Revista de Derecho Privado
ISSN: 0123-4366
ISSN: 2346-2442
Universidad Externado de Colombia

PADILLA SÁNCHEZ, JORGE ALBERTO

Blockchain y* contratos inteligentes: aproximación a sus problemáticas y retos jurídicos

Revista de Derecho Privado, núm. 39, 2020, Julio-Diciembre, pp. 175-201
Universidad Externado de Colombia

DOI: https://doi.org/10.18601/01234366.n39.08

Disponible en: https://www.redalyc.org/articulo.oa?id=417564980007

Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos*

Jorge Alberto Padilla Sánchez**

Resumen. El desarrollo de tecnologías *blockchain* ha permitido la creación de nuevas formas de ejecución automática de obligaciones contractuales mediante los mal denominados "contratos inteligentes" (*smart contracts*). Las características propias de la *blockchain*, esto es, su lenguaje de código, la desintermediación, autonomía e inmutabilidad, crean nuevas problemáticas asociadas a la ejecución contractual mediante contratos inteligentes; y al mismo tiempo implican retos para los actores involucrados, así como para los reguladores. El presente artículo tiene como objeto servir de introducción al análisis de las problemáticas asociadas a la tecnología *blockchain* y a los contratos inteligentes.

Palabras clave: *blockchain*, sistemas de registro distribuido, contrato inteligente, ejecución automática, codificación.

* Fecha de recepción: 29 de noviembre de 2019. Fecha de aceptación: 30 de marzo de 2020.
Para citar el artículo: Padilla Sánchez, J. A., "*Blockchain* y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos", *Revista de Derecho Privado*, n.º 39, julio-diciembre 2020, 175-201, doi: https://doi.org/10.18601/01234366.n39.08.

** Universidad Externado de Colombia, Bogotá, Colombia; docente investigador. López Montealegre Asociados & Abogados, Bogotá, Colombia; abogado asociado. Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, Bogotá, Colombia; secretario. Magíster en regulación financiera y bursátil, Georgetown University Law Center, con distinción *Dean's List Honoree*. Abogado, Universidad Externado de Colombia, Bogotá, Colombia. Contacto: jorge.padilla@uexternado.edu.co. Orcid: 0000-0002-0744-8508.

Blockchain and Smart Contracts. Approach to their Legal Problems and Challenges

ABSTRACT. The development of blockchain and distributed ledger technologies has allowed the creation of new forms of self-execution of contractual obligations through the so-called "smart contracts". The characteristics of the blockchain, that is, its code language, disintermediation, autonomy and immutability, create new problems associated with contractual execution through smart contracts; and, at the same time, they imply challenges for the actors involved, as well as for the regulators. The purpose of this article is to introduce the analysis of the problems associated with blockchain and smart contracts.

KEYWORDS: blockchain, distributed ledger techonologies, smart contracts, self-enforcement, contractware.

SUMARIO: Introducción. I. ¿Contratos inteligentes? II. Tecnologías de registro descentralizado (*distributed ledger tecnologies* [DLT]) y *blockchain*. III. La ejecución automática de los contratos inteligentes. IV. Traducción y codificación del lenguaje natural-*contractware*. Conclusiones. Referencias.

Introducción

Vivimos en una sociedad donde la tecnología afecta de manera cada vez más incisiva la forma como nos relacionamos y conectamos con los demás[1]. En efecto, las personas utilizan cada vez más la tecnología para celebrar contratos o realizar transacciones en tiempo real, ya sea el pago de servicios públicos mediante aplicaciones de telefonía móvil, o incluso la inversión en proyectos productivos mediante páginas virtuales[2]. Hoy resulta extraño que una persona vaya físicamente a un banco a hacer una fila para realizar un pago o para abrir una cuenta de ahorros. El panorama de la prestación de servicios financieros ha venido mutando rápidamente, verbigracia ante la presencia de nuevos bancos digitales, plataformas de pago digitales, *robo advisors*, entre otros. Es más: el uso de aplicaciones como *Rappi* permite a los particulares sacar dinero de un cajero automático sin necesidad de salir de la comodidad de su hogar.

1 DE FILIPPI, P. & WRIGHT, A. *Blockchain and the Law. The Rule of Code*. Harvard University Press, 2018, 13.

2 "We are living at a turning point. Day by day, new game-changing technologies are being developed under our eyes at an incredible pace. But how does it differ from the usual development of mankind's history? The answer is that never before did we rely on such efficient tools to create knowledge and support our intelligence. While yesterday the machines served mostly to complete physical tasks, today, we can count on machines and computing to augment our intelligence and even automate our thinking". OLIVER, G. & JACCARD, B. "Smart Contracts and the Role of Law". *Jusletter IT*. Noviembre 2017, vol. 23, 2.

Ahora bien: el uso de la tecnología para satisfacer necesidades humanas no es algo nuevo, incluso para el reino de los contratos. Así, por ejemplo, el ser humano se ha valido de la ayuda de máquinas o instrumentos tecnológicos para la celebración de contratos desde tiempos inmemoriales. Se tienen referencias de la primera máquina dispensadora desde el año 215 a. C., que servía para distribuir agua bendita en los templos egipcios, donde las personas introducían una moneda en un artefacto, y el peso del *token* o moneda activaba la apertura de una puerta, que a su vez activaba una válvula que dispensaba el agua bendita[3]. En últimas, la máquina dispensadora de agua ejecutaba un contrato de compraventa sin la intervención del ser humano en el extremo vendedor. En 1822, el vendedor de libros Richard Carlile inventó la primera máquina dispensadora de libros con el fin de vender libros tales como *La era de la razón* de Thomas Paine, buscando evitar ser perseguido por sedición por la Corona inglesa debido a la venta de material blasfemo[4]. Carlile sostenía que no podría ser perseguido por la venta de libros, comoquiera que el contrato de compraventa era celebrado entre el comprador y una máquina[5]. Sin embargo, el uso de la máquina no impidió su arresto, pues las cortes consideraron que el uso de la máquina servía como un instrumento, pero no suplantaba a Carlile como parte del contrato. En todo caso, el ejemplo es útil en este punto para demostrar la manera como el ser humano se ha valido de máquinas y del uso de herramientas tecnológicas para satisfacer necesidades políticas, económicas e incluso religiosas.

Posteriormente, en 1965, se creó el sistema de intercambio electrónico de datos (en inglés, *electronic data interchange* o EDI) como un mecanismo para enviar mensajes electrónicos con respecto a información de carga entre empresas y sus transportistas[6]. En la actualidad, los sistemas EDI se utilizan para supervisar las cadenas

3 "The first known reference to a vending machine came in 215 B.C. in *Pneumatika*, a book by the Greek mathematician, Hero. In it, he detailed a machine that dispensed holy water for use in Egyptian temples. The user would put a coin in a particular spot, which would trigger a lever that opened a valve that dispensed the water. Fear of divine retribution would combat the use of fake coins". Raskin, M. "The Law and Legality of Smart Contracts". *Georgetown Law Technology Review,* 2017, 1 *Geo. L. Tech. Rev*., 315.

4 "The first book-dispensing vending machine was built by Richard Carlile in England in 1822. Carlile was a bookseller who wanted to sell seditious works like Paine's Age of Reason without being thrown in jail. His answer was a self service machine that allowed customers to buy questionable books without ever coming into contact with Carlile. The customer turned a dial on the devise to the publication he wanted, deposited his money, and the material dropped down in front of him. It's unclear whether this was an automated process, but that didn't stop England's own automated process from convicting one of Carlile's employees for selling 'blasphemous material'". Geoghegan, J., "A Brief History of Book Vending Machines", *The Huffington Post,* 2013, disponible en [www.huffingtonpost.com/john-geoghegan/book-vending-machines_b_2945364.html] [consultado el 12 de agosto de 2018].

5 "Perhaps it will amuse you to be informed that in the new Temple of Reason my publications are sold by Clockwork!! In the shop is the dial on which is written every publication for sale: the purchaser enters and turns the hand of the dial to the publication he wants, when, on depositing his money, the publication drops down before him". Carlile, R., "To the Republicans of the Island of Great Britain", *Republican,* Abril, 1822, n.º 16, vol. v.

6 De Filippi, P. & Wright, A., *cit*., 73.

de suministro en industrias de alimentos, automóviles, etc. Sin embargo, estos sistemas simplemente se limitan a traducir los términos y condiciones de un contrato ya existente a un formato electrónico; no establecen una forma particular de celebrar y ejecutar transacciones comerciales.

Hoy, los acreedores que cuentan con una garantía prendaria o mobiliaria sobre vehículos automotores han empezado a instalar dispositivos denominados "interruptores de arranque" (*starter interrupters*) sobre los vehículos objeto de garantía. Se trata de dispositivos que permiten al acreedor garantizado prevenir que el deudor que haya incumplido con sus obligaciones pueda iniciar el arranque de su vehículo[7]. En efecto, una vez el deudor ha incumplido, el acreedor puede hacer uso del interruptor de arranque inmediatamente e impedir que el deudor haga uso del vehículo automóvil. Como puede verse, es un mecanismo de autoayuda que el acreedor implementa en el objeto de garantía para obstaculizar su uso por parte del deudor en caso de incumplimiento. Ahora bien: el uso de interruptores de arranque por parte de los acreedores ha de privilegiar otro tipo de bienes jurídicos[8]. Así, por ejemplo, los interruptores de arranque no pueden hacer que un vehículo en marcha se apague automáticamente, pues, de lo contrario, podría poner en riesgo la vida de sus ocupantes. Por otro lado, se ha permitido que los deudores tengan un código que permita iniciar el vehículo por una sola vez, incluso si el interruptor de arranque se encuentra en uso, con el fin de que se pueda utilizar el vehículo en caso de emergencia.

Los anteriores son ejemplos de la manera como los desarrollos tecnológicos se articulan con las relaciones contractuales. Se trata de mecanismos de ejecución automática de obligaciones previstas en documentos contractuales, que hacen uso de la tecnología como un mecanismo de autoayuda y evitan la necesidad de acudir al sistema jurisdiccional para la satisfacción de intereses. Así, por ejemplo, los interruptores de arranque tienen como efecto generar presión en los deudores para el cumplimiento de sus obligaciones, pues mientras no lo hagan, no podrán hacer uso de dichos bienes. Pues bien, eso es lo que realiza un *smart contract* o contrato inteligente. Desde ya puede anticiparse que un contrato inteligente es un mecanismo de ejecución automática de obligaciones mediante un código computacional, que pretende reducir la ambigüedad propia de todo contrato y la intervención del juicio humano en su ejecución[9]. Dicho

7 "Starter interrupters are an archetypical example of a smart contract and how the law deals with them is instructive in crafting appropriate legal regimes. A starter interrupter is a device that is installed in an automobile that allows for a remote party to prevent the engine from starting. It allows a user who controls the starter interrupter to remotely shut off an automobile. These devices often also include global position systems, so that the collateral can be located. The New York Times reported on an Arizona company, C. A. G. Acceptance Corporation, which offers its automobile loans on a condition that if the debtor is in default, the company reserves the right use the device to prevent the car from starting. Such devices are estimated to be installed in over two million automobiles". RASKIN, M., *cit*., 330.

8 *Ibid*., 331.

9 "Technology promises to replace slow and imprecise paper institutions with efficient, digitized counterparts. Contract law is a frequent target of these hopes. Though contracts ostensibly provide

mecanismo tiene la potencialidad de simplificar el desarrollo de contratación, reducir costos de transacción al eliminar intermediarios y facilitar la ejecución contractual. El concepto no es nuevo, pero su potencial desarrollo únicamente se hizo latente con la creación de la *blockchain*, esto es, un sistema de registro descentralizado que sirve de ecosistema necesario para la puesta en marcha de los contratos inteligentes.

Con el desarrollo de la tecnología *blockchain* y sus primeras manifestaciones en el mundo contemporáneo, mucho se ha dicho o especulado sobre los contratos inteligentes: desde afirmaciones según las cuales gracias a ellos los abogados dejarán de existir, hasta sus efectos en la reducción de costos de transacción en el interior de las empresas. Para el caso en particular que ahora nos ocupa, debe indicarse que en el siglo xxi los mercados financieros han venido evolucionando a una velocidad increíble gracias a la tecnología, razón por la cual se ha acuñado el término *fintech*, para hacer referencia a cualquier innovación tecnológica en el sector financiero, esto es, el uso de tecnología y programación de computadores para soportar y habilitar servicios financieros[10], incluyendo innovaciones en mecanismos de recaudo de dinero, educación financiera e incluso en criptomonedas (o mejor critpoactivos) como el bitcóin.

En este contexto, el presente artículo tiene como objeto servir de introducción al análisis de las problemáticas asociadas a la tecnología *blockchain* y a los contratos inteligentes. En este punto se describirá qué es un contrato inteligente, cuál es su fundamento o tecnología base sobre la cual opera, y su ejercicio como mecanismo de autoejecución contractual mediante lenguaje de código, así como sus alternativas en materia de regulación y la manera como se ha planteado que el código sirva como ley del contrato. Así las cosas, se analizará el concepto de contrato inteligente o *smart contract*, para lo cual se hace necesario analizar tres de sus elementos más relevantes: esto es, (1) la *blockchain* como tecnología sobre la cual opera; (2) *instantiation*, o la ejecución automática de obligaciones; y (3) *contractware* o, lo que es lo mismo, la traducción del lenguaje natural al lenguaje de código. A lo largo del texto el lector encontrará un análisis de nuevas tecnologías y aplicaciones tecnológicas realizado desde un punto de vista jurídico, sin dejar de lado las explicaciones

relief from the inefficiencies of public law, creating stable and predictable rules with which parties can privately order their affairs, many claim that contract law is broken, and sorely in need of a 'killer app'". Sklaroff, J. M., "Smart Contracts and the Cost of Inflexibility". *University of Pennsylvania Law Review*, 2017, vol. 166, 265.

10 "'Financial technology' or 'FinTech' refers to the use of technology to deliver financial solutions. The term's origin can be traced to the early 1990s and referred to the "Financial Services Technology Consortium", a project initiated by Citigroup to facilitate technological cooperation efforts.1 However, it is only since 20142 that the sector has attracted the focused attention of regulators, industry participants and consumers alike. The term now refers to a large and rapidly growing industry representing between US$12 billion3 and US$197 billion4 in investment as of 2014, depending on whether one considers start-ups (FinTech 3.0) only or the full spectrum of applications, including traditional financial institutions (FinTech 2.0). This rapid growth has attracted greater regulatory scrutiny, which is certainly warranted given the fundamental role FinTech plays in the functioning of finance and its infrastructure". Arner, D. *et al*., "The Evolution of Fintech: A New Post-Crisis Paradigm?", *University of Hong Kong Faculty of Law*, 2015, 3.

técnicas estrictamente necesarias para la debida comprehensión del fenómeno. Para tal efecto se utilizó bibliografía tanto técnica como jurídica.

I. ¿Contratos inteligentes?

En 1996, Nick Szabo, abogado y científico computacional, introdujo por primera vez el concepto de *smart contract*[11]. Con el uso de protocolos criptográficos robustos, Szabo reconoció la posibilidad de escribir *software* de computadores que se asemejaran a cláusulas contractuales, que fueran vinculantes para las partes y que redujeran sus posibilidades de incumplimiento[12]. En este sentido, planteaba que la revolución digital ofrece la posibilidad de crear nuevas instituciones mediante contratos "inteligentes", en el sentido de que son más funcionales que aquellos incorporados en papel[13]. Así mismo, reconocía que el término no involucraba el uso de inteligencia artificial, pero sí el uso de algoritmos computacionales que eventualmente serían utilizados en todo tipo de contratos. Si bien para los años noventa se trataba de una idea novedosa, no se contaba con la tecnología necesaria para su adecuado desarrollo[14]. Fue sólo en el 2008 cuando el desarrollo de la tecnología *blockchain* ofreció la plataforma y el ecosistema necesarios para los contratos inteligentes[15]. Hoy nos encontramos ante, tal vez, la mayor revolución tecnológica desde la aparición del internet; un modelo concebido desde el 2008 y que tiene el potencial de transformar la forma en que vivimos e interactuamos con los demás en todos y cada uno de los ámbitos sociales[16].

11 SZABO, N., "Smart Contracts: Building Block for Digital Markets", *Phonetic Sciences Amsterdam,* 1996, disponible en [www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT-winterschool2006/szabo.best.vwh.net/smart_contracts_2.html] [consultado el 12 de agosto de 2018].

12 SZABO, N., "Formalizing and Securing Relationships on Public Networks", *First Monday 2,* n.° 9, septiembre, 1997.

13 "By extending the logic underlying mechanical devices such as the vending machine, Szabo suggested that the computer code could be used in place of vending machines. This idea could be implemented to negotiate more complex transactions, forging strategic relationships, and coordinating transactions arising under diverse jurisdictions. Instead of transferring the ownership of a can of soda, a Smart Contract could transfer ownership of shares, real estate, intellectual property rights, etc". CORRALES, M. *et al*., "Digital Technologies, Legal Design and the Future of the Legal Profession", en *Legal Tech, Smart Contracts and Blockchain*, Springer Nature, 2019, 5.

14 MENDELSON, M., "From Initial Coin Offerings to Security Tokens: A U. S. Federal Securities Law Analysis", 22 *Stan. Tech. L. Rev*., n.° 52, 2019, 56.

15 "Given that Szabo's paper was written in the mid-1990s, it does not surprise that it portrays courts and legal principles as inconvenient legacies to be made redundant by suitable technologies. Other propositions made therein, such as the use of technology to secure contractual performance or to ensure adherence to the law, have evolved into the theory that 'code is law' and that technology has normative implications. Using technology to enforce the law or private agreement is thus not a novel idea. What is new in the smart contract narrative, however, is the combination of an indiscriminate trust in technology, especially *blockchains*, with an unparalleled misapprehension of basic legal concepts". MIK, E., "Smart Contracts: Terminology, Technical Limitations and Real World Complexity", *Law, Innovations and Technology*, 2017, vol. 9, n.° 2, 273.

16 TAPSCOTT, D. y TAPSCOTT, A., *La revolución blockchain*, Salmerón J. M. (trad.), Barcelona, Ediciones Deusto, 2016, 16.

En este contexto, la definición del término "contrato inteligente" es de suma importancia para el objeto de estudio del presente documento, toda vez que su lectura gramatical puede conducir a error[17]. En efecto, lo primero que le llega a la mente a cualquiera es que se trata de contratos que involucran el uso de inteligencia artificial o de *software* inteligente. Sin embargo, y como se verá a continuación, no son contratos ni son inteligentes. En este punto, debe indicarse que se han formulado varias y diversas definiciones de la figura. Así, hay quienes definen los contratos inteligentes como "sistemas que automáticamente mueven activos digitales según reglas arbitrarias pre-especificadas"[18]. Otros los definen como "acuerdos cuya ejecución es automática" y es "usualmente efectuada a través de un código de computador puesto en funcionamiento que ha traducido la prosa legal en un programa ejecutable"[19].

Por su parte, Nick Szabo se ha pronunciado sobre el particular en varias oportunidades, de la siguiente manera: en 1996, dijo que "un contrato inteligente es un conjunto de promesas especificadas en forma digital, incluyendo los protocolos dentro de los cuales las partes cumplen con estas promesas"[20]; y en 1997 señaló que "Los contratos inteligentes combinan protocolos con interfaces de usuario para formalizar y asegurar las relaciones a través de las redes de computadoras. Los objetivos y principios para el diseño de estos sistemas se derivan de principios legales, teoría económica y teorías de protocolos confiables y seguros"[21]. Se trata de un concepto que refleja la importancia que la sociedad le da a las revoluciones digitales, bajo la asunción de que la tecnología puede remediar todas las falencias de los sistemas no-digitales.

De acuerdo con lo anterior, es razonable concluir que, para los efectos del presente artículo, un contrato inteligente es un *software* que permite ejecutar de manera automática códigos que incorporan obligaciones entre partes acordadas de manera previa y que se encuentran almacenadas en un registro descentralizado, ante la verificación de las condiciones codificadas. El primer comentario que merece el concepto es que no es inteligente en el sentido de que no piensa por sí mismo, como se supone

17 "Arguably, the entire idea of smart contracts may be the result of a series of terminological misunderstandings. At the same time, assuming that in some instances smart contracts are or represent contracts in the legal sense, their practical deployment may raise some interesting issues that transcend the simple question of whether it is technically and legally possible to automate the contracting process". Mik, E., *cit*., 271.

18 Traducción libre del autor. Versión original: "[…] systems which automatically move digital assets according to arbitrary pre-specified rules". Buterin, V., *Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform*, 2015, Mik, E., *cit*., 272.

19 "A smart contract is an agreement whose execution is automated. This automatic execution is often effected through a computer running code that has translated legal prose into an executable program." Raskin, M., *cit*., 309.

20 Traducción libre del autor. Versión original: "A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises". Szabo, N., *cit*., 1.

21 Traducción libre del autor. Versión original: "Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols". Szabo, N., *cit*.

que sí lo haría un abogado. Tal vez algún día la tecnología permita la existencia de contratos que piensen por sí mismos mediante inteligencia artificial. Mientras eso ocurre, los contratos inteligentes se limitan a ser mecanismos de ejecución de códigos de computador. En segundo lugar, el uso del término "contrato" puede generar confusiones: no es un contrato en tanto no es una fuente de obligaciones, sino un mecanismo de ejecución de obligaciones contractuales. En efecto, el término "contrato" es usado de manera informal y a la ligera, lo cual ha generado opiniones según las cuales los contratos inteligentes eliminarán la necesidad de contar con abogados y jueces al garantizar y automatizar la ejecución de contratos.

II. Tecnologías de registro descentralizado (*distributed ledger tecnologies* [DLT]) y *blockchain*

Los contratos inteligentes están previstos para operar en conjunto con la tecnología *blockchain*, precisamente para ejecutar las transacciones que se encuentren en el registro descentralizado; de ahí que sea fundamental realizar un breve análisis sobre dichos registros.

A. Origen de la *blockchain*

Tal vez lo primero en lo que piense el lector al escuchar la palabra *blockchain* sea bitcóin o criptoactivos. En efecto, *blockchain* está asociado con bitcóin, pues es la tecnología que subyace a las transacciones de criptoactivos. Pero no se limita a ello. Por el contrario *blockchain* es una tecnología de registros descentralizados, que opera a través de una cadena de bloques y puede servir para múltiples propósitos, tales como sistemas de pagos, asientos contables, y para el caso que nos ocupa, el desarrollo de contratos inteligentes, entre otros[22]; de ahí que en ciertos casos se prefiera utilizar el concepto de "tecnologías de registro distribuido" o "DLT", por sus siglas en inglés (*distributed ledger technologies*)[23]. En este contexto, debe indicarse que la *blockchain* o DLT es un sistema de registro descentralizado que es validado por

22 "Increasingly, *blockchain*s are recognised as a generic technology that can be deployed for other purposes, such as a payment network, a platform for asset and supply chain management or a technology facilitating recordkeeping.16 There are hundreds (if not thousands) of different *blockchain*s that often significantly diverge from the original bitcoin *blockchain* and share very few of its characteristics". MIK, E., *cit*., 275.

23 "The hallmark of a centralized database is that storage devices are all connected to a common processor, while in a distributed database, they are independent. Write access in a centralized database is tightly controlled; in a distributed database, many actors have writing privileges. As a result, each storage device maintains its own growing list of ordered records, which, if necessary for the sake of efficiency, can be organized in blocks, which explains the name *blockchain* (BC). In a traditional centralized ledger, there is a designated gatekeeper, who collects, verifies and performs the write requests of multiple parties, while in a distributed ledger (DL) these tasks are distributed". LIPTON, A., "Toward a Stable Tokenized Medium of Exchange", BRUMMER, C. (ed,), *Cryptoassets, Legal, Regulatory and Monetary Perspectives*, Oxford, 2019, 97.

pares a través de procedimientos criptográficos, y que provee un récord cronológico y permanente, públicamente visible, de todas las transacciones[24].

El origen del *blockchain* se encuentra ligado al nacimiento de Bitcoin. El protocolo Bitcoin fue creado en 2008 por una persona desconocida cuyo pseudónimo es Satoshi Nakamoto[25]. Nakamoto hacía parte de un movimiento denominado *cypherpunks*, que pretendía sustituir a las autoridades centrales y organizar sistemas donde se protegiera la información personal de las personas a través del anonimato. Nakamoto reaccionó ante el salvamento de las entidades *too big to fail* por parte de los gobiernos en la crisis financiera del 2008. Los gobiernos centrales estaban utilizando los recursos de los particulares para salvar entidades financieras en crisis dentro de un sistema financiero que era inestable[26]. La confianza en los bancos, en general en las entidades financieras, y en los bancos centrales se encontraba minada[27]. Es este el contexto en que Nakamoto propone un sistema que no depende de ninguna autoridad central, como respuesta a las falencias de regulación y de supervisión por parte de los gobiernos. El bitcóin nace como una moneda libre de la autoridad de los gobiernos, con el fin de romper el monopolio de la soberanía monetaria de los estados[28]. En octubre 31 de 2008, Nakamoto publicó un *White paper* denominado "Bitcoin:

24 "And so, in laymen's terms, the *blockchain* can be described as a decentralised, peer-validated crypto-ledger that provides a publicly visible, chronological and permanent record of all prior transactions. It resembles a spreadsheet that anybody can add a row to, but cannot otherwise update or delete anything". Mik, E., *cit*., 275.

25 "At the end of 2008 a paper by the pseudonym Satoshi Nakamoto submitted to the Internet Bitcoin, a system distributed among the nodes of a *peer-to-peer* network, designed to secure electronic payments independently from the conventional transfer schemes, relying on the intervention of a third party guaranteeing that the digitally transferred money has been moved from the sender's bank account to the recipient's". Perugini, M.L. & Dal Checco, P., "Smart Contracts: a Preliminary Evaluation", Università di Bologna, 2015, 7, disponible en [http://ssrn.com/abstract=2729548].

26 "Nakamoto released the Bitcoin network in the middle of the financial crisis, as a reaction to an unstable international banking system. In doing so, he gave birth to a new currency – one controlled not by any government or central bank but only by cryptography or code". De Filippi, P. & Wright, A., *cit*., 205.

27 "Toda esta situación ha producido un importante hartazgo de la población en general minando la confianza en los bancos y en las instituciones. Es ahí donde el Bitcoin ha encontrado terreno abonado para echar raíces y florecer: un sistema que no depende de ningún banco central, que facilita transacciones inmediatas sin posibilidad de que sean limitadas como por ejemplo pudiera hacerse con la retirada de efectivo de los cajeros automáticos y que además sirve como depósito de valor porque incrementa su precio. A pesar de los problemas causados por su enorme volatilidad estos argumentos han resultado suficientemente poderosos para convencer a muchos usuarios de las bondades de dicho sistema". Del Castillo Ionov, R., *Las Initial Coin Offerings (*icos*) y la tokenización de la economía*, Thomson Reuters, Aranzadi, 2018, 22.

28 "The idea of strangers organizing via pseudonyms and trying to coordinate a governance structure is not as unthinkable as one might suppose. The true identity of bitcoin's designer or designers is unknown "Satoshi Nakamoto" is the pseudonym he, she, or they used. Bitcoin was born out of a distrust for authority and driven by a desire for governance by community consensus rather than central authority. Nakamoto seems not to have been a promoter looking to make a quick buck, but rather an idealist looking to break governments' monopoly on currency by offering an alternative to fiat currency". Rodrigues, U. R., "Law and the *Blockchain*", *Iowa Law Review*, vol. 104, 2019, 715.

A Peer-to-Peer Electronic Cash System", en bitcoin.org. Bitcoin fue previsto para operar con base en una tecnología denominada *blockchain*. En efecto, el *blockchain* sirve como libro de registro de las transacciones de bitcóin.

La *blockchain* nació con el propósito de prevenir la duplicación de gastos (*double spending*) de criptoactivos en un sistema sin una autoridad central o intermediario que controlara la emisión y transferencias de dichos activos[29]. La *blockchain* permite solucionar dicho problema sin necesidad de acudir a una autoridad central o intermediario al hacer visibles a todos los interesados la totalidad de las transacciones. En efecto, el registro público de las transacciones hace posible prescindir de una autoridad o intermediario dentro de un sistema de pagos.

B. Operación de los sistemas de registro distribuido

La *blockchain* está compuesta por un grupo de bloques interconectados (de ahí su nombre "cadena de bloques"). Cada bloque contiene una lista de transacciones pasadas, esto es, las transferencias de *tokens* de una persona a otra. Así mismo, los bloques se encuentran identificados con una especie de huella digital denominada *hash*, junto con una marca de tiempo y la identificación (o *hash*) del bloque anterior[30]. Así las cosas, "Mientras que un libro se basa en los números de página para ordenar su contenido interno –lo cual hace posible que cualquier persona pueda armar un libro en el orden apropiado–, la cadena de bloques de Bitcoin depende de los datos almacenados en el encabezado de cada bloque para organizar la base de datos compartida, que incluye un *hash* del bloque anterior y una marca de tiempo, creando una cadena organizada secuencialmente"[31].

Para crear un nuevo bloque es necesario que cada nodo[32], o partícipe, ofrezca una verificación denominada "proof-of-work"[33], que garantiza la integridad y seguridad

29 "Without a central clearinghouse or any other intermediary capable of validating transactions and updating account balances, anyone in possession of a unit of digital cash would have the ability to send funds to two parties simultaneously, creating a 'double spending' problema. For example, if Bob owned $5 worth of digital currency, he could transfer that amount to both Alice and John at the same time, thereby illegitimately spending a total of $10". DE FILIPPI, P. & WRIGHT, A., *cit*., 20.

30 "The 'blocks' on the *blockchain* are the records of the valid transactions across the network, coded with a hash function. Each subsequent block includes the hash of the prior block, linking them together. This 'chains' the blocks together, hence the term *blockchain*. As the number of transactions grows, so does the *blockchain*, which records the time and sequence of each new block". MENDELSON, M., *cit*., 57.

31 Traducción libre del autor. Versión original: "While a book relies on page numbers to order its internal contents – making it possible for anyone to assemble a book in its appropriate order – the Bitcoin *blockchain* depends on data stored in each block´s header to organize the shared database, which includes a *hash* of the previous block and a timestamp, creating a sequentially organized chain". DE FILIPPI, P. & WRIGHT, A., *cit*., 23.

32 "A node is an individual point in a network which, in relationship to other nodes, validates data before adding it to the *blockchain*". CATCHLOVE, P., "Smart Contracts: A New Era of Contract Use", *Independent Research Project*, 2017, LLH473, 3.

33 "As the name implies, the *blockchain* is made of interconnected blocks. Each block contains a list of all prior transactions. The term 'transaction' denotes the transfer of tokens from one account to

del sistema. En efecto, para poder crear un nuevo bloque se debe generar un *hash* a través de un procedimiento matemático complejo encaminado a la solución de un acertijo. A esta operación se le conoce como "mining"[34] o minería[35]. El protocolo ajusta el nivel de dificultad del acertijo dependiendo del número de nodos (o mineros) que participen: cuanto mayor sea el número de partícipes, mayor será la dificultad para crear un *hash* para un bloque. Una vez un minero ha encontrado un *hash* válido, comunica dicha situación a la red de *blockchain*, para que los demás nodos verifiquen que el *hash* cumple con los requisitos del protocolo. Por último, el minero recibe una remuneración como incentivo económico para mantener el esquema en funcionamiento, denominada "block reward". Actualmente se han creado grupos de mineros (*mining pools*), con el propósito de combinar esfuerzos y recursos, y distribuir las recompensas[36].

Se trata, por tanto, de un sistema que opera como una base de datos inalterable, replicada y accesible. Es un registro inalterable, en tanto es garantizado mediante criptografía, lo cual permite la generación de cadenas de datos –o bloques–, en virtud de la cual los bloques sucesivos que se vayan formando requieren incorporar los anteriores, identificados con su correspondiente *hash*. En este sentido, si una persona pretende modificar una transacción registrada en un bloque, terminará por romper la cadena, comoquiera que al realizar la modificación del contenido del bloque, el protocolo inmediatamente creará un nuevo *hash* para identificar al nuevo bloque modificado, que será imposible de vincular a la cadena de bloques posteriores[37].

another. In most contexts, it has a narrow and technical meaning, limited to shifts of tokens between accounts. The creation of each block requires a significant amount of computation ('mining'). To create a block and append it to the *blockchain*, each mining node (*i. e.* participant in the network) must provide a 'proof-of-work' – a piece of data which is computationally difficult to produce but easy for other nodes to verify". Mik, E., *cit*., 276.

34 Hayes, A. & Tasca, P., "*Blockchains* y criptodivisas", *El futuro es Fintech,* Chishti, S. & Barberis, J. (Eds.), Ediciones Deusto, 2016, 248.

35 "Minería: por medio de la minería «se transmiten y confirman las transacciones pendientes a ser incluidas en la cadena de bloques. Este proceso hace cumplir un orden cronológico en la mencionada cadena, protege la neutralidad de la red y permite un acuerdo entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones deberán ser unidas en un bloque que se ajuste a estrictas normas de cifrado y que será verificado por la red, lo que impedirá que cualquier bloque anterior se modifique» (Pacheco Jiménez, 2016, p. 6)". Corredor Higuera, J.A. & Díaz Guzmán, D., "*Blockchain* y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología *Blockchain* en los mercados de crédito de América Latina", *Revista de la Facultad de Derecho* pucp n.º 81, 2018, 412.

36 "These pools largely control the processing of transactions on Bitcoin and Ethereum. As of December 2017, four minning pools controlled over 50 percent of the Bitcoin network and two minning pools controlled more than 50 percent of Ethereum. These pools thus have the power to control the operation of Bitcoin and Ethereum and shape their development". De Filippi, P. & Wright, A., *cit*., p. 25.

37 "Proof of work guessing game is useful not just for ensuring the orderly storage of records in the Bitcoin *blockchain*. This consensus algorithm also prevents people from creating fake transactions or otherwise altering the records stored in the Bitcoin *blockchain*. Because the header of each block incorporates a hash of the preceding block's header, anyone trying to modify the content stored in a block will inevitably break the chain. Even a small alteration will give rise to a new, unique hash tied

Así, para modificar un bloque sin afectar o romper la cadena de bloques el interesado tendría que generar un nuevo *hash* para cada uno de los bloques posteriores de la cadena. Cuantas más transacciones se celebren y registren en la *blockchain*, más difícil será modificar de manera retroactiva un bloque. Así mismo, y teniendo en cuenta que se trata de un registro que se encuentra replicado en todos los participantes[38], ya que opera mediante un protocolo de comunicaciones estándar que se basa en aplicaciones descentralizadas[39], el interesado en modificar un bloque deberá modificar el *hash* de la mayoría de los nodos para validar el cambio[40]. En síntesis, es sumamente difícil, y por lo tanto se volverá extremamente excepcional, que una persona logre modificar o eliminar la información que se encuentre registrada en la *blockchain*: su diseño técnico favorece el *statu quo* y hace a la información resistente al cambio[41].

Así las cosas, la confirmación o validación de la información se establece mediante un consenso[42] distribuido, esto es, la confirmación se realiza cuando la mayoría de los nodos verifica que un bloque determinado ha cumplido con la denominada

to the altered block, and will necessarily trigger a change to the hashes of all subsequent blocks". *Ibid*., 40.

38 "Some advantages of a *blockchain* are that every user could have a copy of a single database, accessible to all (or a *blockchain* can have limited access or require permission, although that could detract from transparency), with records of every single transaction, and transactions can be validated and recorded in minutes. That could provide transparency, make transactions simple and streamlined, and allow anyone who wishes to use the system. For example, if a *blockchain* were used to record ownership of shares of a corporation, buyers and sellers could quite simply settle their transaction with a message to the block chain, without paying an intermediary, without the transaction going through the books of the numerous entities that are now required in settling stock sales, and without delay – the *blockchain* recording will take minutes, where stock sales today take days to finally settle". MCJOHN, S. & MCJOHN, I. "The Commercial Law of Bitcoin and *Blockchain* Transactions", *Legal Studies Research Paper Series*, noviembre, 2017, Suffolk University Law School, Research Paper 16-13, 6.

39 "*Blockchains* operate differently than earlier databases in that they are not centrally maintained. They are collectively managed by a peer-to-peer network comprised of computers (known as 'peers' or 'nodes'), often scattered across the globe. These nodes store exact or nearly exact copies of a *blockchain* and coordinate by using a software protocol that precisely dictates how network participants store information, engage in transactions, and execute software code". DE FILIPPI, P. & WRIGHT, A., *cit*., 2.

40 "The most plausible way to change a record in the Bitcoin *blockchain* would be for a group of attackers to engage in a ´51% attack´ and effectively take over the network so that they can approve transactions at a rate that outpaced the resto f the network." *Ibid*., 25.

41 "Moreover, because of the way cryptographic programming occurs, it is impossible to modify a block once a subsequent block has been added because it would require all of the blocks that come after it to be updated across every node that is connected to the *blockchain*. In this way, the transaction data contained in the individual blocks of the *blockchain* is extremely resilient." CATCHLOVE, P., *cit*., 5.

42 "El consenso en la cadena de bloques es el elemento esencial que define el sistema *blockchain*. Puesto que los participantes del sistema no cuentan con una confianza plena al no conocerse, para tener certeza sobre el cumplimiento de las obligaciones, información sobre cada uno de los miembros y certeza sobre posibles fraudes, se requiere que las partes cuenten con un consenso sobre la existencia, la evolución y el estado de una serie de información compartida (PREUKSCHAT, 2017)". CORREDOR HIGUERA, J.A. & DÍAZ GUZMÁN, D., *cit*., 414.

proof-of-work. En este sentido, la *blockchain* reemplaza la necesidad de confiar en terceros intermediarios o autoridades centrales, por la confianza en la tecnología[43]. Por consiguiente, la inclusión de un contrato inteligente en la *blockchain* eliminaría la necesidad de acudir a un tercero para asegurar su inalterabilidad y su ejecución; a diferencia de modelos que operan bajo la estructura cliente-servidor (*client-server model*), como, por ejemplo, eBay, Uber y Spotify[44]. En este orden de ideas, se trata de un registro accesible a todos los partícipes, donde no hay una autoridad central o un intermediario que confirme la información, lo cual les permite interactuar directamente entre ellas.

La ausencia de una autoridad central implica, además, que se trata de un esquema de naturaleza transnacional en el que los partícipes pueden tener acceso a servicios globales desintermediados. En este contexto, nos encontramos ante un sistema distribuido, en el sentido de que no hay un servidor central o nube donde se encuentre almacenada la información por una autoridad central. Así lo ha indicado Mendelson:

> En el modelo *blockchain*, la red se basa en una arquitectura distribuida entre pares que requiere cálculos o algoritmos de consenso para garantizar que las transacciones en la red *blockchain* se repliquen para que el libro mantenga su integridad. No hay un depósito central de datos ni un procesador central que ejecute los algoritmos. Cualquier persona con acceso a la red *blockchain* verá la misma información[45].

Ello, empero, genera preocupaciones jurisdiccionales, comoquiera que el alcance de la *blockchain* escapa a límites nacionales, de ahí que los gobiernos se encuentren ante un conjunto de retos con respecto a la manera como pueden regularse las operaciones asociadas a aplicaciones de *blockchain*.

Sin embargo, desde ya puede llamarse la atención sobre el hecho de que la *blockchain* es únicamente una base de datos donde se registran transacciones, pero no es una plataforma transaccional[46]. Así mismo, debe resaltarse que la validación de la

43 "As a result, the *blockchain* itself is 'trustless' because it creates and confirms a certain state of affairs and replaces the need to trust third parties with the ability to trust the technology itself. It is interesting to observe that trustlessness lies at the core of all theories that associate *blockchain*s with radical disintermediation." Mik, E., *cit*., 277.

44 De Filippi, P. & Wright, A., *cit*., 35.

45 Traducción libre del autor. Versión original: "In the *blockchain* model, the network is based on a peer-to-peer distributed architecture that requires consensus calculations or algorithms to ensure that the transactions across the *blockchain* network are replicated so that the ledger maintains its integrity. There is no central repository of data and no central processor executing the algorithms. Anyone with access to the *blockchain* network will see the same information." Mendelson, M., *cit*., 57.

46 "The *blockchain* is the output of a computationally intensive process but does not perform any complex computations itself. Apart from a limited number of native scripts, no code executes within the *blockchain*. In fact, its trustlessness derives from the fact that it does not perform any complex computations and accepts extremely limited external inputs. As a result, the original *blockchain* cannot be regarded as a transaction platform – unless the term transaction is interpreted very narrowly, as the movement of tokens between accounts. If the *blockchain* were to become a platform

información de manera alguna implica una validación de los elementos del contrato inteligente que sea incorporado en el registro: la *blockchain* únicamente sirve de prueba de que una transacción ocurrió, pero no tiene la virtualidad de establecer la validez de un contrato[47]. La validez de un contrato, o de su mecanismo de ejecución, depende del contraste que se realice entre circunstancias del mundo real con el ordenamiento jurídico vigente. En efecto, un contrato puede ser registrado de manera adecuada en la *blockchain*, pero al mismo tiempo ser inválido por cuanto, por ejemplo, las partes carecen de capacidad legal para celebrarlo. En suma, la validación que hagan los nodos de las transacciones realizadas no tiene impacto alguno sobre la validez del negocio jurídico que subyace a dichas transacciones.

C. *Blockchain* permitido y no permitido

Dicho lo anterior, en este punto solo resta mencionar que hay dos tipos de *blockchain*: *blockchain* no permitido (*permissionless*) y *blockchain* permitido (*permissioned*). El primero, esto es, el *blockchain* no permitido, se refiere a aquel que se encuentra abierto y es accesible para todas las personas, como por ejemplo Bitcoin y Ethereum[48]. En este tipo de *blockchain*, cualquier persona con acceso a internet puede descargar el *software* correspondiente (*open source software*) y hacer parte de la red, incluso sin revelar su información personal o identidad, y sin solicitar permiso para hacerlo[49]. Se trata de la expresión más pura de un *blockchain*: descentralizado, pseudónimo[50] y accesible a cualquiera. Sin embargo, es aquel que más preocupaciones genera, pues facilita la comisión de actividades de lavado de activos, financiación de terrorismo o, en general, ilícitas.

for more complex types of transactions, it would be necessary to extend its functionalities. This, in turn, would necessitate the addition of protocol layers or scripts on top of it or the creation of a new *blockchain*." MIK, E., *cit*., 278.

47 "Whether a contract has been formed and whether it correctly reflects the parties' agreement are questions of proof that are determined during the process of adjudication. The *blockchain* provides evidence that a transaction occurred: that one or more tokens were transferred from one account to another. It cannot, however, establish its validity in the legal sense." *Ibid*., 279.

48 "Public *blockchain* is *blockchain* in its traditional form evidenced in Bitcoin. The beauty of *blockchain* is that its authority is in the consensus mechanism that sits at its heart; there is neither a single point of control nor an infrastructural centre." CATCHLOVE, P., *cit*., 3.

49 DE FILIPPI, P. & WRIGHT, A., *cit*., 31.

50 "Bitcoin is not an anonymous system. No one's name need be used. But every transfer identifies an account number of the sender and an account number of the recipient. A bitcoin user may have lots of accounts, even using a different one for every transaction. This is often called a pseudonymous system, because every participant is identified by a number, his or her account number. It may be possible to match the account number to a name using other information available online. But matching numbers to names is not necessarily easy. In particular, software used often generates a new account for every transaction. In other payment systems, banks take care of all the details, in return for considerable fees. Many people who use bitcoin avoid these complexities by using an intermediary to handle their accounts and transactions." MCJOHN, S. & MCJOHN, I., *cit*., 6.

Por un lado, comoquiera que se trata de un sistema accesible por cualquier persona, y que se encuentra replicado en cada uno de los nodos o partícipes, nos encontramos frente a una base de datos con información que puede ser utilizada para publicidad, estudios de *big data* e incluso crímenes. Así las cosas, ciertas transacciones que las partes no quieran hacer públicas no podrán llevarse a cabo mediante un sistema *blockchain*. Las operaciones que sean ejecutadas por contratos inteligentes serán registradas sin que sea posible eliminar dicho registro, y dado el pseudoanonimato de las partes, será posible identificar las transacciones con sus titulares, de ahí que nos encontremos ante el lado negativo de la transparencia[51]. En este orden de ideas, los reguladores habrán de encontrar la manera de integrar el derecho al olvido con la inmutabilidad de la *blockchain*.

Como respuesta a los inconvenientes o preocupaciones que pueda llegar a causar el pseudoanonimato propio del *blockchain*, un nuevo tipo de registros descentralizados han venido emergiendo: los *blockchains* permitidos[52]. Se trata de nuevos esquemas donde las características propias del *blockchain* se matizan para mitigar los riesgos asociados a su operación y mejorar su eficiencia. En efecto, en este tipo de *blockchains* el acceso se encuentra limitado. No cualquier persona puede hacer parte de la red, sino que, por el contrario, es necesario que una autoridad central autorice a las partes que participarán en ella. Así las cosas, la autoridad central tendrá conocimiento de la identidad y las características de las personas que interactúan dentro de la red[53]. Sin embargo, en el interior de la red las partes podrán conservar su pseudoanonimato al momento de interactuar entre ellas. Pues bien, estas restricciones de acceso permiten rastrear fácilmente a los responsables de cualquier actividad ilícita que se realice a través de la red.

Además, debe indicarse que los *blockchains* permitidos operan de manera más rápida y ágil que los *blockchains* no permitidos. Comoquiera que los *blockchains* no permitidos son abiertos y accesibles a cualquier persona que se encuentre interesada en hacer parte de la red, el número de intervinientes, o nodos, necesario para llegar a un consenso para validar las transacciones será mayor, de ahí que el proceso de validación sea más demorado; mientras que, por el contrario, en los *blockchains*

51 "Not everyone would like their every stock transaction permanently saved on a freely accessible database. If the database is open to all, that could permit gathering of information for all kinds of purposes (advertising, crime, data mining), the flip side of transparency." *Ibid*., 9.

52 "Consortium *blockchains* have many of the same essential characteristics of public *blockchains*. There is one major difference between public and consortium *blockchains*. A Consortium *blockchain* has an authority structure shared across a pre-selected set of nodes that control the verification of blocks in the chain. Private *blockchains*, however, operate differently through the employment of a centralized structure. Generally, private *blockchains* require a user to be granted permission to add a block to the chain." Catchlove, P., *cit*., 4.

53 "Anonymity on private *blockchains* is not robust. Before being permitted to use a private *blockchain*, permission must be granted by the entity who created it. Private *blockchain* administrators often impose, as a term of use, a requirement on a user to disclose and verify identity. On the issue of anonymity, consortium *blockchains* provide a middle ground between public and private *blockchains*". *Idem*.

permitidos la validación de las transacciones es más rápida, en tanto el número de personas necesario para llegar a un consenso será considerablemente menor[54].

Si bien se trata de dos tipos distintos de *blockchain*, nada obsta para que puedan funcionar de manera articulada y complementaria. Es razonable considerar que los *blockchains* no permitidos puedan ser utilizados como la base sobre la cual operen distintos tipos de *blockchains* permitidos. Así las cosas, el no permitido podría ser utilizado de manera general; mientras que el permitido podría ser utilizado para operar sobre transacciones específicas que requieran o justifiquen un mayor nivel de seguridad[55].

III. La ejecución automática de los contratos inteligentes

Uno de los elementos principales de los contratos inteligentes es su capacidad de autoejecución (*self-enforcement*). Los contratos inteligentes son de ejecución automática en cuanto que automáticamente ejecutan una transacción ante la ocurrencia de eventos definidos de manera previa. Dicha característica pretende evitar que en la ejecución contractual intervenga el hombre, que se presume parcial y poco fiable, al introducir un algoritmo o código que no puede cambiar de opinión y rehusarse al cumplimiento de sus obligaciones[56]. El código es imparcial y objetivo, lo cual garantiza que el contrato se ejecutará al pie de la letra, sin que se puedan presentar alteraciones o modificaciones a su contenido, o circunstancias imprevistas en su ejecución. En este orden de ideas, es razonable considerar que la necesidad de acudir al sistema judicial para solicitar el cumplimiento de obligaciones, si no es eliminada, es altamente reducida.

En este contexto, debe resaltarse que los contratos inteligentes no pueden ser modificados ni detenidos, o, lo que es lo mismo, son inmutables. Una vez se ingrese el código en el registro descentralizado, su protocolo es imparable sin importar los cambios que puedan ocurrir en la realidad. Si bien la inmutabilidad puede resultar atractiva de manera preliminar, se trata de un atributo que puede presentar varios problemas.

54 "Currently, one notable advantage of permissioned *blockchains* is speed. In an open and permissionless network, such as Ethereum and Bitcoin, active nodes need to reach consensus as to the validity of every transaction. These networks can only process transactions every ten minutes in the case of Bitcoin and every twelve seconds in the case of Ethereum, lagging behind modern databases, which store information in milliseconds. Because permissioned *blockchains* tend to be operated by a smaller number of preselected participants, they can implement alternative ways to validate and approve transactions, often in a faster manner." DE FILIPPI, P. & WRIGHT, A., *cit*., 31.

55 *Ibid*., 32.

56 "Smart contracts are useful because they eliminate the possibility of breach, forcing parties to honor their original agreements. This quality reduces the amount of resources each party needs to monitor the other and avoids the high cost of litigation. Thus, smart contracts enable "trustless" transactions, agreements in which parties are secure without a formal legal contract." SKLAROFF, J. M., *cit*., 279.

A. Retos jurídicos propios de la autoejecución

Lo primero que ha de indicarse con respecto a las problemáticas asociadas a la ejecución automática de los contratos es que si el cumplimiento del contrato depende de un código de computador, debe garantizarse que dicho código no contenga errores. Si bien la inmutabilidad del contrato inteligente prescinde de la intervención humana en su ejecución, no elimina la posibilidad de que el código contenga errores de programación (*bugs*)[57]. Así las cosas, es del todo posible que el contrato se ejecute de manera incorrecta debido a un error en su programación, lo cual genera inconvenientes para las partes contractuales, máxime cuando resulta imposible retrotraer la operación o modificarla, incluso si antes de su ejecución se ha identificado el error. En este orden de ideas, resulta oportuno que las partes acuerden en el contrato, y de manera previa, quién asumirá dicho riesgo. En conclusión, incluso si los contratos inteligentes implican la autoejecución de obligaciones contractuales, no por ese hecho garantizan un cumplimiento perfecto de las obligaciones derivadas del contrato.

En segundo lugar, es necesario que el código refleje de manera adecuada la voluntad de las partes. En efecto, quien codifique las condiciones contractuales y las traduzca de un lenguaje natural a un lenguaje de código puede generar resultados que se alejen de la verdadera intención de las partes contratantes. Por un lado, debe recordarse que los contratos inteligentes se traducen en códigos de computadora que no son creados por abogados, sino por ingenieros de sistemas que, probablemente, no tienen formación jurídica, razón por la cual pueden interpretar, y traducir, de manera inadecuada las previsiones contractuales. Por otro lado, es normal que las partes o sus abogados no tengan los conocimientos necesarios y suficientes para verificar que la codificación refleje íntegramente su voluntad.

En tercer lugar, un contrato inmutable requiere que todos los posibles eventos que puedan afectar su desarrollo sean previstos e incorporados en él[58], pues una vez introducido en la *blockchain*, no será posible que el ser humano intervenga o modifique su contenido. Pues bien, en los contratos tradicionales (por oposición a los contratos inteligentes), es normal que las partes modifiquen sus cláusulas para que aquellos puedan ser adaptados a circunstancias externas, tales como cambios en la regulación o económicos. Incluso es normal que las partes toleren incumplimientos no esenciales sin la necesidad de modificar el contrato. En los contratos inteligentes

57 "If, however, self-enforcement is to guarantee performance and if neither subsequent human intervention nor a modification of the smart contract are possible then, logically, its code must be perfect. It is, however, practically impossible to ensure an absence of coding errors ('bugs') because, statistically, each computer program contains such. Perfect performance, implicit in the concept of self-enforcement, may thus be impossible to guarantee." Mik, E., *cit*., 281.

58 "However, parties can never reduce the universe of their agreement to fully-defined terms ex ante. It is impossible to completely predict events that may complicate performance, and even when events or outcomes can be defined ex ante, the parties' potential responses are too complex to model with static contract language." Sklaroff, J. M., *cit*., 279.

las partes no cuentan con dichas posibilidades, razón por la cual se ha considerado que la principal virtud de estos mecanismos de ejecución de contratos puede llegar a convertirse, al mismo tiempo, en uno de sus mayores inconvenientes: "puede entonces argumentarse que los contratos inteligentes son rígidos y pueden fácilmente desconectarse de la realidad transaccional sobre la cual operan porque no es técnicamente posible realizar ajustes"[59]. Dicha rigidez priva a las partes contractuales de la posibilidad de decidir si desean o no cumplir con sus obligaciones contractuales. En efecto, es posible que el cumplimiento de las obligaciones derivadas de un contrato sea mucho más oneroso que su incumplimiento, y las partes decidan incumplir el contrato (*deliberate non-performance*) y asumir las consecuencias. La teoría del incumplimiento eficiente (*efficient breach theory*) establece que para una de las partes de un contrato puede resultar más rentable el incumplimiento de sus obligaciones que su cumplimiento[60], incluso si dicha conducta llega a ser moralmente reprochable[61]. Dicha posibilidad se encuentra proscrita tratándose de contratos inteligentes. En suma, los contratos inteligentes sacrifican la flexibilidad y el dinamismo propio de los contratos, por la inmutabilidad y su autoejecución.

En cuarto lugar, la inflexibilidad de los contratos inteligentes desconoce la realidad de las relaciones comerciales, en donde muchas veces el cumplimiento de las obligaciones de una de las partes se analiza bajo criterios de razonabilidad o buena fe[62]. Se trata de situaciones en las que para las partes puede ser más eficiente evaluar el cumplimiento de obligaciones de manera *ex post* y no de manera *ex ante*. Este tipo

59 Traducción libre del autor. Versión original: "It could thus be argued that smart contracts are rigid and can become easily disconnected from the transactional reality in which they operate because no such adjustments are technically possible". MIK, E., *cit*., 282.

60 "La teoría del incumplimiento eficiente del contrato (en inglés: *efficient breach theory*) es la más conocida y la más criticada en el derecho de contratos estadounidense. Como su nombre lo indica, esta teoría sostiene que es rentable, en términos económicos, que una parte de un contrato incumpla su obligación principal. Por ejemplo, vender un bien o prestar un servicio, si esa misma venta la puede hacer a un tercero a un mejor precio de tal manera que, aun después de compensar a su contraparte por los perjuicios causados, obtenga una utilidad. En ese caso, se dice que el incumplimiento es eficiente desde el punto de vista de Pareto, porque: (1) la víctima recibió una compensación por los perjuicios sufridos que la dejó tan bien como si el contrato se hubiera cumplido (es decir, en una situación de indiferencia entre cumplimiento e incumplimiento); (2) quien incumplió el contrato obtuvo una utilidad aun después de pagar esos perjuicios (es decir, le fue mejor incumpliendo que cumpliendo con sus obligaciones); y (3) el tercero que terminó siendo el beneficiario del bien o servicio inicialmente contratado es quien más valora ese producto, al haber pagado más por él, y por lo tanto, quien le podrá dar un mejor uso productivo." GAVIRIA GIL, J. A., "Sobre la aplicación de la teoría del incumplimiento eficiente de contratos en el derecho colombiano", *Revista Con-texto*, 2015, n.º 44, 38.

61 "If the normative foundation of contract doctrine is promissory morality, then contract law serves to enforce the moral obligation to keep promises. Fried maintained that a contract 'is first of all a promise', and therefore 'the contract must be kept because a promise must be kept'. In his view, the law should enforce contracts because it should respect individuals' moral capacity to bind themselves through their promises. Fried further recognized that 'promissory obligation […] ha[s] its roots in [the] deeper moral soil' of 'trust and respect for persons'. Accordingly, on Fried's view, if the law failed to enforce contracts, it would fail to respect our moral agency and autonomy. Other scholars have similarly found the normative basis of contract in the morality of promising." SELIGMAN, M. A., "Moral Diversity and Efficient Breach", *Michigan Law Review*, vol. 117, n.º 5, 2019.

de parámetros ofrece flexibilidad a las partes para adaptar el cumplimiento de las obligaciones a las vicisitudes de los mercados y a los contextos transaccionales[62], circunstancia que, debido a su estructura condicional, no se permite en los contratos inteligentes. Pues bien, la flexibilidad semántica de la que carecen los contratos inteligentes permite a los interesados contratar en escenarios o situaciones volátiles y evita una negociación innecesaria sobre la totalidad de las posibles eventualidades que puedan presentarse en el curso del desarrollo de la relación negocial, lo cual elevaría los costos de transacción[63]. En suma, la inflexibilidad de los contratos inteligentes destruye la adaptabilidad que requieren los contratos dentro de relaciones contractuales de largo plazo, donde cierto tipo de incertidumbre y ambigüedad ha de ser anticipada y tolerada. No todas las obligaciones pueden ejecutarse mediante contratos inteligentes. En palabras de Mik, "La precisión tiene un costo: la relación contractual se vuelve rígida y determinista, mientras que el aumento en la extensión del contrato inevitablemente conduce a una mayor probabilidad de mal funcionamiento"[64].

En este punto debe recordarse que el hecho de que los contratos inteligentes se encuentren inmersos en una *blockchain* no implica que se encuentren aislados del ordenamiento jurídico. En efecto, si la *blockchain* dejara de funcionar, los contratos seguirían existiendo, simplemente su ejecución debería llevarse a cabo en otro escenario. Los ordenamientos jurídicos deben crear mecanismos para integrar ambos mundos, como, por ejemplo, garantizar la efectividad de medidas cautelares en procesos judiciales que operen sobre actuaciones que han de llevare a cabo en la *blockchain*. En efecto, la autoejecución puede enfrentarse a una multiplicidad de problemas si ella depende de factores que ocurren por fuera del mundo de la *blockchain*, como, por ejemplo, embargos o prendas posesorias.

Por último, vale la pena mencionar que en ciertos casos la ejecución manual de los contratos puede ser recomendable frente a la autoejecución de los contratos inteligentes. En efecto, puede ser oportuno para ambas partes establecer que la ejecución de ciertas obligaciones del contrato sea manual, con el fin de dejar abierta la puerta para poder reequilibrar las prestaciones en aquellos mercados que pueden ser muy volátiles.

62 "Performance standards present further difficulties by creating a logical gap or undefined term in the contract. A term like 'commercial reasonableness' will mean different things to different parties, in different transactions, at different times. As described above, sophisticated parties can use textual tools to imbue standards with meanings that are unique to the contract's specific transactional context." *Ibid*., 293.

63 "This technical sophistication creates the possibility of truly automated contract formation and execution. Paradoxically, it also makes smart contracting more expensive and less efficient than traditional semantic contracts in environments when there is ex post uncertainty, or where parties prefer to avoid drafting highly customized agreements." *Ibid*., 291.

64 Traducción libre del autor. Version original: "[P]recision comes at a cost: the contractual relationship becomes rigid and deterministic, while the increase in the length of the contract inevitably leads to a higher likelihood of malfunction". Mik, E., *cit*., 293.

IV. Traducción y codificación del lenguaje natural-*contractware*

Como se ha puesto de presente, los contratos inteligentes se expresan mediante códigos computacionales inmersos en una *blockchain*. En este sentido, y comoquiera que dicha plataforma tecnológica cuenta con su propio lenguaje, se hace menester que el lenguaje del contrato que se quiera ejecutar mediante un contrato inteligente habrá de ser traducido a lenguaje de código o de programación (*contractware*)[65]. En efecto, es posible que el contrato inteligente se encuentre ligado a un contrato preexistente escrito en lenguaje natural o que, por el contrario, el contrato que se pretende ejecutar haya sido concebido en lenguaje de código.

A. Traducción al lenguaje de código

En efecto, el *iter* de formación del contrato inteligente supone que los términos y condiciones del contrato (que por lo general se acuerdan en lenguaje natural) sean válidos de conformidad con lo previsto en el artículo 1502 del Código Civil colombiano[66]; y que la ejecución de las prestaciones de las partes se realizará mediante un código de computador ante la verificación de la información que la desencadena. Lo anterior lleva consigo la necesidad de que el lenguaje que se traduzca al lenguaje de código sea condicional (*if-then-rules*)[67] o que se encuentre en términos de falso y verdadero[68], pues deben poder ser expresados de manera que un computador sea capaz de leerlos y de ejecutar un comando contra la entrada de la información que lo activa.

En este contexto, el lector podrá intuir desde ya que resulta imposible traducir la totalidad de un documento contractual a un lenguaje de código sin que se comprometa considerablemente su contenido, máxime cuando los codificadores no deberían incidir o influir en los aspectos sustanciales concernientes a las obligaciones que se pretenden ejecutar vía contratos inteligentes. Debe reiterarse que los programadores no tienen una formación jurídica y por lo tanto no entienden el lenguaje jurídico, que

65 "I will define contractware as the physical instantiation of a computer-decipherable contract. The terms of many contracts can be written in programming languages that are communicated to a machine. The reason for this is that performance and enforcement of a contract essentially boils down to conditional statements, which are foundational to computing." RASKIN, M., *cit*., 312.

66 Artículo 1502, Código Civil colombiano: "Para que una persona se obligue a otra por un acto o declaración de voluntad, es necesario: (1) que sea legalmente capaz. (2) que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio. (3) que recaiga sobre un objeto lícito. (4) que tenga una causa lícita. La capacidad legal de una persona consiste en poderse obligar por sí misma, sin el ministerio o la autorización de otra".

67 "In contract law, promises are made in exchange for other promises: if *x* does *this*, *y* will do *this*. Similarly, in smart contracts and in the code that constitutes them, a conditional framework is at their core. In the codification of smart contracts conditional statements are essential. Essentially, code can only do what it is programmed to do." CATCHLOVE, P., *cit*., 8.

68 "Smart contracts are codified using Boolean logic. Boolean logic involves a computation that resolves in a value as either true or false. Simply put, the computer coding does not permit ambiguity, something either does or does not happen, is or is not triggered, as a result of the code." *Idem*.

por lo demás tiene una poca o nula tolerancia a los errores[69]. En efecto, los programadores tienden a leer los contratos bajo la óptica de manifestaciones condicionales o de verdadero y falso, y dejan de lado el hecho de que el lenguaje jurídico muchas veces adquiere sentido por el contexto que lo rodea, razón por la cual la traducción de este al lenguaje de código puede ser compleja[70]. Pues bien, en este tipo de estructuras lingüísticas la limitación expresiva de los signos se exacerba, máxime cuando, por el contrario, en los contratos tradicionales nos encontramos ante una necesidad de espacio para la ambigüedad y para la interpretación. La ambigüedad es el anatema del lenguaje de código. Además, el hecho de que el contrato sea ejecutado mediante contratos inteligentes no elimina la necesidad de interpretar las previsiones contractuales para llenar de contenido las obligaciones de las partes, para lo cual es necesario contar con los conocimientos jurídicos necesarios, de los cuales, se reitera, carecen los programadores.

Los juristas y las partes pueden solucionar la problemática anterior realizando una interpretación *ex ante* y fijando el alcance e interpretación que quien ejecute el *smart contract* debe darles a los términos del contrato[71]. En efecto, es posible que un término sea sujeto a varias interpretaciones, de ahí que se puedan presentar inconvenientes sobre el alcance de los términos al momento de traducir el lenguaje contractual al lenguaje de código.

B. Codificación directa (*direct coding*)

Una alternativa a la codificación del lenguaje natural consiste en escribir el contrato inteligente directamente en lenguaje de código (*direct coding*), sin necesidad de contar desde el inicio con un contrato escrito en lenguaje natural. Se trata de una

69 "Machine learning enthusiasts might have been misled by the relative success of Google Translate or the sensationalistic reports of AI-based systems beating their human opponents at complex games. Approximations seem permissible in automated translations natural languages, where the overall meaning of a sentence can be gleaned from the context. They are intolerable, however, when it comes to legal provisions, which are drafted with meticulous precision and where one single word may give rise to unintended commercial consequences and prolonged disputes. Programmers fail to appreciate the low tolerance for mistakes in legal documents. Moreover, precision seems paramount when the Smart contract is to self-execute and cannot be stopped or amended. If a smart contract is to embody an existing agreement, its translation into code will involve a tedious manual process." Mik, E., *cit*., 288.

70 "With its lengthy sentences, subordinate clauses, nested expressions and references to abstract concepts, legal language may be more difficult to translate into code than 'normal' natural language. It is often suggested that smart contracts necessitate the creation of a custom-built, domain-specific programming language that could capture the nuances of legal text." *Ibid*., 289.

71 "Whoever interprets the contract must be able to decide between the literal and the purposive approach and, in the event of competing interpretations, select the one that is more consistent with business common sense. The interpreting programmer would have to ascertain the meaning that the contract 'would convey to a reasonable person having all the knowledge which would reasonably have been available to the parties in this situation in which they were at the time of the contract." *Ibid*., 290.

alternativa que podría disminuir la ambigüedad del contrato, en tanto el lenguaje de código es binario; y reduciría los errores de traducción, en tanto el contrato sería inteligente desde su concepción. De nuevo nos encontramos ante la necesidad de que los abogados piensen en términos binarios al momento de redactar contratos y de que los programadores comprendan los principios básicos del derecho contractual.

C. Integración con el mundo real y el problema del oráculo

Como ya se ha puesto de presente, los contratos inteligentes son mecanismos de ejecución de obligaciones que operan de manera automática ante la verificación del cumplimiento de una condición. Por ejemplo, si un contrato inteligente se diseña para realizar el pago contra entrega de una mercancía, es necesario que el sistema sepa si efectivamente se realizó la entrega. Una vez tenga certeza de que se realizó la entrega, el contrato inteligente habrá de ejecutarse y proceder al pago; de ahí que se requiera una fuente de información proveniente del mundo real que transmita los datos necesarios, en tiempo real, a la *blockchain*, para que el contrato inteligente pueda ejecutarse. Lo anterior hace necesario que el evento que sirve de catalizador del contrato inteligente se pueda verificar con base en información disponible y que dicha información pueda transmitirse a la *blockchain*.

Para la verificación del cumplimiento de una condición es preciso que la *blockchain* tenga un contacto con el mundo real y una fuente de información para tal efecto, fuente que ha sido denominada *oráculo*[72]. Los oráculos son programas, empresas o incluso personas naturales que transmiten información del mundo real a la *blockchain* para que los contratos inteligentes puedan ejecutarse[73]. De este modo, es posible distinguir entre eventos que ocurren en el interior de la *blockchain* (*on-chain events*) de aquellos eventos que ocurren por fuera de la *blockchain* (*off-chain events*)[74]. Así, por ejemplo, un sistema *blockchain* puede tener información por parte de Bloomberg,

72 "Contracting parties will be able to solve this conundrum by using a so-called "oracle." Oracles are trusted third parties that retrieve off-chain information and then push that information to the *blockchain* at predetermined times. In the foregoing example, the oracle would monitor the daily temperature, determine that the freezing event has occurred and then push that information to the smart contract." LEVI, S. D. & LIPTON, A., "An Introduction to Smart Contracts and Their Potential and Inherent Limitations", disponible en [http://vlex.com/vid/an-introduction-to-smart-781421025] [consultado el 20 de junio de 2019].

73 "Oracles can be individuals or programs that store and transmit information from the outside world, thereby providing a means for *blockchain*-based systems to interact with real-world persons and potentially react to external events." DE FILIPPI, P. & WRIGHT, A., *cit*., 75.

74 "In this context, technical writings distinguish between on-chain and off-chain events. If a particular process, asset or event concerns or occurs in the *blockchain*, it is referred to as 'on-chain'. Only on-chain events are natively visible to the *blockchains*. Such events are few: the passage of time, the addition of blocks (which includes the generation of tokens and the validation of transactions) and the transfer of tokens, which occurs in response to the presentation of private keys (see below). All processes, objects or events in the physical world are 'off-chain'. The *blockchains* cannot 'see' or accept direct input about or from off-chain events." MIK, E., *cit*., 295.

Augur, un banco central, otra *blockchain* o incluso de sensores de temperatura (internet de las cosas), para activar la ejecución de los contratos inteligentes. Solo resta mencionar en este punto que es importante que las partes del contrato inteligente designen de antemano a un oráculo confiable que sirva de fuente de información, y que acuerden también previamente que aceptan de modo irrevocable la información que proporcione dicho tercero.

En efecto, un contrato inteligente diseñado para la compra de acciones de una empresa listada en bolsa que ha de hacerse efectivo ante la baja de su precio de cotización por debajo de un valor determinado requiere obtener dicha información de un oráculo para que la operación pueda llevarse a cabo en tiempo real. Este ejemplo no presenta mayor inconveniente, en tanto se trata de información que es pública y de fácil acceso para el oráculo. Sin embargo, es posible que se presenten situaciones distintas donde haya diferentes fuentes con información divergente, de ahí la importancia de que las partes acuerden de antemano la fuente de información que utilizarán. También es posible que se presenten situaciones en las que no haya información sobre un evento que ocurra por fuera de la *blockchain* o que sea de difícil acceso.

Por otro lado, es posible que las partes de un contrato asignen a un oráculo la verificación de condiciones que escapan el carácter binario de los contratos inteligentes. Así las cosas, las partes podrían ponerse de acuerdo para que un tercero, ajeno a la *blockchain* y al contrato inteligente, determine si las obligaciones de un contrato inteligente se cumplieron de manera razonable, con los mejores esfuerzos o de buena fe, verificación que resulta imposible realizar a la *blockchain*. En este orden de ideas, es posible flexibilizar a los contratos inteligentes, sacrificando su independencia frente al mundo exterior, en tanto el juicio humano volvería a entrar en juego como catalizador de la ejecución de contratos inteligentes. Así, por ejemplo, establecer si un vendedor realizó una entrega de mercancías conforme requiere un examen del contenido de las mercancías para verificar su conformidad con lo dispuesto en el contrato, de ahí que el juicio humano sea necesario.

Por último, es posible que las partes asignen mecanismos de resolución de conflictos por intermedio de terceros, reconociendo a un árbitro como un oráculo[75]. Uno de los principales retos asociados a la tecnología *blockchain* y a los contratos inteligentes es la forma en que se solucionarán las disputas que surjan de ellos. Debido al componente tecnológico que involucran, es recomendable someter dichas controversias a un tribunal de arbitramento, cuyos árbitros deban cumplir con ciertas calificaciones que les permitan contar con los conocimientos necesarios para resolver de la mejor manera las diferencias entre las partes. Pues bien, la designación y la

75 "A further possibility is programming into a smart contract a dispute resolution process whereby two actors who otherwise might not be identified to each other can attempt to resolve their differences *via* digital arbitration or expert determination, with the smart contract code recognizing the agreed third party arbitrator or expert as an oracle for the purposes of implementing a decision concerning the dispute." Bacina, M., "When Two Worlds Collide: Smart Contracts and the Australian Legal System", *Journal of Internet Law*, 2018, vol. 21, n.º 8, 25.

vinculación de dichas partes a la ejecución de los contratos inteligentes se podrían realizar mediante la figura del oráculo, como un tercero que resuelve una controversia y transmite dicha información a la *blockchain*.

Conclusiones

Si bien el uso de la tecnología para satisfacer necesidades humanas no es nuevo, lo cierto es que con el advenimiento de nuevas tecnologías, como *blockchain*, la manera como estamos relacionándonos unos con otros, y por ende, entablando relaciones contractuales, está mutando rápidamente. Así las cosas, es preciso que cualquier debate sobre los contratos inteligentes se base en un sólido entendimiento de lo que es contractual y tecnológicamente posible. En efecto, en la actualidad hay transacciones comerciales cuya complejidad requiere protocolos complejos para que su ejecución pueda materializarse mediante contratos inteligentes. Pues bien, es recomendable el uso de contratos inteligentes para operaciones condicionales de fácil verificación y ejecución. Sin embargo, tratándose de obligaciones complejas, tal vez asociadas a deberes de conductas o criterios de razonabilidad, es recomendable su ejecución manual, comoquiera que en la actualidad no resulta viable su ejecución automática, debido a las dificultades que se pueden presentar en su traducción del lenguaje natural al lenguaje de código. En suma, solo unos contratos pueden expresarse en código y solo unas obligaciones pueden traducirse a lenguaje computacional para su ejecución en sistemas de registro distribuido.

Además, debe indicarse que la rigidez propia de los contratos inteligentes, producto de la inmutabilidad inherente a la *blockchain*, tiene la virtualidad de eliminar la dependencia del ser humano y sustituirla por la "voluntad" del código. Sin embargo, al mismo tiempo priva a las partes de la posibilidad de decidir si desean cumplir o no con las obligaciones contractuales que recaen en ellos; y deja de lado el reconocimiento de que en la realidad se puedan presentar situaciones que hagan necesario modificar las condiciones contractuales. En este sentido, es incierta la manera como los contratos inteligentes se articularán con la teoría de la imprevisión o la teoría del incumplimiento eficiente. Así las cosas, la eliminación del juicio humano y la automatización de la elección pueden evolucionar en una situación en que las partes contratantes pierdan efectivamente la posibilidad de ejercer sus derechos. En suma, la reducción de la ambigüedad puede ser menos atractiva de lo esperado.

Debe indicarse asimismo que una vez los contratos inteligentes involucran el cumplimiento de obligaciones en el mundo real, la operación se vuelve dependiente de entidades externas, lo cual sacrifica los beneficios provenientes de la autonomía de la *blockchain*. En efecto, la presencia del oráculo para verificar que las condiciones y los supuestos de hecho que activan la ejecución de los contratos inteligentes conlleva la necesidad de intervención humana en la introducción de información proveniente del mundo real a la *blockchain*.

Solo resta mencionar que los contratos inteligentes introducen nuevos riesgos a la contratación contemporánea, tales como errores en programación y discrepancias entre la implementación del contrato y la intención de las partes. Por esto los juristas deben propender a la creación de puentes entre los sistemas jurídicos y los sistemas tecnológicos que permitan reducir estos riesgos. Por su parte los reguladores deben aproximarse a esta nueva realidad reconociendo que se trata de protocolos independientes que pueden crear conjuntos de reglas propios, sin perjuicio de que puedan influir en la conducta de los particulares que intervienen en estos esquemas tecnológicos. Así pues, la mejor manera de crear un ambiente de regulación propicio consiste en regular a los intermediarios que participan en dichos sistemas.

Bibliografía

Arner, D. *et al*., "The Evolution of Fintech: A New Post-Crisis Paradigm?", *University of Hong Kong Faculty of Law*, 2015.

Bacina, M., "When Two Worlds Collide: Smart Contracts and the Australian Legal System", *Journal of Internet Law*, 2018, vol. 21, n.º 8.

Buterin, V., *Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform*, 2015.

Carlile, R., "To the Republicans of the Island of Great Britain", *Republican*, abril, 1822, n.º 16. vol. v.

Catchlove, P., "Smart Contracts: A New Era of Contract Use", *Independent Research Project*, 2017, llh473.

Corrales, M. *et al*., "Digital Technologies, Legal Design and the Future of the Legal Profession", Corrales, M. *et al*. (eds.), *Legal Tech, Smart Contracts and Blockchain*, Springer Nature, 2019.

Corredor Higuera, J. A. & Díaz Guzmán, D., "*Blockchain* y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología *Blockchain* en los mercados de crédito de América Latina", *Revista de la Facultad de Derecho* pucp, n.º 81, 2018.

De Filippi, P. & Wright, A., *Blockchain and the Law. The Rule of Code,* Harvard University Press, 2018.

Del Castillo Ionov, R., *Las Initial Coin Offerings (icos) y la tokenización de la economía,* Thomson Reuters, Aranzadi, 2018.

GAVIRIA GIL, J.A., "Sobre la aplicación de la teoría del incumplimiento eficiente de contratos en el derecho colombiano", en *Revista Con-texto*, 2015, n.º 44.

GEOGHEGAN, J., "A Brief History of Book Vending Machines", *The Huffington Post*, 2013, disponible en [www.huffingtonpost.com/john-geoghegan/book-vending-machines_b_2945364.html] [consultado el 12 de agosto de 2018].

HAYES, A. & TASCA, P., "*Blockchains* y criptodivisas", en CHISHTI, S. & BARBERIS, J. (eds.), *El futuro es Fintech*, Ediciones Deusto, 2016.

LEVI, S. D. & LIPTON, A., "An Introduction to Smart Contracts and Their Potential and Inherent Limitations", disponible en [http://vlex.com/vid/an-introduction-to-smart-781421025] [consultado el 20 de junio de 2019].

LIPTON, A., "Toward a Stable Tokenized Medium of Exchange", BRUMMER, C. (ed.), *Cryptoassets. Legal, Regulatory and Monetary Perspectives*, Oxford, 2019.

MCJOHN, S. & MCJOHN, I., "The Commercial Law of Bitcoin and *Blockchain* Transactions", *Legal Studies Research Paper Series*, Suffolk University Law School, Research Paper, 2017, n.º 16-13.

MENDELSON, M., "From Initial Coin Offerings to Security Tokens: A U. S. Federal Securities Law Analysis", 22 *Stan. Tech. L. Rev.*, n.° 52, 2019.

MIK, E., "Smart Contracts: Terminology, Technical Limitations and Real World Complexity", *Law, Innovations and Technology*, 2017, vol. 9, n.º 2.

OLIVER, G. & JACCARD, B., "Smart Contracts and the Role of Law", *Jusletter IT*, 2017, vol. 23.

PERUGINI, M. L. & DAL CHECCO, P., "Smart Contracts: a Preliminary Evaluation", Università di Bologna, 2015, disponible en [http://ssrn.com/abstract=2729548].

RASKIN, M., "The Law and Legality of Smart Contracts", *Georgetown Law Technology Review*, 2017, 1 *Geo. L. Tech. Rev.*

RODRIGUES, U. R., "Law and the *Blockchain*", *Iowa Law Review*, vol. 104, 2019.

SELIGMAN, M. A., "Moral Diversity and Efficient Breach", *Michigan Law Review*, 2019, vol. 117, n.º 5.

Sklaroff, J. M., "Smart Contracts and the Cost of Inflexibility", *University of Pennsylvania Law Review*, 2017, vol. 166.

Szabo, N., "Formalizing and Securing Relationships on Public Networks", *First Monday* 2, 1997, n.º 9.

Szabo, N., "Smart Contracts: Building Block for Digital Markets", *Phonetic Sciences Amsterdam*, 1996, disponible en [www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html] [consultado el 12 de agosto de 2018].

Tapscott, D. & Tapscott, A. *La revolución blockchain*, Salmerón, J. M. (trad.), Barcelona, Ediciones Deusto, 2016.