crédito, pero ello no convierte el derecho del token en un derecho real, como sucede en las criptomonedas, cuando se trata de relaciones con terceros. En consecuencia, resultan claves diversas cuestiones en aras de regular los tokens, por tratarse de un derecho real o un derecho de crédito según su ámbito material de aplicación: la pérdida de control sobre el token; la eventual alteración del token por un *hacker*; la protección *erga omnes,* de tratarse de un derecho real; la clase de posesión del token, que deberá ser mediata; y, finalmente, la imposibilidad de transmitir el token sin la intervención de mineros o terceros. La solución que debería adoptarse al respecto es una adaptación legislativa para que el objeto tokenizado tenga las mismas garantías en el tráfico jurídico que el que no lo esté, con previsiones específicas para cada tipo de contrato y, en particular, su adaptación al Derecho del consumo.

En definitiva, la Tokenización implica la extensión de la tecnología *blockchain* a un objeto, de manera que los titulares de los tokens puedan utilizar un bloqueo inteligente para excluir a terceros mediante una clave privada. Este control permanente del objeto y la facultad de exclusión materializan la *smart property* que Szabo concibió (SZABO, 1996). Sin duda, la Tokenización está muy vinculada al desarrollo tanto de la tecnología *blockchain* como del IoT[102], por lo que deberemos prestar atención a una evolución difícil de prever, pero que va a incorporar supuestos que actualmente no son susceptibles de articularse mediante un *smart contract.* El IoT facilita el control del objeto de un contrato, y la Tokenización permite el control de la propiedad o el uso del objeto. Por tanto, cuando el objeto se encuentre vinculado mediante el IoT al *smart contract*, será posible atender a un cambio de titularidad formal, con la firma electrónica del titular de dicha modificación, pero para comprobar el cambio en la situación posesoria será necesaria, además, la Tokenización del objeto. Todo ello, junto con la tecnología *blockchain,* hace que en un futuro los *smart contracts* pongan en jaque, o al menos hagan replantearse, la configuración actual de tres instituciones: el papel del Notario, pues una adecuada programación puede reducir su necesidad material en el ámbito de la contratación civil y mercantil, por lo que subsistiría para otros negocios jurídicos; la función de calificación del Registrador de la Propiedad, porque puede hacerlo la tecnología *blockchain;* e incluso la propia existencia o necesidad del Registro de la Propiedad, cuya función es la constitución o publicación de titularidades inatacables, porque la Tokenización posibilita materialmente el control de una

[102] STARK (2016) indica que puede alterar la naturaleza de las transacciones comerciales. Sobre la vinculación del IoT y de *blockchain* para garantizar la seguridad de las transacciones, véase BISWAS (2018, pp. 1-10).

finca, la exclusión de terceros e impide la consolidación de realidades extrarregistrales como la usucapión *contra tabulas*.

6. Conclusiones

Los *smart contracts* plantean una serie de ventajas[103], relacionadas con la eficiencia material que implica la sustitución de la confianza de las partes por un control informático externo de las vicisitudes en la formación y ejecución del contrato. Esta confianza virtual se sustenta en tres elementos: la inmutabilidad de los eventos, pues quedan registrados sin posibilidad de alteración en la cadena de bloques; el cumplimiento de las prestaciones, que no se somete a la interpretación humana y se automatizan los remedios frente al incumplimiento; y la autoejecución del contrato conforme a lo pactado y programado.

Sin embargo, muchos son los retos[104] que una aplicación extensiva de los *smart contracts* debe afrontar, como la utilización de un lenguaje menos técnico que los haga accesibles al público en general, y una regulación detallada y armonizada a nivel europeo que evite los abusos y solucione los desajustes analizados a lo largo de este trabajo. Principalmente, se refieren a la dificultad para programar los eventos extrínsecos al contrato, lo que obstaculiza la automatización de la ineficacia en sentido estricto, la extensión de los vicios del consentimiento al *M2M contract* posterior, y las limitaciones derivadas de una aplicación acrítica de la codificación que ocasione resultados inadecuados. Por todo ello, podemos concluir que el éxito y la extensión de los *smart contracts,* para que se consolide como la evolución del comercio electrónico y constituya la alternativa al comercio tradicional, dependerá, por un lado, de la simplificación y, por otro lado, de la protección y seguridad jurídica que la codificación informática y la legislación proporcionen.

7. Bibliografía

Joseph ABADI, Markus K. BRUNNERMEIER (2019), "Blockchain Economics", *CEPR Discussion Paper,* DP13420, págs. 1-53 (https://ssrn.com/abstract=3310346).

Mustafa AL-BASSAM (2017), "SCPKI: A Smart Contract-based PKI and Identity System", *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts 2017,* págs. 1-6.

Mustafa AL-BASSAM, Alberto SONNINO, Shehar BANO, Dave HRYCYSZYN, George DANEZIS (2018), "Chainspace: A Sharded Smart Contracts Platform", *Network and Distributed Systems Security Symposium 2018,* págs. 1-16 (https://www.semanticscholar.org/paper/Chainspace%3A-A-Sharded-Smart-Contracts-Platform-Al-Bassam-Sonnino/11628f59857d7a85971e8b68496016e9d1737d9d).

[103] Sobre las ventajas, O'SHIELDS (2017, p. 183) indica que presenta una mayor rapidez y cuidado en las transacciones, mayor eficiencia y un mayor cumplimiento, reduciendo los costes por litigación. También se observa, como señala KEMP (2018, p. 18), una disminución de las tasas de error en determinadas operaciones, reducción de costos, retrasos injustificados, en virtud de más automatización, una reducción de la intermediación e intervención directa. Sobre las ventajas e inconvenientes en su conjunto, véase ALLAM (2018, pp. 137-156).

[104] SALVADOR (2018, pp. 1-5) plantea algunos de los interrogantes que hemos pretendido resolver a lo largo de este artículo, referidos a la *selfhelp* o autoayuda, el alcance del pacto comisorio, la *exceptio non adimpleti contractus,* y el papel del Derecho del consumo.

Maher ALHARBY, Aad VAN MOORSEL (2017), "Blockchain-based smart contracts: a systematic mapping study", *Computer Science & Information Technology,* págs. 125-140 (https://www.semanticscholar.org/paper/Blockchain-based-Smart-Contracts%3A-A-Systematic-Alharby-Moorsel/5a0e7eebceec42686d39b42de17820f0781a61aa#paper-header).

Jawad ALI, Toqeer Ali SYED, Shahrulniza MUSA, Ali ALZAHRANI (2018), "Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure", *International Journal of Advanced Computer Science and Applications,* vol. 9, núm. 10, págs. 584-591.

Muhammad Salek ALI, Massimo VECCHIO, Miguel Rodrigo PINCHEIRA CARO, Koustabh DOLUI, *et al.* (2018), "Applications of Blockchains in the Internet of Things: A Comprehensive Survey", *IEEE Communications Surveys & Tutorials,* vol. 21, núm. 2, págs. 1676-1717.

Zaheer ALLAM (2018), "On Smart Contracts and Organizational Performance: A Review of Smart Contracts through The Blockchain Technology", *Review of Economic Business Studies,* vol. 11, núm. 2, págs. 137-156.

Ahmed ALMASOUD, Maged M. ELJAZZAR, Farookh Khadeer HUSSAIN (2018), "Toward a self-learned Smart Contracts", *IEEE 15th International Conference on e-Business Engineering,* págs. 1-6.

Cristina ARGELICH COMELLES (2019), "Remedios del consumidor ante la abusividad en los instrumentos no financieros", *Revista Crítica de Derecho Inmobiliario,* núm. 771, págs. 13-65.

Benito ARRUÑADA (2018), "Blockchain's Struggle to Deliver Impersonal Exchange", *Minnesota Journal of Law Science & Technology,* vol. 19, núm. 1, págs. 55-105 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903857).

Kevin ASHTON (2009), "That 'Internet of Things' Thing; In the real world, things matter more than ideas", *RFID Journal* (https://www.rfidjournal.com/articles/pdf?4986).

Nicola ATZEI, Massimo BARTOLETTI, Tiziana CIMOLI (2017), "A survey of attacks on Ethereum smart contracts", *Proceedings of the 6th International Conference on Principles of Security and Trust,* vol. 10204, págs. 1-23.

James BELLAMY, Chris HILL (2016), "Can the Blockchain Make Our Contracts Smarter?", *Cyberspace Lawyer NL 2,* vol. 21, núm. 11, págs. 6-12.

Karthikeyan BHARGAVAN, Antoine DELICNAT-LAVAUD, Cédric FOURNET, *et al.* (2016), "Formal verification of smart contracts: Short Paper", en PLAS'16, *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security,* New York, ACM, págs. 91-96 (https://dl.acm.org/citation.cfm?id=2993611).

Sujit BISWAS, Kashif SHAIF, Fan LI, Yu WANG *et al.* (2018), "A Scalable Blockchain Framework for Secure Transactions in IoT", *IEEE Internet of Things Journal,* núm. 9, págs. 1-10.

Rainer BÖHME (2015), "Bitcoin: Economics, Technology and Governance", *Journal of Economic Perspectives,* vol. 29, núm. 2, págs. 213-238.

Joseph F. BORG, Tessa SCHEMBRI (2019), "The regulation of blockchain tecnology", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2019,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/15-the-regulation-of-blockchain-technology).

Lee A. BYGRAVE, (2015), *Internet Governance by Contract,* Oxford, Oxford University Press.

Daniel CAWREY (2016), "Why Ethereum Needs 'Dumb' Contracts", *CoinDesk* (https://www.coindesk.com/ethereum-dao-dumb-smart-contracts).

Dimitris CHATZOPOULOS, Sujit GUJAR, Boi FALTINGS, Pan HUI (2018), "Privacy Preserving and Cost Optimal Mobile Crowdsensing Using Smart Contracts on Blockchain", *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS),* págs. 442-450.

Jiin-Chiou CHENG, Narn-Yih LEE, Chien CHI, Yi-Hua CHEN (2018), "Blockchain and Smart Contract for Digital Certificate", en IEEE, *Proceedings of IEEE International Conference on Applied System Innovation,* Chiba, IEEE, págs. 1046-1051.

Zhu CHENWEI (2004), "In Code, We Trust? Regulation and Emancipation in Cyberspace", *SCRIPT-ed,* vol. 1, núm. 4, págs. 585-610.

Konstantinos CHRISTIDIS, Michael DEVETSIKIOTIS (2016), "Blockchains and Smart Contracts for the Internet of Things", *IEEE Access,* vol. 4, págs. 2292-2303 (https://ieeexplore.ieee.org/document/7467408).

Franca CIAMBELLA, En-Lai CHONG (2019), "Singapore", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/singapore).

Jenny CIEPLAK, Simon LEEFATT (2017), "Smart Contracts: A Smart way to automate performance", *Georgetown Law Technology Review,* vol. 1, núm. 2, págs. 417-427.

Christopher D. CLACK, Vikram A. BAKSHI, Lee BRAINE (2017), "Smart contract templates: essential requirements and design options", *ArXiv eprints,* págs. 1-15.

CNMV (2018), *Criterios en relación con las ICOs,* de 20 de septiembre de 2018, págs. 1-4 (http://cnmv.es/DocPortal/Fintech/CriteriosICOs.pdf).

- (2019), *Preguntas y Respuestas dirigidas a empresas FinTech sobre actividades y servicios que pueden tener relación con la CNMV* (https://www.cnmv.es/docportal/Legislacion/FAQ/QAsFinTech.pdf).

CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA (2019), *Abogacía Futura 2020: áreas de negocio emergentes* (https://www.congresoabogacia.es/noticia/presentacion-del-informe-abogacia-futura-2020-areas-de-negocio-emergentes-un-mundo-de-oportunidades-por-explorar/).

Olena DEMCHENKO (2018), "CRAB Technology Platforms and CRAB Technology Based Smart Contracts. Benefits, Ways of Application, Legal Challenges and Future Development", *Pécs Journal of International and European Law,* núm. 11, págs. 44-53.

Josias N. DEWEY (2019), "USA", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa).

Conrad DRUZETA, Simon GRANT, Matthew PETERS (2019), "Canada", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/canada).

Mateja DUROVIC, André JANSSEN (2018), "The Formation of Blockchain-based Smart Contracts in the Light of Contract Law", *European Review of Private Law,* vol. 26, núm. 6, págs. 753-771.

Vimal Kumar DWIVEDI, Alex NORTA, (2018), "A Legally Relevant Socio-Technical Language Development for Smart Contracts", *2018 IEEE 3rd International Workshops on Foundations and Applications of Self Systems,* págs. 1-4 (https://ieeexplore.ieee.org/document/8599523).

Marina ECHEBARRÍA SÁENZ (2017), "Contratos electrónicos autoejecutables (smart contract) y pagos con tecnología blockchain", *Revista de Estudios Europeos,* núm. 70, págs. 69-97 (http://www.ree-uva.es/images/numeros/70/2017-70-69-97.pdf).

EU BLOCKCHAIN OBSERVATORY AND FORUM (2019), *Legal and Regulatory framework of blockchains and smart contracts* (https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf?width=1024&height=800&iframe=true).

FINANCIAL TIMES (2019), "Cryptocurrency Visa card could open a back door for dirty money" (https://www.ft.com/content/7b823d04-809b-11e9-9935-ad75bb96c849).

Michèle FINCK (2019), "Smart contracts as a form of solely automated processing under the GDPR", *International Data Privacy Law,* vol. 9, núm. 2, págs. 78-94 (https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz004/5488488).

FINMA (2018), *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs),* págs. 1-11 (https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/).

FORBES (2019), "Secretary-General Says United Nations Must Embrace Blockchain" (https://www.forbes.com/sites/michaeldelcastillo/2019/12/28/secretary-general-says-united-nations-must-embrace-blockchain/#5b2296181379).

Martin FRIES (2018), "Private Law Compliance through Smart Contracts?", *Compliance Elliance Journal,* vol. 4, núm. 1, págs. 11-18.

- (2018), "Smart Contracts: Brauchen schlaue Verträge noch Anwälte?", *Anwaltsblatt,* núm. 2, págs. 86-90.

Joey GARCIA, Jonathan GARCIA (2019), "Gibraltar", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/gibraltar).

Emmanuelle GANNE (2018), *¿Pueden las cadenas de bloques revolucionar el comercio internacional?,* Lausanne, Publicaciones de la OMC.

Jack GILCREST, Arthur CARVALHO (2018), "Smart Contracts: Legal Considerations", *IEEE International Conference on Big Data,* págs. 1-5.

Alfonso GONZÁLEZ GOZALO (2013), "La formación del contrato", en Rodrigo BERCOVITZ RODRÍGUEZ-CANO (Director), Nieves MORALEJO IMBERNÓN, Maria Susana QUICIOS MOLINA (Coordinadores), *Tratado de Contratos,* vol. 1: Concepto, límites, significación, requisitos, formación, forma documentación, interpretación e integración, eficacia e ineficacia del contrato, Valencia, Tirant lo Blanch, págs. 747-840.

Manuel GONZÁLEZ-MENESES (2019), *Entender Blockchain: una introducción a la tecnología de registro distribuido,* Cizur Menor, Aranzadi.

Stefan GRUNDMANN, Philipp HACKER (2017), "Digital Technology as a Challenge to European Contract Law - From the Existing to the Future Architecture", *European Review of Contract Law,* núm. 13, págs. 255-293 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3003885).

Daniel HAEBERLI, Stefan OESTERHELT, S., Alexander WHERLOCK (2019), "Switzerland", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/switzerland).

Teresa HUALDE MANSO (2016), *Del consumidor informado al consumidor real. El futuro del Derecho de Consumo europeo,* Madrid, Dykinson.

Gayle M. HYMAN, Matthew P. DIGESTI, (2017), "New Nevada Legislation recognizes blockchain and smart contracts tecnologies", *Nevada Lawyer,* núm. 25, págs. 13-17 (https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf).

Gary J. JOHNSON, (2017), "Planning the future: blockchain Technology and the Insurance Industry", *In-House Defense Quarterly,* núm. 73, págs. 73-78 (https://www.rbmn.com/wp-content/uploads/2017/10/16J1065-GLJ-BLOCKCHAIN-TECHNOLOGY_.pdf).

Richard KEMP (2018), "Legal Aspects of Artificial Intelligence (v2.0)", *Cyberspace Lawyer NL 2,* vol. 22, núm. 1, págs. 1-48.

Joshua KRUMHOLZ, Ieuan MAHONY (2019), "Blockchain and intellectual property: A case study", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2019,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/4-blockchain-and-intellectual-property-a-case-study).

Karl LARENZ (1963), *Geschäftsgrundlage und Vertragserfüllung: die Bedeutung "Veränderter Umstände" im Zivilrecht,* Berlin-München, C.H. Beck.

Priit LATT (2019), "Estonia", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/estonia).

Antonio LEGERÉN MOLINA (2018), "Los contratos inteligentes en España. La disciplina de los smart contracts", *Revista de Derecho Civil,* vol. V, núm. 2, págs. 193-241.

- (2019), "Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de blockchain", *Revista de Derecho Civil,* vol. VI, núm. 1, págs. 177-237.

Lawrence LESSIG (1999), *Code and Other Laws of Cyberspace,* New York, Basic Books, 1999.

Loi LUU, Duc-Hiep CHU, Hrishi OLICKEL, Prateek SAXENA, *et al.* (2016, "Making Smart Contracts Smarter", en CCS 2016, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security,* New York, ACM, págs. 254-269.

Bridget MARSH, Josias N. DEWEY (2019), "The loan market, blockchain, and smart contracts: the potential for transformative change", en Josias N. DEWEY, (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/03-the-loan-market-blockchain-and-smart-contracts-the-potential-for-transformative-change).

Stephen M. MCJOHN, Ina MCJOHN (2016), "The Commercial Law of Bitcoin and Blockchain Transactions", *Uniform Commercial Code Law Journal,* núm. 16-13, págs. 1-23.

Eliza MIK (2017), "Smart Contracts: Terminology, Technical Limitations and real World Complexity", *Law, Innovation and Technology,* vol. 9, núm. 2, págs. 269-300.

Miguel Ángel MORENO NAVARRETE (1999), *Contratos electrónicos,* Madrid, Marcial Pons.

Reggie O'SHIELDS (2017), "Smart contracts. Legal agreements for the blockchain", *North Carolina Banking Institute,* vol. 21, núm. 1, págs. 177-194.

Emiliano B. OCARIZ (2018), *Blockchain y Smart contracts. La revolución de la confianza,* Madrid, RC Libros.

Mike ORCUTT (2019), "Once hailed as unhackable, blockchains are now getting hacked", *MIT Technology Review* (https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/).

Maria Ángeles PARRA LUCÁN (2015), "Riesgo imprevisible y modificación de los contratos", *InDret,* núm. 4, págs. 1-54 (http://www.indret.com/pdf/1187_es.pdf).

Christophe PERCHET, Juliette LOGET, Stéphane DANIEL (2019), "France", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/france).
Douglas E. PHILLIPS (2009), *The Software License Unveiled: how legislation by License Controls Software Access,* Oxford, Oxford University Press.

Dan PUTERBAUGH (2017), "The future of contracts: automation, blockchain and smart contracts", *The Australian corporate lawyer,* vol. 27, núm. 1, págs. 24-26.

Max RASKIN (2017), "The Law and Legality of Smart Contracts", *Georgetown Law Technology Review,* núm. 305, págs. 1-37.

Raúl ROJAS (2017), "Los Smart Contract o contratos inteligentes en el ámbito laboral", *Revista Byte* (https://ecija.com/wp-content/uploads/2017/05/Los-Smart-Contract-o-contratos-inteligentes-en-el-%C3%A1mbito-laboral.pdf).

Pablo SALVADOR CODERCH (2009), "Alteración de circunstancias en el art. 1213 de la Propuesta de Modernización del Código Civil en materia de obligaciones y contratos", *InDret,* núm. 4, págs. 1-60 (http://www.indret.com/pdf/687_es.pdf).

- (2018), "Contratos inteligentes y derecho del contrato", *InDret,* núm. 3, págs. 1-5 (http://www.indret.com/pdf/editorial__1.pdf).
-

Alexander SAVELYEV (2017), "Contract Law 2.0: "Smart" contracts as the beginning of the end of classic contract law", *Information & Communications Technology Law,* págs. 3-24.

- (2018), "Some risks of tokenization and blockchainizaition of private law", *Computer Law & Security Review,* 34, págs. 863-869.

John SCHINDLER (2017), "FinTech and Financial Innovation: Drivers and Depth", *Finance and Economics Discussion Series 2017-081,* Washington, Board of Governors of the Federal Reserve System, 2017, págs. 1-16.

Jeremy M. SKALAROFF (2017), "Smart Contracts and the Cost of Inflexibility", *University of Pennsylvania Law Review,* vol. 166, págs. 263-303 (https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9605&context=penn_law_review).

Josh STARK (2016), "How Close Are Smart Contracts to Impacting Real-World Law?", *CoinDesk* (https://www.coindesk.com/blockchain-smarts-contracts-real-world-law).

- (2016), "Making sense of Blockchain Smart Contracts" (https://www.coindesk.com/making-sense-smart-contracts).

Vasilisa STRIZH, Dimitry DIMITRIEV, Anastasia KISELEVA (2019), "Russia", en Josias N. DEWEY (Editor), *Blockchain & Cryptocurrency Regulation 2020,* London, Global Legal Insights (https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/russia).

Nick SZABO (1996), "Smart contracts: building blocks for digital markets", *Extropy: The Journal of Transhumanist Thought,* vol. 16 (http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html).

Alexander TAPSCOTT, Don TAPSCOTT (2016), *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world,* New York, Penguin Random House.

Carlos Enrique TUR FAÚNDEZ (2018), *Smart Contracts. Análisis jurídico,* Madrid, Reus.

UNCITRAL (2017), *Modernizing International Trade Law to Support Innovation and Sustainable Development. Proceedings of the Congress of the United Nations Commission on International Trade Law,* Vienna, United Nations (http://www.uncitral.org/pdf/english/congress/17-06783_ebook.pdf).

- (2018), *Legal aspects of smart contracts and artificial intelligence: submission by the Czechia* (http://www.uncitral.org/pdf/english/commissionsessions/51st-session/CN.9-960_CZ_proposal.pdf).

UNIDROIT (2017), *Work Programme for the triennial period 2017-2019* (https://www.unidroit.org/about-unidroit/work-programme).

- (2019), *Draft Triennial Work Programme 2020-2022,* págs. 1-54 (https://www.mpo.cz/assets/cz/zahranicni-obchod/mezinarodni-organizace-a-obchod/uncitral/uncitral-e-commerce/2019/4/cd-98-14-e.pdf).

Aura Esther VILALTA NICUESA (2019), *Smart legal contracts y blockchain. La contratación inteligente a través de la tecnología blockchain,* Madrid, Wolters Kluwer.

Angela WALCH (2018), "In Code(rs) we trust: software developers as fiduciaries in public blockchains", en Georgios DIMITROPOULOS, Stefan EICH, Philipp HACKER, Ioannis LIANOS (Editors), *The Blockchain Revolution: Legal and Policy Challenges,* Oxford, Oxford University Press, págs. 4-27.

Kevin WERBACH, Nicolas CORNELL (2017), "Contracts ex machina", *Duke Law Journal,* núm. 67, págs. 313-382.

Thomas WILHELMSSON (2004), "The Abuse of the "Confident Consumer" as a Justification for EC Consumer Law", *Journal of Consumer Policy,* vol. 27, núm. 3, págs. 317-337.

WORLD ECONOMIC FORUM (2016), "The future of financial infrastructure. An ambitious look at how blockchain can reshape financial services" (http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf).

Rui YUAN, Yu-Bin XIA, Hai-Bo CHEN, Jan XIE, *et al*. (2018), "ShadowEth: Private smart contract on public blockchain", *Journal of Computer Science and Technology,* vol. 33, núm. 3, págs. 542-556.