

---

## CONTRATOS INTELIGENTES Y DERECHO DE LOS CONTRATOS ¿EL PRINCIPIO DEL FIN?\*

Bárbara RACKEVICIUS\*\*

---

Fecha de recepción: 2 de agosto de 2019

Fecha de aprobación: 15 de agosto de 2019

### Resumen

Actualmente hay quienes creen que los contratos inteligentes provocarán un cambio revolucionario en el Derecho Contractual tal y como lo concebimos hoy en día, siendo necesario el desarrollo de un nuevo derecho “inteligente”. ¿Es esto realmente cierto?

El presente trabajo busca analizar los denominados “contratos inteligentes” ejecutados dentro de una cadena de bloques –o *blockchain*–, a la luz del derecho contractual español y argentino, junto con la obtención de un conocimiento preliminar de sus implicancias jurídicas.

¿Constituyen verdaderos contratos? ¿Reemplazarán a los contratos tradicionales? ¿Qué retos jurídicos presenta la tecnología *blockchain* en materia contractual? ¿Son compatibles con las normas de defensa del consumidor?

---

\* El presente trabajo fue evaluado y aprobado por la Universidad de Salamanca en el marco del Curso de Especialización en Contratos y Daños, dirigido por Eugenio Llamas Pombo, año 2019. A los fines de la presente publicación, se agregó una referencia a la legislación vigente en Argentina, que coincide sustancialmente con la de España.

\*\* Abogada por la Universidad de Buenos Aires con orientación en Derecho Tributario, graduada con Diploma de Honor. Posgrado en Finanzas en la Pontificia Universidad Católica Argentina. Especialista en Contratos y Daños por la Universidad de Salamanca. Ayudante docente en la materia "Derecho Aduanero" de la Facultad de Derecho de la Universidad de Buenos Aires. Actualmente cursando la Carrera de Especialización en Derecho Tributario en la Facultad de Derecho de la Universidad de Buenos Aires.

## Palabras clave

Contratos inteligentes – cadena de bloques – ejecución automática – consentimiento – error – forma de los contratos – firma digital – derecho del consumidor –

## SMART CONTRACTS AND CONTRACT LAW. THE BEGGINING OF THE END?

### Abstract

Nowadays, many people believe that smart contracts will cause a revolutionary change in Contract Law as we conceive it today, and that it will be necessary the development of a new “smart” law. Is this really true?

The present paper aims to analyze the smart contracts stored and executed in a blockchain, in the light of Spanish and Argentine contract law, as well as obtain a preliminary knowledge of their legal implications.

Are they real contracts? Will they replace traditional contracts? What legal challenges does blockchain technology present in contractual matters? Are they compatible with consumer defense standards?

### Keywords

Smart contracts – blockchain – automatic execution – consent – error – form of contract – digital signature – consumer law

## I. Introducción

Los denominados “*smart contracts*”, principalmente aquellos almacenados y ejecutados en cadenas de bloques, están revolucionando el mundo jurídico. Actualmente es muy común escuchar a profesionales hablar o escribir al respecto. Sin embargo, muchos no llegan a comprender realmente en qué consisten, mucho menos sus implicancias jurídicas.

Como primera aproximación, podríamos decir que un contrato inteligente es aquel que se ejecuta por sí mismo, automáticamente, sin que medien terceros intervinientes entre las partes.

El origen del término “*smart contract*” se remonta a la década del 90, cuando Nick SZABO (1996) –jurista y experto en criptografía– esbozó su idea por primera vez: un conjunto de promesas, plasmadas en forma digital, con protocolos que controlen su cumplimiento o haciendo que éste sea prohibitivamente costoso.

Para esclarecer su idea, el citado jurista mencionó como ancestro de su novedosa idea un ejemplo de la vida real: las máquinas expendedoras de productos. Alguien selecciona el producto que quiere comprar, deposita el dinero en la máquina y a través de un simple mecanismo, la máquina entrega el cambio y el producto.

Sin embargo, la clásica máquina expendedora no era más que su ancestro. En efecto, lo que Nick SZABO se imaginaba con este tipo de contratos era posibilitar el cumplimiento automático de las cláusulas más comunes (condiciones de pago, garantías e, incluso, la ejecución de ciertas obligaciones), minimizar todo tipo de errores (intencionales o no) y finalmente, disminuir la intervención de terceros. Ello, no solo con el fin de reducir los costos de transacción, de ejecución del contrato, de resolución de conflictos, sino también las pérdidas derivadas de actuaciones fraudulentas.

Ahora bien, cabe preguntarse ¿por qué los bautizó con dicho nombre? ¿Funcionan con inteligencia artificial?

Afortunadamente, desde el primer momento SZABO (1996) aclaró que decidió llamar “inteligentes” a estos contratos por ser mucho más funcionales que los contratos tradicionales, destacando que no requieren del uso de “inteligencia artificial”. Sin embargo, la tecnología existente en ese entonces no había alcanzado el grado de desarrollo necesario para que su idea pudiera ser llevada a cabo.

De hecho, hubo que esperar casi veinte años para poder ver a los *smart contracts* dar sus primeros pasos. Recién en el año 2009, tras la aparición de la criptomoneda *Bitcoin* (en rigor, de la tecnología que subyace a dicha criptomoneda denominada “*blockchain*”–o cadena de bloques, en español–) se volvió a trabajar sobre su idea.

En esta línea, podemos afirmar que existen dos tipos de contratos inteligentes: aquellos que son almacenados, verificados y ejecutados en una cadena de bloques y aquellos que no lo están. La diferencia entre unos y otros es, precisamente, el soporte

donde se verifican (dentro de una cadena de bloques o no), lo que conlleva características y consecuencias diferentes.

El presente trabajo abordará los contratos inteligentes almacenados en cadena de bloques, debido a la trascendencia que –consideramos– tendrán en un futuro.

## II. La tecnología *blockchain*

La tecnología *blockchain* fue desarrollada por Satoshi NAKAMOTO (2008),<sup>1</sup> alrededor del año 2008, para la creación de la criptomoneda *Bitcoin*. Tal como surge de su trabajo "*Bitcoin: a Peer-to-Peer Electronic Cash System*" (NAKAMOTO, 2008), su finalidad era crear una moneda digital basada en una red descentralizada, abierta y pública, capaz de garantizar que una transacción pudiera realizarse eficazmente.

Sin perjuicio de que esta tecnología fue ideada para la creación de *Bitcoin*, gracias a sus particulares características, su uso se ha extendido a otros fines, tales como la creación de registros de datos, procesos electorales y contratos inteligentes.<sup>2</sup>

*Blockchain* nació con la finalidad de mejorar la confianza entre las partes de un negocio, eliminar o minimizar la intervención de terceros y evitar el problema del doble gasto<sup>3</sup>.

Principalmente, la creación del *Blockchain* buscaba sustituir el recurso a las autoridades centrales (por ejemplo, un banco central) como garantía del correcto funcionamiento de las transacciones de los particulares (GÓRRIZ LÓPEZ, 2017).Y lo está consiguiendo.

---

<sup>1</sup> Pseudónimo asignado a la persona o grupo de personas que creó *Bitcoin*. Al día de hoy se desconoce su identidad. Ver DOMINGO (2018).

<sup>2</sup> A modo de ejemplo, cabe señalar el caso de Estonia, uno de los países más avanzados en el uso de la tecnología en distintos ámbitos tales como la salud nacional, sistemas de códigos judiciales, legislativos, de seguridad y comerciales, entre otros. Consultar <https://e-estonia.com/>.

<sup>3</sup> El doble gasto es uno de los principales problemas que presentan los sistemas digitales de pago, y consiste esencialmente en gastar la misma moneda digital más de una vez (debido a la posibilidad de duplicar el archivo digital de la moneda).

Si bien existen tantas definiciones de *Blockchain* como autores, podríamos decir que es una base de datos descentralizada, apoyada en una red entre pares o “*peer to peer*” (P2P), en la que se registran bloques de información relacionados matemáticamente y que son validados mediante un proceso de consenso. De igual forma, se la ha caracterizado como un libro de contabilidad descentralizado y transparente, donde se registran todas las transacciones (DOMINGO, 2018).

Esta red entre pares está formada por un conjunto de ordenadores o “nodos” que se comportan como iguales y se comunican entre sí a través de internet mediante un protocolo (MORALES BARROSO, 2018). Los nodos trabajan de forma colaborativa: se encargan de almacenar, compartir y preservar la información de la base de datos descentralizada que constituye la cadena de bloques.

Se trata de un modelo de confianza distribuida y descentralizada. El concepto de distribución al que nos referimos no alude a dividir y repartir la información en múltiples ordenadores, sino a que todos los nodos poseen una copia sincronizada de la cadena de bloques en su totalidad (MORALES BARROSO, 2018). Así, en lugar de depositar la confianza del funcionamiento del sistema en una autoridad central (como podría ser un banco o un registro público), la confianza se deposita en una red de ordenadores interconectados (nodos) que se encargan de registrar, en forma continua y secuencial, las transacciones que conforman las cadenas.

Los nodos reciben la información de las aplicaciones de los usuarios, es decir las transacciones (que pueden ser una transferencia de fondos, un *smart contract*, etc), luego comprueban estas transacciones mediante un mecanismo de consenso (denominado “*proof of work*”) y, una vez validada la transacción, se inserta en un bloque. Así, se construyen nuevos bloques que se van insertando a la cadena, que luego se envían a los demás nodos (GATES, 2017).

Para que proceda el registro de una transacción es necesario que –al menos– la mitad de los nodos verifiquen que es correcta, es decir, que el titular del activo digital (por ejemplo de una moneda electrónica) es el verdadero propietario, y no ha dispuesto de él con anterioridad (no ha utilizado ya esa moneda). Para verificar esto, los nodos deben resolver un algoritmo matemático y verificar la solución (GÓRRIZ LÓPEZ, 2017).

Asimismo, *blockchain* crea una huella temporal. Cada bloque posee una huella digital del conjunto de transacciones que se almacenan, denominada “*hash*”, que sirve como prueba de su orden cronológico. Los nodos identifican temporalmente cada operación y la vinculan a una anterior. Los bloques se enlazan según un orden cronológico de forma tal

que cada bloque contiene un hash y una referencia al bloque que le ha precedido. En consecuencia, si se modificara algún dato, aunque sea un simple espacio entre caracteres, se obtendría un hash totalmente distinto.

La modificación del *hash* provocaría que la cadena se rompiera ya que, sin perjuicio de que el bloque modificado continúe vinculado con su predecesor (puesto que éste no ha variado), el bloque posterior al que se modificó apuntaría a un bloque inexistente (LAGE SERRANO, 2017).

Esto impide que un bloque pueda ser modificado o insertado entre dos bloques preexistentes (TUR FAÚNDEZ, 2018), logrando que, una vez registrada la información, ésta no pueda manipularse por ningún participante. Es por ello que se califica al sistema de inmutable.

En concordancia con la clasificación más amplia, y sin perjuicio de que existen muchas más, podemos decir que existen *blockchains* públicas y privadas (MORALES BARROSO, 2018). En las cadenas públicas los datos son visibles para todos, cualquiera puede descargar los programas necesarios y constituirse en nodo (pudiendo así enviar transacciones, examinar las existentes, participar del proceso de consenso, etc). Por el contrario, en las cadenas privadas el acceso a los datos y el envío de transacciones está limitado. Para formar parte de ellas se requiere una invitación o permiso, y existen controles que restringen el acceso a la red.

En lo que hace a la seguridad e identidad, cabe mencionar que las transacciones se registran a través de firmas electrónicas asimétricas que contienen claves públicas y privadas. La clave pública es la dirección de un usuario en la cadena de bloques, pero sin develar la identidad de su titular. Ello genera que muchas veces se califique al sistema como anónimo o semi-anónimo. Por otro lado, la clave privada es la contraseña que le da al titular de los activos digitales la posibilidad de acceder y disponer de ellos siendo fundamental su protección, ya que su pérdida supone la pérdida de todos los activos que de ella dependen (MORALES BARROSO, 2018).

La tecnología de cadena de bloques, lejos de ser algo excepcional, existe y se utiliza en el mundo, cada vez con mayor frecuencia y generalidad. Para citar un ejemplo, en nuestro país, el Boletín Oficial de la República Argentina utiliza la plataforma "*Blockchain Federal Argentina*" para asegurar que el contenido de sus ediciones no cambia a través del tiempo. Diariamente, una vez generada la edición electrónica del Boletín Oficial, se genera un hash que resume el contenido de la edición. Dicho hash se utiliza para generar una transacción que se inserta en la cadena de bloques, obteniendo como resultado un recibo

digital. El recibo (disponible en PDF en la página web) permite a los usuarios del Boletín Oficial corroborar en el tiempo las ediciones diarias, verificando el día y la hora en que el documento original fue sellado.<sup>4</sup>

Por otro lado, actualmente se analiza la posibilidad de utilizar la tecnología blockchain para el seguimiento de licitaciones y sistemas de trazabilidad de productos, entre otros.<sup>5</sup>

En el caso de España, resulta obligado mencionar el caso de Alastria,<sup>6</sup> el primer consorcio multisectorial de cadena de bloques español, promovido por diversas empresas e instituciones. Su finalidad es establecer una infraestructura *blockchain*/DLT semipública (tecnologías de registro distribuido –DLT por sus siglas en inglés–), que soporte servicios con eficacia legal en el ámbito español y acorde con la regulación europea (MORALES BARROSO, 2018). Se trata de una red independiente y neutral, sin un modelo de negocios particular: lo que busca, precisamente, es habilitar un espacio digital común para sus miembros, en el que puedan desarrollar sus servicios y productos *blockchain*/DLT conforme al marco legal.

A nivel comunitario, el interés y la esperanza en la tecnología *Blockchain* es mucho más fuerte.

El 01/02/2018 la Comisión de la Unión Europea lanzó el Observatorio y foro *Blockchain* de la Unión Europea, con el objeto de “promover *blockchain* en Europa mediante el mapeo de las iniciativas de *blockchain* existentes, analizar e informar sobre temas importantes de *blockchain*, promover la educación y el intercambio de conocimientos de *blockchain* y realizar eventos para promover el debate y la discusión”.<sup>7</sup>

Con posterioridad, se creó la Asociación Europea de *Blockchain* que ya cuenta con 29 miembros, tanto de la Unión Europea como del Espacio Económico Europeo. Lo que se busca es establecer una infraestructura de servicios de cadena de bloques europea que permita, en el caso del sector público, el intercambio de datos confidenciales en un entorno

---

<sup>4</sup> Boletín Oficial de la República Argentina. Consultado en [<https://www.boletinoficial.gob.ar/#!estatica/certificacionBlockchain>] el 30/07/2019.

<sup>5</sup> Al respecto, ver [<https://bfa.ar/blockchain/smart-contracts>] consultado el 25/07/2019

<sup>6</sup> Alastria. National Blockchain Ecosystem. Consultado en [<https://alastria.io/#1>] el 30/07/2019.

<sup>7</sup> EU Blockchain Observatory and Forum. Comisión Europea. Consultado en [<https://www.eublockchainforum.eu/>] el 30/07/2019.

seguro. A modo de ejemplo, por un lado, esta infraestructura de servicios posibilitará a las autoridades aduaneras intercambiar datos para verificar las declaraciones de importación de bienes y combatir el fraude mediante la certificación notarial de los pagos de fondos de la UE<sup>8</sup>, mientras que, por otro lado, permitirá a los ciudadanos compartir digitalmente los diplomas universitarios fuera del país, sin temer que sus datos se vean comprometidos.

De modo similar, la Comisión Europea ha propuesto un nuevo programa de financiación denominado “Programa Europa Digital”, que se pondrá en marcha en 2021, para apoyar la transformación digital de las sociedades europeas y sus economías.<sup>9</sup>

Finalmente, el pasado 3 de abril se creó la Asociación Internacional de las Aplicaciones *Blockchain* de Confianza o INATBA (por sus siglas inglés)<sup>10</sup> que agrupa a 105 asociaciones del sector público y del sector privado, con la finalidad de desarrollar un marco global más transparente, predecible y de confianza que permita la adopción de *blockchain* y la tecnología DLT de manera masiva y fomente el desarrollo de aplicaciones basadas en esta tecnología (FERNÁNDEZ ESPINOSA, 2019).

Como podemos advertir, la tecnología de cadena de bloques no es algo que esté pasando desapercibido ni mucho menos. En efecto, hay muchas esperanzas y expectativas en su implementación, incluso hay quienes afirman que acabará por implantarse de forma generalizada en la economía digital.

### III. Contratos inteligentes

Actualmente no existe una definición universal de *smart contract*, sino que cada autor, generalmente incidido por su profesión (sea jurista, financista, ingeniero,

---

<sup>8</sup> Discurso del Comisionado de la Economía Digital y Sociedad Mariya Gabriel sobre aplicaciones *blockchain*. Comisión Europea. Bruselas. 3 de abril de 2019. Consultado en [[http://europa.eu/rapid/press-release\\_SPEECH-19-1973\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-19-1973_en.htm)] el 30/07/2019.

<sup>9</sup> Programa Europa Digital: el Consejo acuerda su posición. Comunicado de prensa. 4 de diciembre de 2018. Consultado en [<https://www.consilium.europa.eu/es/press/press-releases/2018/12/04/digital-europe-programme-council-agrees-its-position/>] el 30/07/2019.

<sup>10</sup> International Association for Trusted Blockchain Applications. Consultado en [<https://inatba.org/>] el 30/07/2019.

programador, etc.), lo define con diversas notas características. A modo de ejemplo, se han esbozado las siguientes definiciones:

- “aplicaciones que operan como programas informáticos y se ejecutan a través del mecanismo de la cadena de bloques de forma descentralizada” (MORALES BARROSO, 2018: 59);
- “secuencias de código y datos que se almacenan en una determinada dirección de la cadena de bloques” (TUR FAÚNDEZ, 2018: 51);
- “acuerdos productores de efectos jurídicos cuya peculiaridad esencial es que son «autoejecutables» por estar total o parcialmente recogidos en secuencias de código: la ejecución del contenido no depende de la voluntad de las partes, sino que tiene lugar de manera automática, una vez se dan las condiciones preestablecidas por aquellas” (LEGERÉN MOLINA, 2018: 4);
- “cualquier contrato que se ejecuta por sí mismo automáticamente sin que medien terceros entre los participantes individuales”.<sup>11</sup>

Igualmente, se ha dicho que son piezas de código almacenadas en la cadena de bloques que se ejecutarán automáticamente una vez implementadas, aprovechando así la confianza y la seguridad de la red de la cadena de bloques. Permiten a los usuarios automatizar la lógica empresarial y, por lo tanto, mejorar o rediseñar completamente los procesos y servicios empresariales.<sup>12</sup>

En definitiva, podríamos decir que existen al menos dos concepciones de los *smart contracts*: aquellas que los conciben como secuencias de código o programas informáticos (almacenados, o no, en una cadena de bloques) y las que los conciben como contratos, es decir, acuerdos productores de efectos jurídicos que se ejecutan de forma automática y autónoma.

---

<sup>11</sup> BBVA Research. Smart Contracts: ¿lo último en automatización de la confianza? Situación Economía Digital. Octubre 2015. Consultado en: [[https://www.bbva.com/wp-content/uploads/2015/10/Situacion\\_Ec\\_Digital\\_Oct15\\_Cap1.pdf](https://www.bbva.com/wp-content/uploads/2015/10/Situacion_Ec_Digital_Oct15_Cap1.pdf)] el 30/07/2019.

<sup>12</sup> European Union Blockchain Observatory Forum. Scalability Interoperability and Sustainability of Blockchain. Consultado en [[https://www.eublockchainforum.eu/sites/default/files/reports/report\\_scalability\\_06\\_03\\_2019.pdf?width=1024&height=800&iframe=true](https://www.eublockchainforum.eu/sites/default/files/reports/report_scalability_06_03_2019.pdf?width=1024&height=800&iframe=true)] el 30/07/2019.

En este sentido, encontramos acertada la distinción efectuada por TUR FAÚNDEZ (2018) que denomina “*smart contracts*” a la primera concepción esbozada, y “*smart legal contracts*” a la segunda.

Siguiendo esta línea, un *smart legal contract* existirá siempre y cuando exista un *smart contract* detrás, como instrumento para su ejecución automática.

Hecha la distinción, a lo largo del presente trabajo utilizaremos los términos “*smart contract*” o “contrato inteligente” para referirnos a la segunda acepción esbozada, es decir, aquellos acuerdos productores de efectos jurídicos.

Las principales características de los contratos inteligentes son las siguientes:

- 1) Se crean como un programa informático en donde los términos del acuerdo se establecen en un lenguaje o código informático. Puede suceder que el contrato se formule desde el inicio en dicho lenguaje, o bien, se formalice en un primer momento en un lenguaje natural y luego se traduzca al código específico.
- 2) Son autoejecutables. Las partes definen el objeto del contrato, las distintas acciones posibles y las cláusulas de aplicación. Una vez que se cumplen las condiciones preestablecidas, se ejecutan automáticamente las consecuencias. Estas "condiciones" se plasman bajo una clásica fórmula del tipo *if/then/else*: si se cumple la circunstancia establecida (*if*), entonces se ejecuta determinada acción (*then*); de no cumplirse, se ejecuta otra acción también prevista (*else*) (LEGERÉN MOLINA, 2018).
- 3) Son autónomos. Una vez consensuados los términos del acuerdo y con la puesta en marcha de la fórmula mencionada, los efectos del contrato se producen sin intervención de las partes ni de terceros.
- 4) El rol de los oráculos. En muchas ocasiones, la información relevante en un contrato inteligente se encuentra fuera de la cadena de bloques, como por ejemplo horarios de vuelos, resultados deportivos, cambios de precios, cotizaciones de divisas, temperatura, etc. La función de los oráculos es, precisamente, conectar dicha información con la cadena de bloques (MORALES BARROSO, 2018). De esta forma, actúan como una base de datos externa a la cadena pero en un lenguaje compatible con ésta, que le brinda información.

A fin de entender acabadamente lo expuesto hasta el momento, a continuación mencionaremos algunos casos de *Blockchain*:

El primero de ellos es HireGo, una aplicación destinada al alquiler de vehículos privados mediante contratos inteligentes y tecnología *blockchain*. Las listas de automóviles, las transacciones de alquiler, el pago y su revisión se realizan a través del *blockchain* de Ethereum (una plataforma descentralizada basada en tecnología de cadena de bloques que permite la creación de *smart contracts*). Las aplicaciones HireGo proporcionan un enlace para acceder a estos datos de una manera fácil, sin necesidad de conocimiento sobre esta tecnología por parte del usuario. Así, cuando un usuario acepta un contrato de alquiler, la aplicación crea un contrato inteligente en nombre del usuario, analiza las respuestas e interactúa con el sistema utilizando un protocolo predefinido y público.<sup>13</sup> Sin embargo, son los usuarios los únicos que tienen el control de sus claves privadas que, en ningún momento, son transferidas a terceros (ni tampoco a HireGo).

Asimismo, la visión a futuro de HireGo es aprovechar dentro de su estructura de negocio, la tecnología de *Internet of Things* (concepto de conectar casi cualquier dispositivo eléctrico a internet y entre sí, en este caso los vehículos–“IoT”–). De esta forma, recibido el pago por parte del usuario, se abrirá automáticamente el vehículo y su acceso se bloqueará una vez finalizado el plazo preestablecido de alquiler (eliminando la necesidad de ir a la agencia de alquiler para firmar el contrato y recoger/devolver las llaves del automóvil).

Otro ejemplo lo encontramos en la compañía aseguradora francesa AXA, que ofrece seguros por retraso o cancelación de vuelo basados en la tecnología *blockchain*. El consumidor contrata el seguro mediante la plataforma Fizzy, dando origen a un *smart contract* conectado a bases de datos globales de tráfico aéreo (oráculos). De existir un retraso de más de dos horas en el vuelo, el contrato se ejecuta automáticamente: el consumidor, sin necesidad de reclamo ni acción alguna, recibe una compensación económica en su cuenta.<sup>14</sup>

Fizzy también funciona con la red Ethereum y brinda a los usuarios la dirección del *smart contract* para que cualquiera pueda acceder a él.<sup>15</sup>

---

<sup>13</sup> HireGo Blockchain P2P car hire. Whitepaper. Enero 2018. Consultado en [[https://www.hirego.io/lib/HireGo\\_Whitepaper-es.pdf](https://www.hirego.io/lib/HireGo_Whitepaper-es.pdf)] el 30/07/2019.

<sup>14</sup> A fin de entender adecuadamente su funcionamiento, recomendamos ver el video consultado en [https://www.youtube.com/watch?time\\_continue=92&v=xJZulZ\\_-CMI](https://www.youtube.com/watch?time_continue=92&v=xJZulZ_-CMI) el 25/07/2019.

<sup>15</sup> En la misma página web se indica que la dirección del *smart contract* de Ethereum es la siguiente: `0xe083515d1541f2a9fd0ca03f189f5d321c73b872`. Consultado en [<https://fizzy.axa/en-gb/faq>] el 30/07/2019.

### III.1. ¿Son los smart contracts verdaderos contratos?

Establecido el concepto de contrato inteligente y explicada la tecnología subyacente, cabe preguntarse: ¿Son los *smart contracts* verdaderos contratos? ¿Resulta de aplicación la normativa vigente, o es necesario el desarrollo de una nueva teoría general de los contratos?

La expresión *smart contract* puede confundir dado que en verdad no todos constituyen verdaderos contratos.

En tal sentido, consideramos que para que un *smart contract* pueda ser calificado como un verdadero contrato es necesario que cumpla los requisitos que el derecho aplicable exige a tal fin. Por el contrario, si no reúne tales requisitos, no será considerado un “contrato”, sin perjuicio de las consecuencias que pueda ocasionar.

Ahora bien, ¿Cuál es la legislación aplicable? ¿Existe hoy en día?

Al estudiar los contratos inteligentes en el presente y siguientes acápite pondremos el foco de análisis particularmente en el caso del ordenamiento jurídico español, ello no sólo porque a él se remiten en numerosas oportunidades los fundamentos del anteproyecto del Código Civil y Comercial argentino, sino también por encontrarse inmerso en el marco de la legislación europea que lleva la vanguardia en las temáticas tecnológicas.

En este punto merece la pena aclarar que si bien actualmente no existe en España una legislación específica sobre contratos inteligentes, el régimen legal vigente en el mencionado país resulta suficiente para otorgarle un marco jurídico a esta novedosa figura. En efecto, las normas actuales brindan los elementos básicos necesarios para determinar si un contrato inteligente puede tener validez jurídica y capacidad suficiente para ser legalmente exigible. Ello, pues consideramos que los contratos inteligentes son, a fin de cuentas, contratos electrónicos.

En tal sentido, la ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (“LSSICE”) define al contrato electrónico como “*todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones*”.

La particularidad de los contratos electrónicos es que tanto la oferta como la aceptación se transmiten mediante dispositivos electrónicos. Y ello es lo que sucede, precisamente, en los llamados contratos inteligentes.

El hecho de que sean redactados en código informático no plantea mayores problemas puesto que rige el principio de libertad de forma para los contratos –artículo 1278 del Código Civil Español (CC) y artículo 51 del Código de Comercio (CCo)–. Por otro lado, si bien su ejecución automática y autónoma presenta ciertas particularidades y consecuencias, ello no es más que una característica del contrato que no incide en su naturaleza contractual, máxime considerando que en el derecho español rige el principio de libertad contractual (artículo 1255 CC).

Consideramos entonces que los *smart contracts* no constituyen una categoría contractual autónoma. Primero son contratos, luego electrónicos (ARIAS POU, 2006) y finalmente, inteligentes. Por otro lado, al regir el principio de “inalteración del derecho preexistente de obligaciones y contratos”, los elementos esenciales del contrato y la tipología contractual no se alteran porque la voluntad comercial se manifieste por medios electrónicos, ni por tener una ejecución automática y autónoma.

En este sentido, el artículo 23.1 de la LSSICE establece: *“los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurren el consentimiento y los demás requisitos necesarios para su validez. Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial”*. Resulta también de aplicación el artículo 3 de la Ley 59/2003 de Firma Electrónica que establece que *“la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel”*.

Finalmente, resulta relevante la ley 7/1998 sobre Condiciones Generales de la Contratación, la Ley general para la Defensa de los Consumidores y Usuarios aprobada por el Real Decreto Legislativo N° 1/2007 y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (“LOPD”), la cual cobra especial relevancia por las particularidades de la tecnología de cadena de bloques.

En otras palabras, para que un contrato inteligente pueda ser considerado como un verdadero contrato en los términos establecidos en el artículo 954 y cdtes. del CC, será necesario analizar, en primer lugar, si el conjunto de líneas de código que conforman el *smart contract* cumple con los requisitos establecidos por el artículo 1261 (consentimiento de los contratantes, objeto y causa) o si, por el contrario, tan solo se limita a establecer la ejecución de una determinada cláusula. En esta línea, podrían verificarse distintos escenarios (NAVARRO DE ANDRÉS, 2018):

- 1) Que el *smart contract* sea tan solo un programa o software que ejecuta instrucciones determinadas, sin conexión con una relación contractual;
- 2) Que el *smart contract* refleje un contrato celebrado previamente en otro soporte (por ejemplo, en papel), que luego es plasmado en código informático;
- 3) Que el *smart contract* sea un contrato redactado y concluido exclusivamente en código informático.

Son solamente los últimos dos escenarios los que –entendemos– pueden dar lugar a la existencia de un verdadero contrato, siempre que se verifiquen los requisitos mencionados precedentemente. En esos casos, al suscribir el *smart contract*, las partes son conscientes que suscriben un acuerdo de ejecución irreversible (siempre que sean capaces y no concurren vicios). Será un acuerdo elaborado en código informático pero que, no por ello, deja de recoger sus intenciones, tanto de constitución de derechos como de obligaciones.

Sin embargo, el hecho de que consideremos a los *smart contracts* como contratos electrónicos no significa que no sea necesario un análisis jurídico más profundo. Las particularidades de esta figura, junto con las de la tecnología *blockchain*, provocan un sinnúmero de interrogantes: ¿Cómo se verifica la capacidad jurídica de las partes, siendo que la tecnología de cadena de bloques no requiere identificación? ¿Cómo se verifica la correcta comprensión del contenido del contrato, si el mismo está redactado en código informático? ¿Cómo prestan las partes su consentimiento? ¿Es posible cumplir con las obligaciones pre y post contractuales de información, principalmente en el ámbito de los contratos de consumo?

### III.2. Consentimiento, objeto y causa en los contratos inteligentes.

Tal como vimos, un *smart contract* debe cumplir con las exigencias básicas del derecho de contratos: consentimiento de los contratantes, objeto y causa.

El objeto y la causa no plantean mayores inconvenientes. El objeto debe ser cierto (artículo 1261 CC), determinado (artículo 1273 CC), recaer sobre cosas posibles (actuales o futuras) que estén dentro del comercio, o sobre servicios que no sean contrarios a las leyes o a las buenas costumbres (artículo 1271 CC). De igual forma, la causa debe ser lícita (artículo 1275 CC). Todo ello puede darse perfectamente en un contrato inteligente.

Sin duda alguna, es el consentimiento el que plantea los mayores inconvenientes.

En primer lugar, el artículo 1262 CC dispone que “*en los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación*” (regulado en el mismo sentido en el artículo 54 del CCO). Si bien pueden generarse ciertas dudas por no existir, en algunos contratos inteligentes, declaraciones de voluntad expresas, el derecho español también admite la aceptación tácita, es decir, la realizada mediante actos concluyentes e inequívocos (GÓRRIZ LÓPEZ, 2017). A modo de ejemplo, el simple envío de dinero a los fines de obtener un determinado producto o servicio puede ser suficiente para originar una aceptación. Asimismo, el sellado de tiempo de la propia cadena de bloques resultaría prueba incuestionable del momento de la prestación del consentimiento.

Expuesto lo anterior, resulta necesario aludir a la etapa de formación del contrato.

Tradicionalmente se han distinguido tres etapas: una primera de generación del contrato, que comprende las negociaciones o acciones llevadas a cabo por las partes para alcanzar el acuerdo; una segunda etapa de perfección, donde tiene lugar el consentimiento de ambas partes; y una tercera etapa de ejecución o consumación del contrato, donde tienen lugar las contraprestaciones.

En los contratos tradicionales, las partes manifiestan su consentimiento en la segunda etapa, sin perjuicio de lo cual, en la tercera etapa deben realizar los actos necesarios para cumplir con las obligaciones emergentes del contrato. De alguna forma, “refuerzan” su acuerdo de cumplir con lo pactado. Sin embargo, ello no sucede en los contratos inteligentes.

La ejecución del contrato inteligente tiene lugar de forma automática y autónoma, sin necesidad de intervención de las partes. Es el propio *smart contract* el que, al verificar las condiciones preestablecidas, ejecuta el contrato. Es por ello que la segunda etapa cobra mayor relevancia, puesto que será necesaria la concurrencia de un doble consentimiento simultáneo: el habitual consentimiento que da lugar a la perfección del contrato, y además, un segundo consentimiento sobre la consumación automática del mismo (TUR FAÚNDEZ, 2018). Las partes deben aceptar y ser conscientes de que la ejecución será realizada automáticamente, sin su intervención (aunque, claro está, en los términos pactados por ellas).

Otro interrogante que se plantea es el de la capacidad de contratar. El derecho español la establece de forma negativa, al disponer, en el artículo 1263 CC, que no pueden prestar consentimiento los menores no emancipados ni quienes tienen su capacidad modificada judicialmente. Así, la necesidad de identificación se encuentra directamente vinculada con los requisitos para contratar válidamente.

El problema se genera en los contratos inteligentes almacenados en cadenas de bloques, principalmente públicas. Tal como mencionamos, las transacciones se registran a través de firmas electrónicas asimétricas, que contienen claves públicas y privadas, en donde la clave pública no contiene la identidad de su titular, sino un pseudónimo. En tal sentido, al desconocer la identidad del contratante, pueden generarse dudas sobre su capacidad (GÓRRIZ LÓPEZ, 2017).

Un claro ejemplo es el de Ethereum, una de las plataformas más importantes para crear, ejecutar y almacenar *smart contracts*, pero que presenta el inconveniente de que resulta imposible saber la identidad de los contratantes. En efecto, solo se puede acceder a la cadena alfanumérica identificativa de la cuenta del titular, pero de ninguna forma acceder a su identidad (DUROVIC y JANSSEN, 2018). Si a ello le sumamos que cualquier persona puede abrir una cuenta a su nombre, sin necesidad de corroborar previamente su identidad, es muy probable que existan casos de contratos celebrados por personas sin capacidad para contratar, pudiendo provocar la nulidad del contrato.

Una solución podría ser que se requiera obtener obligatoriamente una identidad digital para contratar. En efecto, resultaría necesario que el usuario asocie sus datos personales (nombre, apellido, D.N.I.) con su usuario digital, lo que podría realizarse mediante la remisión a un tercero de confianza, o mediante mecanismos criptográficos. Ello, teniendo en consideración los requisitos establecidos por el Reglamento e-IDAS N°910/2014 del 23 de julio de 2014, del Parlamento Europeo y del Consejo para la identificación electrónica y los prestadores cualificados de servicios de confianza.

En esta línea, Italia aprobó recientemente una reforma de ley que define las tecnologías de registro distribuido y contratos inteligentes y les otorga fuerza legal.<sup>16</sup> Un aspecto destacable de la norma es que especifica que la memorización de un documento electrónico mediante el uso de tecnologías basadas en registros distribuidos produce los efectos legales de la validación electrónica de tiempo a que se refiere el artículo 41 del Reglamento e-IDAS N° 910/2014 (es decir, gozará de presunción de exactitud de la fecha y hora que indica, de la integridad de los datos a los que la fecha y hora estén vinculadas y deberá ser reconocido por todos los Estados miembros).

---

<sup>16</sup> Senato della Repubblica. Modifica n. 8.0.3 al DDL n. 989. Consultado en [<http://www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Emendc&leg=18&id=1096791&idoggetto=1095835>] el 30/07/2019.

Si bien no puede desconocerse que la verificación de la identidad de los contratantes es un problema real en materia de contratos inteligentes, han surgido diversos proyectos que buscan solucionar esta situación. A modo de ejemplo puede citarse el caso de Uport,<sup>17</sup> una aplicación que permite a sus usuarios registrar su identidad en Ethereum, firmar transacciones, enviar y solicitar credenciales, etc.

Sin embargo, el ámbito de aplicación de UPort excede los contratos inteligentes, puesto que apunta, ni más ni menos, a la “identidad digital”. En esta línea, la ciudad suiza de Zug creó un sistema de identidad electrónica utilizando Ethereum (mediante UPort), que permite a los ciudadanos registrar sus datos personales a través de la *app* móvil, datos que luego deben ser validados por la administración del cantón. Una vez validados los datos, se crea una identidad digital, que permite a los usuarios acceder a servicios municipales y ejercer sus derechos como ciudadanos (ALLEN, 2018). De hecho, entre el 25 de junio y el 1 de julio de 2018 tuvo lugar la primera prueba de voto electrónico basada en dicha tecnología, la cual no sólo se realizó con éxito, sino que tuvo una amplia aceptación por parte de la población.<sup>18</sup>

Finalmente, con el desarrollo del IoT, muchos expertos sostienen que los dispositivos van a poder contratar entre sí, lo que genera incertidumbre sobre la existencia de la voluntad de las partes (GÓRRIZ LÓPEZ, 2017). En efecto, se trata de los denominados “contratos M2M” (*machine to machine*), que tendrían lugar cuando las cláusulas preestablecidas en un *smart contract* (formulado entre personas) habilita a los distintos dispositivos objeto de dicho contrato a concluir nuevos contratos inteligentes, si se cumplen determinados requisitos previstos (LEGERÉN MOLINA, 2018).

El problema se plantea debido a que el consentimiento únicamente puede ser otorgado por personas. Si bien su análisis excede el marco del presente trabajo, cabe destacar la opinión de LEGERÉN MOLINA (2018) quien sostiene que este problema podría solucionarse acudiendo a un “precontrato”. El citado autor sostiene que cuando las partes aceptan el contenido de un acuerdo están dando su consentimiento por adelantado a los futuros contratos que automáticamente se vayan a concluir. Asimismo, también se ha sostenido que habría que apuntar, como parte y como responsable, al propietario del

---

<sup>17</sup> UPort. Disponible en [<https://www.uport.me/>].

<sup>18</sup> El informe sobre la primera votación basada en *blockchain* de Suiza revela que los ciudadanos quieren que se realicen más votaciones electrónicas. Comunicado de prensa. 30 de noviembre de 2018. Consultado en [<https://www.luxoft.com/pr/report-on-switzerlands-first-blockchainbased-vote-reveals-citizens-want-more-evoting/>] el 30/07/2019.

dispositivo, puesto que es quien lo ha configurado (o ha encargado su configuración a un programador que actuó bajo sus instrucciones) para poder realizar los contratos necesarios (GÓRRIZ LÓPEZ, 2017).

En conclusión, si bien la identidad de los contratantes puede generar hoy en día inconvenientes, el avance de la identidad digital es una solución más que prometedora.

### III.3. El error como vicio del consentimiento

El artículo 1265 CC establece que “*será nulo el consentimiento prestado por error, violencia, intimidación o dolo*”. A su vez, el artículo 1266 CC prevé: “*Para que el error invalide el consentimiento, deberá recaer sobre la sustancia de la cosa que fuere objeto del contrato, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo. El error sobre la persona sólo invalidará el contrato cuando la consideración a ella hubiere sido la causa principal del mismo (...)*”.

Asimismo, para que el error actúe como vicio del consentimiento debe ser esencial, excusable (es decir, no imputable a quien lo sufre) y debe existir un nexo causal entre el error sufrido y la celebración del contrato.

En primer lugar, cabe analizar aquellos casos en los que existe vicio en el consentimiento prestado como consecuencia del error en la persona con la que se contrata. Tal como vimos precedentemente, no es obligatorio registrar la identidad de quien contrata en Ethereum, sino que cualquier persona puede abrir una cuenta y operar bajo un pseudónimo. En este supuesto, consideramos que cabría el error como vicio del consentimiento únicamente en aquellos contratos *intuitu personae*, es decir, aquellos que fueron celebrados teniendo en consideración a la contraparte, por sus cualidades o habilidades personales. Sin perjuicio de ello, el consentimiento prestado por aquel que se hace pasar por otro, usurpando una identidad (casos de *hackers* por ejemplo) es un contrato radicalmente nulo (SALMERÓN MANZANO, 2018).

Otro problema vinculado con el consentimiento se da respecto de la correcta comprensión sobre lo que se está contratando. Al respecto, la Real Academia Española establece que el consentimiento en los contratos es la “*conformidad que **sobre su contenido expresan las partes***” (el destacado es propio). Sin embargo, en la mayoría de los casos las partes no sabrán leer ni comprenderán el código en el cual se escribe el contrato.

En este punto es necesario diferenciar aquellos casos en los cuales existe un error vicio, de aquellos en los que existe un error obstativo.

En relación con el error vicio, debe tenerse en cuenta la reiterada jurisprudencia del Supremo Tribunal de Justicia, que si bien refiere al consentimiento en contratos de SWAP resulta aplicable a estos contratos. Dicho tribunal ha fallado que *“hay error vicio cuando la voluntad del contratante se forma a partir de una creencia inexacta, cuando la representación mental que sirve de presupuesto para la realización del contrato es equivocada o errónea. Es necesario que la representación equivocada merezca esa consideración, lo que exige que la equivocación se muestre, para quien afirma haber errado, como suficientemente segura y no como una mera posibilidad dependiente de la concurrencia de inciertas circunstancias”*.<sup>19</sup>

Sobre el error obstativo, resulta clara la siguiente sentencia del mismo tribunal: *“El error obstativo es un caso de falta de coincidencia entre voluntad y declaración, en el negocio jurídico, con la característica de que tal desacuerdo es inconsciente y, como consecuencia, excluye la voluntad interna real y hace que el negocio jurídico sea inexistente”*.<sup>20</sup> Más recientemente, sostuvo *“Se puede precisar que en el error vicio aparece errónea la voluntad y en el error obstativo, lo erróneo es la declaración, divergente con la voluntad. En el primero se declara con una voluntad equivocada (viciada) y en el segundo se quiere una cosa y se declara otra, se declara lo que no se quiso”*.<sup>21</sup> En otras palabras, el error vicio provoca la anulabilidad del contrato, mientras que el error obstativo su inexistencia, por la falta de uno de sus elementos.

En el caso particular de los *smart contracts*, pueden darse ambos supuestos; es decir, un error vicio, por tener una representación mental errónea de la realización del contrato, o bien un error obstativo, en donde el código informático no refleja la verdadera voluntad de las partes.

En función de lo expuesto, cobra especial relevancia que las partes sean conscientes del contenido del contrato, lo que implica no sólo conocer acabadamente las contraprestaciones pactadas, sino también todo lo relativo a la ejecución del *smart contract*, las particularidades de la tecnología subyacente (por ejemplo, si se trata de una red pública o privada), las consecuencias de su incumplimiento, etc.

---

<sup>19</sup> Tribunal Supremo de España (en pleno) Sala en lo Civil. Sentencias N° 840/2013, de 20 de enero de 2014, y N° 491/2015, de 15 de septiembre de 2015. Doctrina reiterada recientemente en la sentencia N° 3593/2018 de 24 de octubre de 2018.

<sup>20</sup>Tribunal Supremo de España. Sala en lo Civil. Sentencia N° 8369/1999 de 22 de diciembre de 1999.

<sup>21</sup>Tribunal Supremo de España. Sala en lo Civil. Sentencia N° 330/2016 de 2 de febrero de 2016.

A su vez, una alternativa para evitar el error obstativo podría ser plasmar en lenguaje humano el *smart contract*, tal como –estimamos– debería ocurrir siempre que se trate de una relación de consumo (tema que analizaremos más adelante).

Pero ello no es suficiente. En efecto, será necesaria la colaboración entre juristas y programadores a fin de lograr que el *smart contract* (redactado en código informático) recepte acabadamente las intenciones y aquello acordado por las partes, sus implicancias y consecuencias, a la vez que evitar que se plasmen instrucciones incorrectas o que se expresen mal las cláusulas de un contrato (es decir, una mala programación) (LEGERÉN MOLINA, 2018).

#### III.4. La forma en los contratos inteligentes

Tal como veremos a continuación, la forma adquiere particular relevancia en el caso de los contratos inteligentes.

El artículo 1278 CC consagra el principio de libertad de forma de los contratos al establecer que *“los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez”*. Este artículo es complementado por el artículo 1279 CC, que dispone *“si la ley exigiere el otorgamiento de escritura u otra forma especial para hacer efectivas las obligaciones propias de un contrato, los contratantes podrán compelerse recíprocamente a llenar aquella forma desde que hubiese intervenido el consentimiento y demás requisitos necesarios para su validez”*.

A su vez, el artículo 23.2 de la LSSICE sostiene que *“siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información de contiene en un soporte electrónico”*.

Si bien rige el principio de libertad de forma para los contratos, en el caso de los *smart contract*, la forma resulta un elemento esencial y hasta constitutivo. Ello es así en tanto si no se cumple con esta particularidad, no estaríamos, técnicamente hablando, de un *smart contract*. Ello, pues la falta de forma determinada impediría los efectos propios de este tipo de contratos, esenciales para su existencia.

Sin perjuicio de lo expuesto, es importante destacar que el contenido formal del *smart contract* no es solo el *software* o código informático, sino que abarca todos los elementos informáticos adicionales al mismo (TUR FAÚNDEZ, 2018)– por ejemplo y como veremos más adelante, incluye los archivos PDF almacenados en IPFS–. Ello,

independientemente de que al día de hoy no existe una forma universal para los contratos inteligentes, sino que hay que atender a las particularidades de la plataforma en la que se realicen.

Por último, cabe destacar que, en tanto contratos electrónicos, resulta de aplicación el artículo 23.4 de la LSSICE que, entre otras disposiciones, excluye de su aplicación a aquellos negocios o actos jurídicos para cuya validez la ley exija documento público o intervención de órganos jurisdiccionales, notarios, registros, etc.

#### IV. Contratos inteligentes y protección de consumidores y usuarios

En función de las características de los *smart contracts*, no cuesta imaginar el desarrollo de contratos en serie, dirigidos principalmente a consumidores. Si bien tal como mencionamos, resulta de aplicación la normativa específica, deviene necesario efectuar unas breves consideraciones.

El derecho a la información constituye uno de los elementos fundamentales de los consumidores y usuarios, contemplado a nivel constitucional. En efecto, el artículo 51 de la Constitución española ordena a los poderes públicos para que promuevan el derecho de los consumidores a una información adecuada.

En primer lugar, por ser contratos electrónicos, resulta de aplicación el artículo 27 de la LSSICE que al regular las obligaciones previas a la contratación, establece la necesidad de poner a disposición del destinatario las condiciones generales del contrato de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

Por tratarse de contratos de consumo, también se deberá cumplir con lo dispuesto en el artículo 97 del Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios ("TRLGDCU") relativo a la información precontractual de los contratos a distancia y los contratos celebrados fuera del establecimiento mercantil. Y ello deberá realizarse en la forma establecida en su artículo 98 que, entre otras cuestiones, dispone que *"el empresario facilitará al consumidor y usuario, en la lengua utilizada en la propuesta de contratación o bien, en la lengua elegida para la contratación, y, al menos, en castellano, la información exigida en el artículo 97.1 o la pondrá a su disposición de forma acorde con las técnicas de comunicación a distancia utilizadas, en términos claros y comprensibles (...). Siempre que dicha información se facilite en un soporte duradero deberá ser legible"*. Pesa

sobre el empresario la obligación de entregar al consumidor una copia del contrato impresa o en soporte duradero.

Advertido esto, se genera el primer interrogante: ¿Cómo cumplirá el empresario con todas estas exigencias, si los contratos inteligentes se plasman en código informático?

Si bien es un tema sumamente complejo, destacamos que ya existen, al día de hoy, posibilidades de cumplir con la normativa vigente. En efecto, no todo el contenido del contrato se encuentra necesariamente en código informático.

En primer lugar, consideramos necesario que la página web brinde toda la información relativa al *smart contract* (incluyendo tanto las características propias de estos contratos, como la relativa a la tecnología de cadena de bloques). Es decir, el sitio web debe explicar, con distintos supuestos y ejemplos, cómo es el funcionamiento de los contratos y la tecnología donde se almacenan y ejecutan (ello podría realizarse, por ejemplo, mediante un texto que los usuarios puedan descargar, complementado con un video explicativo).

En segundo lugar, el sitio web deberá contener información clara, precisa y detallada del producto o servicio que se está ofreciendo, preferentemente en diversos lenguajes, cumpliendo con los requisitos establecidos en la LSSICE, en el TRLGDCU y en la LOPD (TUR FAÚNDEZ, 2018).

Una cuestión distinta se plantea en relación con el contenido del contrato, que necesariamente deberá estar redactado en código informático para poder ejecutarse en forma automática y autónoma. Si bien el contrato y las condiciones generales pueden estar disponibles en lenguaje humano en la página web (por ser, generalmente, contratos de adhesión), luego deberá plasmarse en código informático. Ante esta situación, ¿Cómo puede asegurarse al consumidor que se mantendrán los términos establecidos y descriptos en la página web?

A modo de ejemplo cabe citar nuevamente el caso de Ethereum, que tiene su propio lenguaje de programación denominado "Solidity" (similar al *Javascript*). Mediante este lenguaje se pueden crear y desarrollar contratos inteligentes que se ejecuten en la Máquina Virtual Ethereum (EVM por sus siglas en inglés). Solidity es un lenguaje de alto nivel ya que es "Turing Completo", es decir, puede expresar cualquier tarea realizable por el ordenador que lo interpreta y ejecuta, y resolver cualquier problema computacional (PREUKSCHAT, 2017).

Sin embargo, no todo el *smart contract* necesariamente se encuentra en lenguaje Solidity. Ethereum permite el almacenamiento del *hash* de un archivo que se encuentre, por

ejemplo, en PDF (y dicho pdf, en cualquier idioma). Si bien existen distintas plataformas para lograr este acceso, nos referiremos al caso de *InterPlanetary File System* (IPFS) que consideramos de gran utilidad.

IPFS es un sistema de archivos distribuido P2P que busca conectar todos los dispositivos informáticos con el mismo sistema de archivos.<sup>22</sup> Posee una estructura similar a la de una cadena de bloques, en tanto se trata de redes descentralizadas compuestas por múltiples nodos, y su ventaja es que permite almacenar, en esta red distribuida, archivos de texto, imágenes, videos, páginas web, etc. Al igual que en la tecnología de cadena de bloques, todos los nodos poseen una copia de la documentación almacenada, permitiendo la disponibilidad permanente de los archivos y utilizan un hash criptográfico de contenido, que impide su manipulación y mutabilidad.

Siguiendo esta línea, resultaría posible alojar el texto del contrato tradicional, así como las condiciones generales, en la plataforma IPFS. El *smart contract* redactado en código informático podría remitir al *hash* del archivo almacenado en IPFS, garantizando que dicho contrato tiene como sustento las condiciones generales y plasma los términos del contrato adjunto en PDF. A su vez, la inmutabilidad de la cadena de bloques evitaría su manipulación por parte del empresario.

Finalmente, cabe realizar una breve mención al derecho de desistimiento en el contrato de compraventa. El artículo 71.2 TRLGDCU establece un plazo de 14 días, computados a partir del día de la recepción del bien, para ejercer el derecho, pudiendo extenderse 12 meses más en caso que el vendedor no hubiera informado al consumidor este derecho. Sin perjuicio de las dificultades que puedan generarse, este derecho debe ser considerado por el programador a fin de asegurar que pueda ser ejercido.<sup>23</sup>

En función de lo expuesto, si bien las particularidades de los *smart contracts* acentúan la habitual posición de desventaja en la que se encuentra el consumidor ya que, en general, prima un desconocimiento respecto de esta tecnología, ello no significa que se encuentre totalmente desamparado. Sin embargo, hay un gran camino por delante.

---

<sup>22</sup> InterPlanetary File System. Disponible en: [<https://ipfs.io/>]

<sup>23</sup> Al respecto, TUR FAÚNDEZ (2018) sugiere una solución técnica para este inconveniente.

## V. El caso Argentino

Si se analiza la legislación vigente en la República Argentina, se arriba a las mismas conclusiones que en el caso español, sin perjuicio de tener que efectuar ciertas aclaraciones.

En primer lugar, la normativa general sobre contratos contenida en el Código Civil y Comercial de la Nación (en adelante, CCyCN) es similar a la española: rigen los principios de libertad de forma (arts. 284 y 1015), libertad para contratar (art. 958), existen similares disposiciones respecto del objeto, causa y consentimiento (entendemos que la teoría de la recepción de la aceptación es compatible con la tecnología de cadena de bloques, precisamente, por el sellado en el tiempo), así como del error como vicio de este último (el artículo 267 contempla los distintos supuestos de error esencial, coincidentes con los regulados en el derecho español).

Los contratos electrónicos se encuentran regulados en el CCyCN dentro de las modalidades especiales de los contratos de consumo, en particular, de los “contratos a distancia” (art. 1105), misma terminología que utiliza la Ley general para la Defensa de los Consumidores y Usuarios (art. 97 y ccdtes.). En su esencia, las disposiciones coinciden con las de la LSSICE: tanto la oferta como la aceptación tienen lugar por medios electrónicos (art. 1108) y se reconoce como satisfecho el requisito del contrato por escrito siempre que se encuentre en un soporte electrónico u otra tecnología similar (en este sentido, el artículo 1106 CCyCN resulta análogo al 23.2 de la LSSICE).

Como señala STIGLITZ (2015), estas disposiciones tienen como fuente el artículo 1268, inc. 2 y 3 de la “Propuesta para la modernización del derecho de las obligaciones y contratos” para España.

Por las particularidades de los contratos inteligentes, cobra especial relevancia el artículo 1107 del CCyCN, al establecer la obligación del proveedor de informar al consumidor, además del contenido mínimo y la facultad de revocar, *“todos los datos necesarios para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos”*.

En la misma línea, resulta de importancia la obligación de información establecida en el artículo 1100 CCyCN referida a las características esenciales de los bienes y servicios, las condiciones de su comercialización y *“toda otra circunstancia relevante para el contrato”*, expresión genérica que adquiere un gran sentido en este contexto. El artículo mencionado exige que dicha información sea proporcionada con *“la claridad necesaria que permita su comprensión”*. De igual forma, cabe destacar el artículo 985 relativo a los contratos

celebrados por adhesión a cláusulas generales predispuestas, en particular, la exigencia de la redacción “*clara, completa y fácilmente legible*” de las cláusulas.

Al respecto, remitimos al comentario efectuado en el Título IV del presente trabajo sobre la necesidad de brindar toda la información necesaria tanto de las particularidades de la tecnología de cadena de bloques, como de los contratos inteligentes propiamente dichos y, claro está, del contrato en particular.

Asimismo, también resulta de aplicación la ley N° 24240 de Defensa del Consumidor (en particular, sus artículos 4 y 10 ) que, en lo que aquí interesa coincide sustancialmente con la Ley general para la Defensa de los Consumidores y Usuarios española, sin perjuicio de la mayor extensión, exigencia y especificidad de esta última.

Por último, el artículo 288 CCyCN admite la firma digital como prueba de la autoría de la declaración de voluntad expresada, cuestión de gran importancia en este tipo de contratos. En consecuencia, consideramos que el marco regulatorio vigente en Argentina brinda las pautas para solucionar el problema de la identidad, máxime considerando la tímida tendencia hacia la identidad digital que se está gestando en nuestro país.<sup>24</sup>

En esta línea, en la última modificación al decreto reglamentario de la ley de Firma Digital N° 25506, efectuada mediante el Decreto 182/2019, se incorporó la figura de los “Servicios de Confianza” y “Prestadores de Servicios de Confianza”, similar a lo establecido en la LSSICE y el Reglamento Reglamento eIDAS (EU 910/2014). Lo novedoso de la reforma es que considera “Servicio de Confianza” al servicio electrónico prestado por un tercero de confianza relativo a “*la operación de cadenas de bloques para la conservación de documentos electrónicos, gestión de contratos inteligentes y otros servicios digitales*” (artículo 36 inc. 5 del Decreto 182/2019). Es decir, nuestra normativa ha expresamente incorporado disposiciones relativas a esta tecnología, así como también a los contratos inteligentes.

En función de lo expuesto, y sin perjuicio de modificaciones que inevitablemente tendrán lugar, la normativa vigente al día de hoy, al menos en principio, otorga los elementos necesarios para dar a los contratos inteligentes un marco legal. Asimismo, se observa cierta modernización e incorporación de la tecnología de bloques y uso de contratos inteligentes para el futuro no tan lejano.

---

<sup>24</sup> Al respecto, ver [<https://www.argentina.gob.ar/sid-sistema-de-identidad-digital>].

## VI. ¿El fin de los contratos tradicionales?

Finalmente, cabe referirnos al ámbito de aplicación de los *smart contracts*. Hay quienes pregonan que el auge de los contratos inteligentes traerá el fin de los contratos tradicionales y, por tanto, de los abogados que a ello se dedican. Sin embargo no compartimos esa postura.

Si bien los *smart contracts* tienen un gran futuro por delante, principalmente con el desarrollo del IoT, entendemos que no reemplazarán a los contratos tradicionales. Ello, puesto que su ámbito de aplicación es limitado.

En efecto, la lógica sobre la que se construyen (código informático basado en la fórmula *if/then/else*), limita el universo de situaciones que pueden abarcar estos contratos, en tanto solo se formalizarán de esta manera aquellos contratos que puedan plasmarse en una secuencia de instrucciones susceptible de ser entendida y ejecutada por un ordenador.

En consecuencia, los contratos inteligentes constituyen una alternativa para aquellos acuerdos en los que las condiciones sean objetivamente comprobables, es decir, verificables de manera objetiva y autónoma (PUTERBAUGH, 2016). Sin embargo, no lo son para aquellos casos en los cuales haya que recurrir a la interpretación para verificar el cumplimiento de determinadas cláusulas, como la diligencia debida, buena fe, interés superior del niño o el acaecimiento de supuestos de caso fortuito o fuerza mayor (LEGERÉN MOLINA, 2018).

## VII. Consideraciones finales

Si bien hemos analizado varios de los interrogantes jurídicos que plantean los contratos inteligentes ejecutados en *blockchain*, no hemos agotado el tema, que sin duda merece un análisis más amplio y profundo.

En efecto, quedan numerosas cuestiones sin resolver: 1. el valor probatorio de la tecnología de cadena de bloques; 2. la determinación de la ley aplicable para hacer cumplir un contrato inteligente ejecutado en una red *blockchain* pública, en donde los contratantes proceden de distintas jurisdicciones; 3. su compatibilidad con la normativa relativa a la protección de datos personales, por ejemplo, en relación con la necesidad de identificar al encargado de tratamiento de los datos o la garantía del derecho al olvido (debido al carácter inmutable y público de la tecnología de cadena de bloques); 4. cuestiones relativas

a la responsabilidad, tanto en relación con la persona que programa el contrato (ante errores que conllevan la ejecución de prestaciones no pactadas), como en relación con los contratos celebrados enteramente mediante dispositivos electrónicos o conectados mediante IoT (los mencionados “contratos M2M”), entre otras.

Sin duda alguna, hay muchos aspectos sobre los cuales tanto la comunidad jurídica como la tecnológica debe trabajar, por lo que insistimos en la necesidad de conformar un equipo interdisciplinario de abogados, programadores, ingenieros y especialistas en esta tecnología para poder aprovechar sus beneficios en la mayor medida posible, pero, al mismo tiempo, brindando seguridad jurídica y protegiendo a la comunidad (especialmente, a los consumidores y usuarios).

### VIII. Conclusiones

Aun considerando que actualmente no existe una regulación específica relativa a los contratos inteligentes, ello no es estrictamente necesario, por cuanto el derecho de contratos vigente brinda un marco jurídico adecuado. Ello, puesto que los contratos inteligentes son, a fin de cuentas, contratos electrónicos y deben cumplir, en consecuencia, con la normativa aplicable a éstos últimos. Por el contrario, en caso de no cumplir con los requisitos establecidos por la normativa aplicable, no constituirán verdaderos contratos.

Por otro lado, los contratos inteligentes tienen un ámbito de aplicación limitado a cuestiones objetivamente comprobables, por lo que no reemplazarán a los contratos tradicionales.

Al día de hoy, los principales retos jurídicos se plantean como consecuencia de las características de la tecnología de cadena de bloques, y no por las características de los contratos inteligentes. En efecto, resulta necesario adoptar una regulación sobre dicha tecnología, principalmente en cuestiones vinculadas con la identidad digital, derecho de consumo, responsabilidad, protección de datos personales, defensa de la competencia, lavado de activos y financiamiento del terrorismo. Ello, pues pareciera que la tecnología *blockchain* abarcará un universo inconmensurable de situaciones. Puede decirse, entonces, que hay un gran trabajo por delante.

## Bibliografía

ALLEN, M. (2018) “Crypto Valley’ Zug to trial blockchain voting” consultado en [[https://www.swissinfo.ch/eng/system-test\\_-crypto-valley--zug-to-trial-blockchain-voting/44177440](https://www.swissinfo.ch/eng/system-test_-crypto-valley--zug-to-trial-blockchain-voting/44177440)] el 30/07/2019.

ARIAS POU, M. (2006) “El consentimiento en la contratación electrónica por internet”, *Diario La Ley*, año 27, N° 6540, pp. 1527-1535.

BIELLI, G. E. (2019) “Terceros de confianza y certificación de prueba electrónica Una nueva frontera en materia de probática”, *Diario La Ley*, año LXXXIII, N° 103, pp. 1-3.

BOTANA GARCÍA, G.A.(2014)“Los contratos electrónicos a la espera de una nueva reforma”, *Diario La Ley*, Actuación Civil N° 2, tomo 1.

DE CARIA, R. (2018) “The legal meaning of smart contracts”, *European Review of Private Law Kluwer Law International BV*, año 2018, volumen 26. N° 6, pp. 731-751.

DIEZ BALLESTEROS, J.A. (2008) “Obligaciones precontractuales de información en la contratación electrónica y protección de los consumidores”. *Estudios sobre Consumo*. N° 85. pp. 61-75.

DOMINGO, C. (2018) *Todo lo que querías saber sobre bitcoin, criptomonedas y blockchain y no te atreías a preguntar*. España. Ediciones Temas de Hoy. Ebook.

DUROVIC, M. y JANSSEN, A. (2018) “The Formation of Blockchain-based Smart Contracts in the Light of Contract Law”, *European Review of Private Law Kluwer Law International BV*, año 2018, volumen 26, N°. 6, pp. 753-771.

FERNÁNDEZ ESPINOSA, L. (2019) “BBVA impulsa INATBA, la alianza internacional de ‘blockchain’ promovida por la CE”, consultado en [<https://www.bbva.com/es/bbva-impulsa-inatba-la-alianza-internacional-de-blockchain-promovida-por-la-ce/>] el 30/07/2019.

GATES, M. (2017) “La guía para entender todo lo referente a la cadena de bloques, Bitcoin, criptomonedas, contratos inteligentes y el futuro del dinero”, *Publicación Independiente, Kindle Edition*.

GÓRRIZ LÓPEZ, C. (2017) “Tecnología Blockchain y contratos inteligentes” en Navas Navarro (dir.) *Inteligencia artificial. Tecnología Derecho*. Valencia. Tirant Lo Blanch, pp. 151-195.

LAGE SERRANO, O. (2017) “¿Es Blockchain realmente inmutable?”, consultado en [<https://www.bbva.com/es/blockchain-realmente-inmutable/>] el 30/07/2019.

LEGERÉN MOLINA, A. (2018) “Los contratos inteligentes en España. La disciplina de los smart contracts”, *Revista de Derecho Civil*, vol. 5, N° 2, pp. 193-241.

MORA, S. J. (2019) “La tecnología blockchain: contratos inteligentes, ofertas iniciales de monedas y demás casos de uso”, *Diario La Ley*, año LXXXIII, N° 62, pp. 1-6.

MORALES BARROSO, J. (2018) “¿Qué es Blockchain?” en GARCÍA MEXÍA, P. (dir.) *Criptoderecho. La regulación de Blockchain*. España, Wolters Kluwer, pp.39-73.

NAKAMOTO, S. (2008) “Bitcoin: a Peer-to-Peer Electronic Cash System. Bitcoin Org” consultado en [<https://bitcoin.org/bitcoin.pdf?>] el 30/07/2019.

NAVARRO DE ANDRÉS, S. (2018) “Contratos Inteligentes. En especial, su implantación práctica en negocios blockchain” en GARCÍA MEXÍA, P. (dir.) *Criptoderecho. La regulación de Blockchain*. España, Wolters Kluwer, pp. 317-361.

PREUKSCHAT, A. (2017) “Blockchain. La revolución industrial de Internet”, consultado en [<https://www.eleconomista.es/economia/noticias/8817210/12/17/Ethereum-es-Turing-completo-y-eso-que-es.html>] el 30/07/2019.

PUTERBAUGH, D. (2016) “The future of contracts: automation, blockchain and smart contracts”, consultado en [<https://acla.acc.com/documents/item/1780>] el 30/07/2019.

SALMERÓN MANZANO, E. (2018) “Los contratos inteligentes o smart contracts y sus implicancias sobre el Nuevo Derecho de la contratación” en LLAMAS POMBO, E. (dir.) *Congreso Internacional de Derecho Civil Octavo Centenario de la Universidad de Salamanca*. España, Tirant lo Blanch. Ediciones Universidad de Salamanca, pp. 333-338.

STIGLITZ, R. (2015) “Contratos celebrados fuera de los establecimientos comerciales y contratos a distancia” En STIGLITZ, R. (dir.) *Contratos en el Nuevo Código Civil y Comercial*. Buenos Aires, Thomson Reuters La Ley. Ebook.

SZABO, N. (1996) “Smart Contracts: Building Blocks for Digital Markets”, *Extropy: The Journal of Transhumanist Thought*, vol. 16.

TUR FAÚNDEZ, C. (2018) *Smart Contracts. Análisis Jurídico*. Madrid, Reus.