FACULTAD DE DERECHO

ESTUDIO DE LOS SMART CONTRACTS DESDE LA PERSPECTIVA LEGAL

Autor: María del Pilar Somé Parra
5º E-3 C
Área del Derecho Civil

Tutor: Jaime Bofill Morientes

Madrid
Junio 2022

ÍNDICE DEL DOCUMENTO

ÍNDICE DE FIGURAS

LISTADO DE ABREVIATURAS

[1] PoW: Proof of Work

[2] PoS: Proof of Stake

[3] DPoS: Algoritmo de pruebas delegadas

[4] LPoS: Prueba de participación alquilada

[5] PBFT: Tolerancia Práctica de Fallas Bizantinas

[6] IP: Protocolo de Internet

[7] DApps: Aplicaciones descentralizadas

RESUMEN

En este proyecto se tratará de aproximar el concepto de la nueva red Blockchain surgida del protocolo expuesto por Satoshi Nakamoto en el año 2008 así como su funcionamiento más básico. También se prestará especial atención a los principales componentes de esta, así como al importante papel que los usuarios toman en este nuevo tipo de sistemas de consenso descentralizado.

Posteriormente se introducirá el concepto de Smart Contracts y se relacionará con la Blockchain de cara a analizar su funcionamiento y características. En objetivo de este trabajo es analizar este nuevo instrumento jurídico desde una perspectiva legal partiendo de su base digital. Se tratará de aportar luz ante aquellas partes más desconocidas del funcionamiento de redes descentralizadas y cómo estas afectan al usuario jurídico. Así mismo, se incluirá en los apartados aquellos límites que podrían impedir el buen funcionamiento de los Smart Contracts.

Por último se mostrarán aquellos retos que hoy se presentan ante el legislador y que son de mayor urgencia. Se partirá de una base ética a la hora de analizar la problemática que este nuevo instrumento jurídico puede comportar. El proyecto finalizará con un breve apartado que integre las conclusiones a las que se haya llegado tras la investigación.

Palabras clave: Blockchain, consenso, descentralizado, Smart Contracts, perspectiva legal, usuario jurídico, instrumento legal.

ABSTRACT:

This project will try to approach the concept of the new Blockchain network that emerged from the protocol exposed by Satoshi Nakamoto in 2008, as well as its most basic operation. Special attention will also be paid to its main components, as well as to the important role that users play in this new type of decentralized consensus system.

Subsequently, the concept of Smart Contracts will be introduced and related to the Blockchain in order to analyse its operation and characteristics. The aim of this work is to analyse this new legal instrument from a legal perspective, starting from its digital basis. It will try to shed light on the most unknown parts of the functioning of

decentralised networks and how these affect the legal user. Likewise, those limits that could impede the proper functioning of Smart Contracts will be included in the sections.

Finally, it will show those challenges that the legislator is currently facing and which are of greater urgency. An ethical basis will be used as a starting point when analysing the problems that this new legal instrument may entail. The project will end with a short section integrating the conclusions drawn from the research.

Key words: Blockchain, consensus, decentralized, Smart Contracts, legal perspective, legal user, legal instrument.

1. INTRODUCCIÓN

1.1. Definición del objeto del TFG

El presente documento está dirigido a presentar y exponer los conceptos de Blockchain o cadena de bloques y de Smart Contract, cada vez más presentes en el mundo tecnológico, así como a presentar los nuevos retos a los que, en consecuencia, se enfrenta el legislador.

De igual forma, se expondrá un caso práctico de lo previamente estudiado que tratará de analizar las vicisitudes a las que se enfrentan los nuevos contratos inteligentes, así como el contenido obligatorio de los mismos.

También será objeto de análisis el plano ético por el que esta nueva herramienta ha de estar afectada, desde un punto de vista tanto jurídico como empresarial. Este estudio ético señalará el camino por el que el legislador habrá de comenzar su estudio de la Blockchain para garantizar al usuario un servicio justo y veraz.

1.2. Justificación del TFG

El tema analizado en este documento ha sido seleccionado de entre otros muchos debido a que supone el estudio de una nueva forma de expresión del derecho y sus instrumentos. Constituye una fuente de aprendizaje poco abordada desde los centros de enseñanza jurídica y por ello muy enriquecedora para el alumnado. Planea ser el futuro de otras muchas formas de expresión jurídicas y trae consigo gran cantidad de novedosos retos para la regulación española y global.

Con esta tesis se pretende analizar la nueva tecnología Blockchain y sus principales aplicaciones jurídicas como son los contratos inteligentes. Se relatará su funcionamiento y principales características, así como retos, ventajas y límites.

1.3. Presentación de la estructura

La estructura del documento toma forma partiendo de un análisis general de lo que supone la nueva tecnología Blockchain así como su funcionamiento, sus riesgos, ventajas e inconvenientes. El autor del documento considera que es fundamental exponer las bases de la cadena de bloques para comprender las funcionalidades y ventajas que la misma aportaría a figuras legales como son los contratos. Posteriormente al apartado de

Blockchain se iniciará una introducción a los Smart Contracts, partiendo de sus orígenes, concepto, partes y otras figuras para llegar a un ejemplo práctico que englobe lo explicado en todo el documento. Dicho ejemplo será utilizado para analizar una situación real y común en el mercado en la que sea susceptible de aplicación un contrato inteligente por las facilidades que pueda aportar con respecto a su versión tradicional.

Después, se abarcarán otras cuestiones éticas y retos que el legislador habrá de afrontar durante los próximos años para dar tratamiento legal a gran parte de las situaciones legales, si no todas.

Por último, un apartado de conclusiones cerrará el estudio y resumirá brevemente el camino por hacer de los contratos inteligentes, así como del legislador y los usuarios.

1.4. Descripción del método empleado

Se ha utilizado el estudio de las fuentes citadas en el documento y al final del mismo.

Durante los inicios de la tesis se estableció un índice con las principales cuestiones a abordar y estas se han ido investigando durante el desarrollo del documento. Han sido fuente de inspiración las noticias actuales sobre este nuevo sistema y se han tratado de plasmar los principales movimientos que se están dado por parte de los usuarios de la cadena de bloques.

El método ha sido eminentemente una investigación, lectura y escucha comprensiva tanto de otras tesis, como de artículos y videos.

2. INICIOS DEL BLOCKCHAIN – SATOSHI NAKAMOTO

Satoshi Nakamoto es el pseudónimo utilizado por el creador de Bitcoin, primera plataforma en utilizar la tecnología Blockchain. En 2008 publicó un protocolo[1] en el que establecía las bases del funcionamiento de la cadena de bloques y sus principales usos con respecto a transacciones económicas digitales.

[1] NAKAMOTO, S., Bitcoin: A Peer-to-Peer Electronic Cash System*, Lista de correo de criptografía metzdowd,* 2008.

Su razonamiento consistió en el análisis de la evolución del comercio en internet. Este, a pesar de nacer como innovador y lleno de ventajas, había decaído ante la necesidad de depender constantemente de entidades financieras o terceros de confianza que dotaran a las operaciones de validez ante el resto de individuos y sociedades. Esto debilitaba las operaciones y aumentaba considerablemente su costo. Además, el mecanismo digital propuesto, para Nakamoto no aportaba realmente una gran credibilidad y confianza puesto que a la hora de la verdad las transacciones permanecen si estos terceros lo permiten, lo cual favorece un clima de posible fraude y de desprotección hacia los particulares privados y empresas.

Es por ello que ofrece Bitcoin como alternativa a lo que podrían ser funcionalidades como las pasarelas electrónicas de pago, como PayPal, o a la mayoría de las operaciones económicas realizadas en la web.

El sistema de pago de Bitcoin elimina la intervención de terceros y la sustituye por pruebas criptográficas. Una vez garantizada la confianza mediante estos puzzles criptográficos, que posteriormente desarrollaremos, la tecnología de Blockchain cubre otra de las grandes desventajas del comercio en internet como es la reversibilidad y dota a la Blockchain de inmutabilidad, es decir, las transacciones realizadas quedan completamente cerradas a modificaciones. Por último, basa el sistema en el Peer-to-Peer, es decir en un servidor colectivo de consenso, que será liderado por la actividad de *nodos* y *mineros*.

2.1. La moneda electrónica

Tanto la criptomoneda de Bitcoin como el Ether de Ethereum, plataformas que serán desarrolladas en posteriores apartados de la presente tesis, constituyen una cadena de firmas digitales. Las mismas son transferidas entre usuarios a modo de transacción y supondrán la retribución monetaria que mantendrá a las plataformas usuarias del sistema Blockchain en actividad.

3. TECNOLOGÍA BLOCKCHAIN

3.1. Introducción, definiciones

La Blockchain o cadena de bloques es, brevemente, una base de datos formada por una secuencia creciente de bloques de almacenamiento. Se trata de la base tecnológica de Bitcoin, explicada por primera vez en el libro blanco *Bitcoin: A Peer-to-Peer Electronic Cash System (2008)*[2]. Esta tecnología Blockchain es aplicable a muy diversas actividades: contratos inteligentes, mantenimiento de registros, sistemas de identificación, etc[3].

Dicha red de bloques es capaz de registrar todo tipo de transacciones y funciona mediante la verificación constante de sus nodos, es decir, es un sistema que se retroalimenta de sus usuarios y cancela cualquier tipo de intervención de terceros. Esto constituye un gran cambio en la industria pues quedarían obsoletos muchos trámites y costos que antes eran preceptivos debido a la necesidad de acudir a terceros como podrían ser los notarios. Además, una de las características más notables de Blockchain es su carácter semiabierto, todos los cambios quedan registrados y asociados al usuario que permuta el sistema, aunque con un *nombre de usuario o pseudónimo* que protege su identidad. También quedan fuera de la filosofía Blockchain todas aquellas entidades financieras que eran necesarias para dotar de confianza a procesos contable[4].

Se configura como un método fiable para aquellas partes que no confíen en el cumplimiento último del contrato. Esto se debe a que presenta un consenso sobre la existencia, el estado y la evolución del trato[5].

Aunque como hemos dicho, en un principio fue diseñada para almacenar el historial de transacciones realizado en Bitcoin, recientemente se han ido creando plataformas alternativas que aprovechan la Blockchain para el registro de los movimientos de otras muchas aplicaciones descentralizadas. Un ejemplo, sería el de los Smart Contracts en Ethereum.

---

[2] Id.
[3] PARRONDO, L., "Tecnología blockchain, una nueva era para la empresa", *Revista de Contabilidad y Dirección*, vol. 27, 2018, pp. 11-31.
[4] NAKAMOTO, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", *Decentralized Business Review*, 2008, pp.1-9.
[5] FORERO FORERO, E. A., & MOYANO SOTO, S. D., "Pasos a tener en cuenta para un proceso de implementación del Blockchain en el sector cafetero colombiano", Trabajo fin de grado, 2020.

En los siguientes apartados se analizarán las operaciones, los agentes de la Blockchain como son los nodos y mineros, así como otras funcionalidades como los métodos de consenso. También serán clasificadas las cadenas de bloques según sus funcionalidades y se tratará de incluir ejemplos gráficos en las explicaciones.

3.2. Operaciones en Blockchain

Para que una operación realizada en Blockchain aproveche las ventajas que el sistema ofrece necesita cumplir con una serie de características[6].

En primer lugar, habrá de incluir complejos mecanismos criptográficos que permitan identificar a las partes y reflejar la autoridad correspondiente a la hora de realizar modificaciones. Además, el sistema y sus protocolos habrán de estar sometidos a las correcciones pertinentes para su buen funcionamiento. Por último, y fundamental, habrá de contener mecanismos que funcionen como incentivos para los nodos de forma que provoquen su participación en el sistema de forma honesta.

3.3. Nodos y mineros

Más concretamente, se trata de terminales u ordenadores conectados en red que utilizan un mismo sistema de comunicación, llamado protocolo. Este sistema, como todo Blockchain, actúa de forma descentralizada.

La función de los nodos es verificar y validar los nuevos bloques, este es un proceso necesario para poder reflejar su contenido en el libro mayor de Blockchain. En el proceso de validación y verificación llevan a cabo cálculos repetidos para averiguar el hash[7] válido en cada transacción que se quiera agregar, así verifican y lo comunican al resto de nodos. Todos los nodos están conectados entre sí y actualizan la información recibida y validada constantemente[8], de este modo, la información está replicada en todos los nodos que componen la cadena de bloques, siendo inmodificable gracias al registro masivo.

---

[6] MELA, J. L., & HERRERA, E. J. C., "Tecnologías Blockchain y sus aplicaciones", *Visión Antataura*, vol 3, nº 2, 2019, pp. 110-126.
[7] El hash de un bloque es su código identificativo. Este concepto será explicado más adelante.
[8] VILALTA NICUESA, A. E., *Smart legal contracts y blockchain*, Wolters Kluwer, Madrid, 2019, p. 24.

Puede suceder que los nodos al iniciar el proceso de validación de un nuevo bloque agregado a la cadena, resuelvan que la información no es válida. En este caso el protocolo a seguir es ignorar dicho bloque, que quedará sin validación y no será transmitido al resto de bloques, con lo cual no tendrá utilidad. Esto no deja de ser una retroalimentación del sistema.

Por el contrario, si la transacción reflejada en el bloque es válida, estos terminales la retransmiten, de forma que el resto de nodos la recibirán, almacenarán y transmitirán. El bloque validado únicamente puede ser añadido a la cadena si se produce un acuerdo entre la mayoría de los nodos. Se habrá llegado a un "consenso", concepto que se explicará en uno de los apartados posteriores y que es de vital importancia para el funcionamiento de la cadena de bloques.

Estos terminales principalmente surgieron para evitar el problema que sigue a la mayoría de objetos digitales intangibles, el fraude a través de la copia. Es decir, reflejado en la plataforma Bitcoin este riesgo sería la posibilidad de que una criptomoneda fuera utilizada dos veces en dos transacciones diferentes[9]. Para evitar este riesgo se necesita una figura que verifique las transacciones realizadas y transmita al resto la veracidad de las transacciones recogidas en los bloques. Satoshi Nakamoto, diseña la figura de los nodos y los mineros, que al funcionar "Peer 2 Peer", es decir entre iguales, posibilitan que no sea necesaria una figura central validadora sino que sea el propio sistema quien de validez a las cadenas de bloques.

Tras la verificación y validación de los nodos, son los mineros los que se encargan de agregar el nuevo bloque a la cadena de bloques. Para ello, de entre todos los bloques validados y aplicando las reglas de consenso mediante el Proof of Work (PoW) o Proof of Stake (PoS) deciden cuál ingresan a la Blockchain.

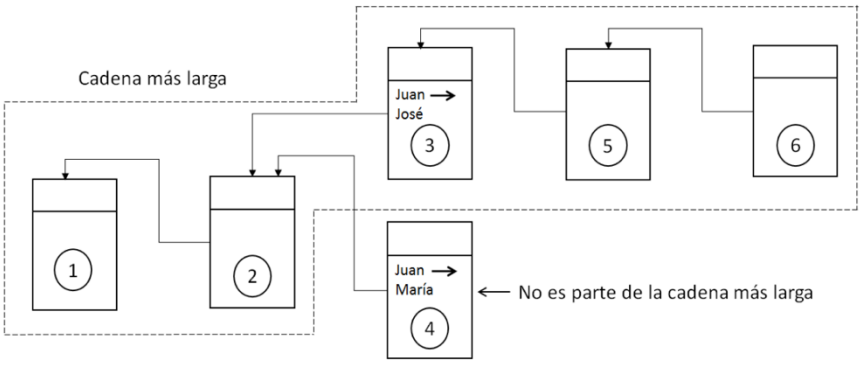
Los mineros seleccionan entre las transacciones válidas cuál ingresan, es decir, pueden ingresar el nuevo bloque en la cadena de bloques. Esta decisión se tomará según las reglas del consenso establecidas para cada red Blockchain. Además de las ya mencionadas PoW, PoS, existen otras muchas como pueden ser DPoS y PBFT, etc. Dichos consensos

[9] ZOZAYA, C., INCERA, J., & FRANZONI, A. L., "Blockchain: un tutorial", *Estudios*, vol 17, nº 129, 2019, pp. 113-126.

entrañan diferencias significativas que permitirán una adaptación mejor y más específica a cada tipo de aplicación descentralizada. Habrán de estar señalados de forma previa y no suelen ser objeto de modificación.

Para dotar al sistema de bloques de veracidad y utilidad, este necesitará de una validación que de fe del contenido o de Block Body y permita que sea replicado por el resto de ordenadores y servidores de la red. De lo contrario, los movimientos reflejados serían susceptibles de falsificación, duplicación, etc., y el sistema sería inútil ya que no habría confianza en lo reflejado por las cadenas.

FIGURA 1: BIFURCACIÓN O FORK



Fuente: ZOZAYA, C., INCERA, J., & FRANZONI, A. L., "Blockchain: un tutorial", *Estudios*, vol 17, nº 129, 2019, pp. 113-126.

Esta imagen nos muestra una *Bifurcación* o *Fork*, en la que a pesar de que dos bloques hayan sido validados, solo tendrá valor aquel que pertenezca a la cadena más larga. Esto nos muestra de forma gráfica, que realmente es el consenso de los nodos el que muestra las transacciones que serán consideradas como válidas o reales.

3.3.1. Tipos de nodos

En este apartado describiremos el papel de cada nodo presente en la Blockchain. Se mencionarán los nodos completos, los ligeros, los maestros, aquellos que comunican o transmiten transacciones y aquellos que generan o minan transacciones.

Cuando hablamos de nodos completos nos referimos a aquellos que contienen todas las transacciones de la cadena de bloques. Comprueban que no se ejecuten cambios en la misma y envían la información al resto de nodos. Por tanto, podemos afirmar que son almacenadores y transmisores de información.

Por otro lado, los nodos ligeros, a diferencia de los completos, solo contienen una parte de las transacciones reflejadas en la cadena de bloques. Estos se encargan de enviar información a la cadena para su validación e incorporación. Son nodos de menor carga, su retribución también será más pequeña.

Los nodos conocidos como nodos mineros inciden sobre el protocolo de forma decisiva. No solo emiten y transmiten, sino que además, comprueban, validan y verifican. Analizan la concordancia de los códigos criptográficos insertos en la cadena y distribuyen una copia de la misma al resto de nodos.

Por último, los nodos maestros o masternodes son los mejor retribuidos económicamente. Esto se debe a que gozan de una mayor capacidad computacional y de almacenamiento. La diferencia más significativa es que votan en los cambios de protocolo y participan de forma activa en la ejecución de operaciones. Para ser un masternode es necesario una garantía de criptomoneda mínima.

3.4. Sistemas de votación y métodos de consenso

Para continuar con la descentralización que caracteriza a la Blockchain y que Satoshi Nakamoto consideraba fundamental, no puede existir ninguna figura o, en este caso, nodo que sea el responsable de decidir cuál de todos los bloques verificados y validados es aquel que se incorpora a la cadena y se transmite y almacena por el resto de nodos. Estableciendo un método de consenso el sistema logra que los participantes de la red distribuida puedan llegar a un acuerdo respecto al orden de las transacciones realizadas. Siendo dichos participantes usuarios desconocidos entre sí y que carecen de una relación de confianza necesitan de ciertas reglas que garanticen una seguridad y confianza en la cadena de bloques[10].

[10] MORALES-MORALES, M., ROSERO-CORREA, L., & MORALES-CARDOSO, S., "Registro de títulos académicos mediante una aplicación basada en Blockchain y Smart Contracts", *Cátedra*, vol. 3, nº 2, 2020, p. 81.

Para llegar a un consenso que permita elegir qué registro utilizar se utilizan distintos mecanismos de consenso, siendo los más conocidos el Proof of Work (PoW) y el Proof of Stake (PoS).

Si en lugar de desarrollar métodos de consenso específicos para la Blockchain se optara por métodos más sencillos ya existentes como podría ser que cada servidor de la red identificado con su IP votara qué registro seleccionar, el sistema perdería seguridad. Se induciría al fraude debido a la sencillez de crear innumerables IPs virtuales, lo que es conocido como un Sybil Atack, que dejaría sin validez la votación. Otros muchos métodos de votación quedan sin validez debido a su poca seguridad o a la pérdida de descentralización que podrían suponer.

Hacer pagar un coste computacional a cada servidor que quiera participar del consenso resuelve en cierto modo la probabilidad de fraude. En este caso el coste consiste en resolver un puzzle criptográfico. Si un nodo malintencionado simulara ser distintos usuarios habría de resolver innumerables puzzles criptográficos, suponiendo esto un gran coste computacional. Esta resolución del nodo se conoce como Prueba de trabajo o PoW.

Por tanto, el trabajo de minería, es decir, una Prueba de trabajo o PoW consiste en la competición de los nodos para resolver un complejo rompecabezas criptográfico consistente en un patrón difícil de calcular y sencillo de verificar. Al lograr resolverlo, este se difunde al resto de nodos dando transparencia y solidez al sistema, de esta forma se va logrando un consenso en la red[11].

Este método realmente no garantiza un proceso de votación justo, otorga la decisión a aquel que tenga una mayor inversión computacional. Aquel que descifra el puzzle criptográfico es el que "mina el bloque". En el caso de que más de un nodo mine el mismo bloque al mismo tiempo provoca que surjan simultáneamente dos versiones del registro en dos bloques verificados y validados. No podrán ser registrados ambos ya que provocaría el registro duplicado de una misma transacción. Se añadirá cada uno a una

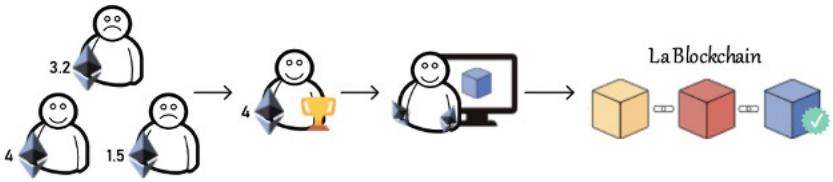
[11] NAWARI, N. O., & RAVINDRAN, S., "Blockchain technology and BIM process: review and potential applications"*, J. Inf. Technol. Constr.*, vol. 24, nº 12, 2019, p. 216.

cadena y será la válida aquella que tenga más bloques verificados de forma posterior, es decir, la cadena más larga[12].

Además, requiere un gran gasto computacional y está sometido al riesgo del fraude del 51%. Se trata de un método anterior a Blockchain.

Otro de los métodos de consenso más utilizados es el Proof of Stake o PoS, en español Prueba de participación. En este método, en lugar de darse una competición entre los nodos del sistema a la hora de descifrar el puzzle criptográfico, lo que sucede es que un solo nodo es elegido de forma previa para realizar la función de validación y verificación[13]. El método de elección del nodo será en función de su participación.

FIGURA 2: EL MECANISMO PROOF OF STAKE



Fuente: MIRANDA PALACIOS, V., "Explorando la Blockchain de Ethereum y el desarrollo de Smart Contracts", Tesis doctoral, Universitat Politècnica de Catalunya, 2018.

El nodo seleccionado participa bloqueando una de su participación en la operación, es decir, se produce un bloqueo monetario que le permite tener la posibilidad de ser elegido como el nodo que liderará la selección del bloque válido. Este nodo elegirá cuál es el siguiente bloque para añadir a la cadena. Evita el problema mencionado antes del fraude de identidades pues solo un nodo podrá ser el que elija el bloque nuevo. El nodo elegido

[12] SANTANA VEGA C., "QUÉ es el BLOCKCHAIN - (Bitcoin, Cryptos, NFTs y más)", 2022 (disponible en https://www.youtube.com/watch?v=V9Kr2SujqHw&t=1054s&ab_channel=DotCSV última consulta el 9 junio 2021).
[13] IZA, X. C., SAMPEDRO, X. Z., MORALES, M. M., & CARDOSO, S. M., "Análisis Comparativo de Métodos de Consenso sobre Plataformas Blockchain", *Revista Tecnológica-ESPOL*, vol. 33, nº 2, 2021, p. 29.

utiliza una firma digital que demuestra[14] su propiedad sobre la participación eliminando así la carrera computacional.

El método de selección del nodo depende de una serie de factores, a mayor participación mayor probabilidades de ser elegido. También hay una parte de aleatoriedad y, además, se valora el tiempo que lleva la participación bloqueada. Ya no se minan bloques sino que se "forjan", aunque el resultado continua siendo el mismo, obtener un bloque válido que añadir a la cadena.

La ventaja principal de este método es que evita el gasto masivo computacional, principal punto de crítica medioambiental hacia el sistema Blockchain. El ataque del 51% tampoco tendrá cabida pues el nodo validador solo puede ser uno, el seleccionado.

Las comisiones de las transacciones que formen parte del bloque serán el incentivo para el nodo forjador que sea elegido. Así deberá validar todas las transacciones y verificarlas para poder añadir el bloque. El Proof of Stake se renueva en cada bloque, de forma que no siempre lidere el mismo nodo[15].

3.5. Otros métodos de consenso menos generalizados

Siendo el PoW y el PoS los métodos de consenso más utilizados en Blockchain, existen otros que también ofrecen múltiples ventajas y se ajustan mejor a otro tipo de aplicaciones descentralizadas. En este apartado describiremos otros métodos conocidos de la cadena de bloques.

En primer lugar, el algoritmo de prueba delegada o DPoS permite a los nodos del sistema delegar su voto en otros nodos de forma que se simula una democracia política en el que aquellos nodos con poder de votación señalarán a un líder que tome las decisiones.

Se crearán además dos tipos de nodos con funcionalidades especificas: los nodos testigos y los nodos delegados. Los primeros crearán nuevos bloques mientras que los segundos

[14] Id.
[15] SANTANA VEGA C., "QUÉ es el BLOCKCHAIN - (Bitcoin, Cryptos, NFTs y más)", 2022 (disponible en https://www.youtube.com/watch?v=V9Kr2SujqHw&t=1054s&ab_channel=DotCSV última consulta el 9 junio 2021).

mantendrán la red y sugerirán los cambios necesarios para su buen funcionamiento. Bitshares, Tron, EOS y Cardano utilizan este método por ser uno de los más robustos, aunque es susceptible de caer en centralizaciones[16] .

FIGURA 3: REPRESENTACIÓN DE LA SELECCIÓN DEL NODO REPRESENTANTE

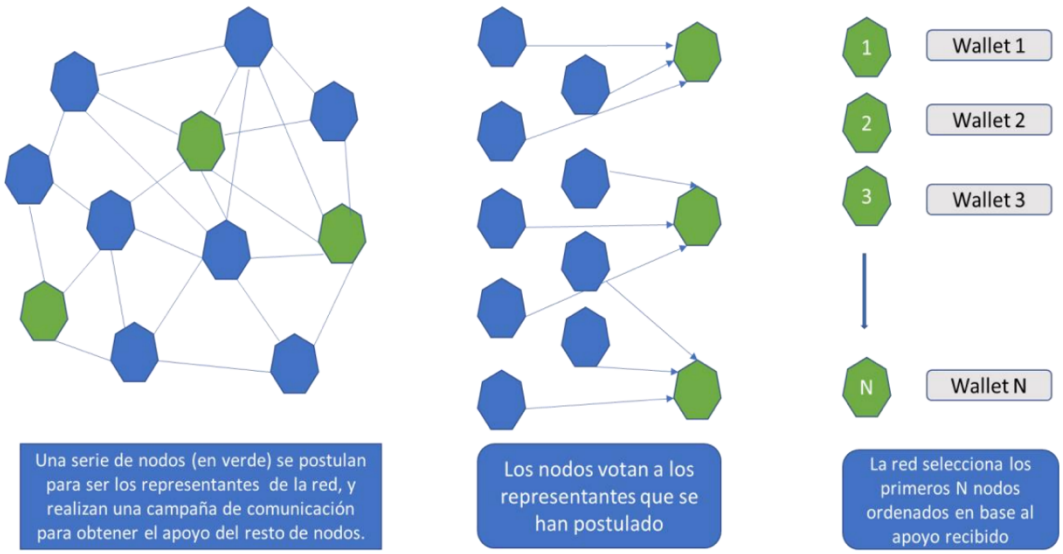


Figura 5. DPoS, Modo de selección del nodo representante y toma de decisión

Fuente: Campaña Iza, X. M., & Zumba Sampedro, W. X. (2020). Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo (Bachelor's thesis, Quito: UCE).

Otro posible método de consenso es la Prueba de Participación Alquilada o LPoS. Se trata del método de consenso PoS pero con una funcionalidad añadida: el arrendamiento. Permite que los nodos con menor participación alquilen fondos a nodos más enriquecidos, consiguiendo así una mayor participación y, por tanto, más posibilidades de ser elegidos de entre el resto de nodos para ser el encargado de crear y verificar el nuevo bloque. Al acabar su función, divide la recompensa con el que le arrendó sus fondos.

Por último, hablaremos de Tolerancia Práctica de Fallas Bizantinas o por sus siglas: PBFT. En este proceso se busca la participación de todos los nodos en la votación de qué

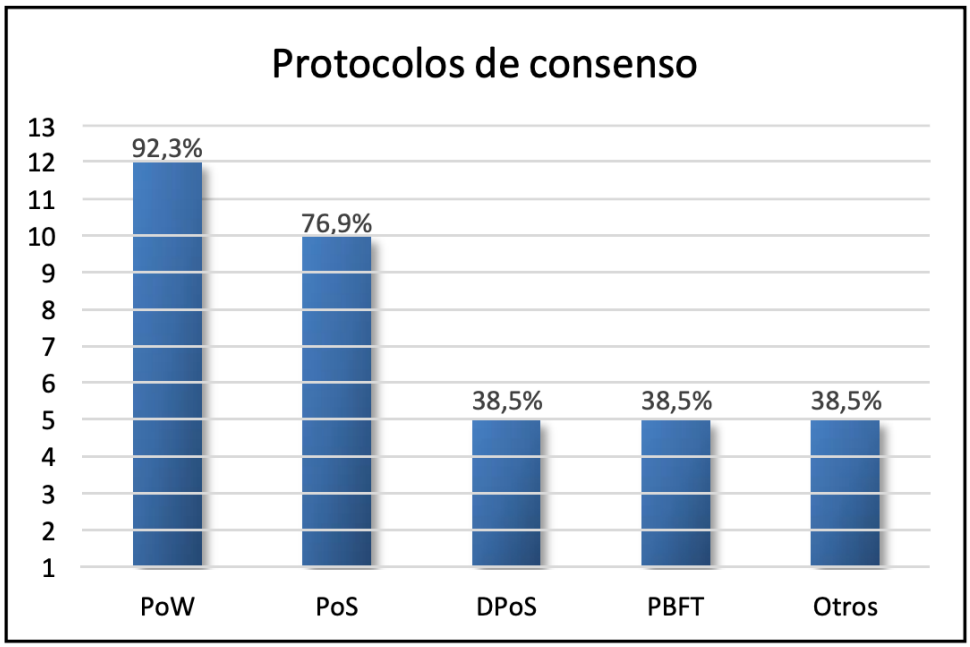
[16] CAMPAÑA IZA, X. M., & ZUMBA SAMPEDRO, W. X., "Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo", Tesis doctoral, Quito: Universidad Central del Ecuador, 2020.

bloque debe ser el siguiente agregado a la cadena de bloques. Al conseguir cualquiera de los bloques al menos 2/3 de los votos se da por finalizada la votación.

Se trata de un algoritmo poco común y utilizado sobretodo por NEO. Sus mayores ventajas son la seguridad que ofrece, su escalabilidad, su eficiencia y robustez. Sin embargo, se trata de un protocolo que lleva poco tiempo en el mercado y por tanto es poco utilizado, además tiende a la centralización y no respeta el anonimato de las transacciones[17].

En la siguiente imagen se muestran los métodos de consenso más utilizados y que han sido explicados anteriormente en el presente documento. Como ya se ha dicho los métodos PoW y PoS lideran la mayoría de procedimientos. Concretamente la imagen hace referencia al número de estudios en los que aparecen los principales protocolos de consenso.

FIGURA 4: PROTOCOLOS DE CONSENSO

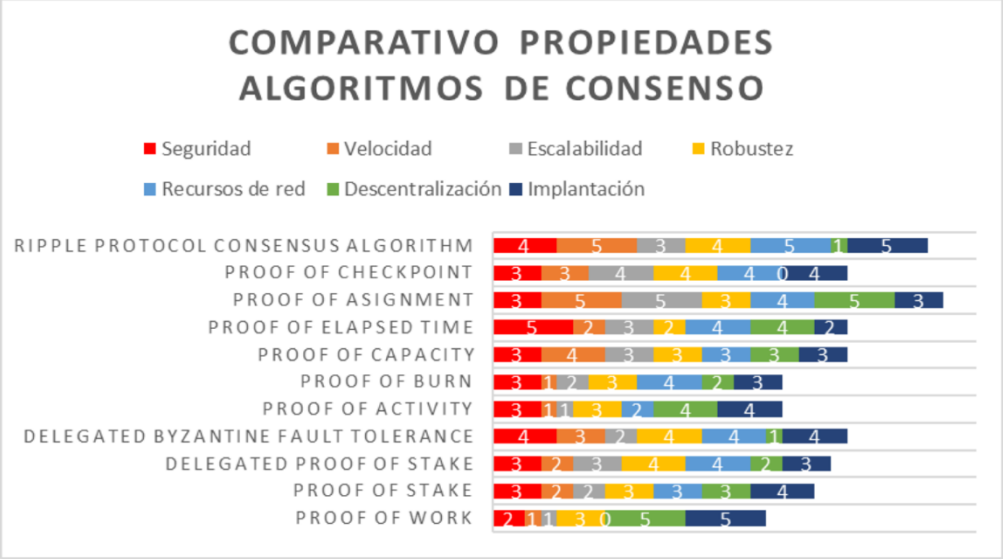


Fuente: HOLGUÍN MENDOZA, J. D., "Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática", Trabajo de fin de grado, 2021, p.7

[17] AMORES MARTÍNEZ, A., "Blockchain, algoritmos de consenso", Trabajo Fin de Máster, Universitat Oberta Catalunya, 2020.

En la siguiente imagen se muestra una comparación gráfica de las propiedades de cada método de consenso, incluyendo otros menos utilizados además de los ya explicados.

FIGURA 5: COMPARACIÓN DE LAS PROPIEDADES DE LOS MÉTODOS DE CONSENSO



Fuente: HOLGUÍN MENDOZA, J. D., "Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática", Trabajo de fin de grado, 2021, p.7

3.5.1. Propiedades del consenso

A pesar de existir múltiples métodos de consenso, todos y cada uno de ellos pretenden garantizar una serie de propiedades clave que les dote de eficacia y utilidad. En este apartado, destacaremos algunas de ellas, las más comunes e importantes: la seguridad, la capacidad de respuesta y la tolerancia[18].

La seguridad la otorga el acuerdo final de los nodos. Este garantiza que las transacciones no se desnaturalicen ni sean contabilizadas doblemente o cualquier otro tipo de fraude. El

[18] VIRIYASITAVAT, W., & HOONSOPON, D., "Blockchain characteristics and consensus in modern business processes", *Journal of Industrial Information Integration*, vol. 13, 2019, pp. 32-39.

sistema de consenso permite que la información de la red sea universal y transparente, además de accesible a sus usuarios. Hay consistencia entre los métodos de consenso y los protocolos a seguir por los nodos, de forma que se genera una cohesión en la actividad general.

La capacidad de respuesta hace referencia a la capacidad de los nodos de validar, transmitir y almacenar las transacciones contenidas dentro de los bloques válidos. Los procesos computacionales dan lugar a una respuesta que genera valor para la cadena de bloques.

Por último, sobretodo el sistema PoW, garantiza tolerancia a los fallos pues su método de consenso los diluye siempre y cuando los nodos defectuosos ocupen una minoría del total. Estos fallos abarcan tanto las acciones maliciosas como los fallos de parada o colisión y los fallos bizantinos[19].

3.5.2. Ataque del 51%

Se trata de un ataque dirigido a las Blockchain que trabajan con el método PoW. Como hemos mencionado en el apartado anterior, el método de prueba de trabajo otorga al nodo de mayor poder computacional la posibilidad de añadir el bloque verificado al libro mayor de Blockchain. Por tanto, podemos destacar el riesgo que supone esto para aquellas redes más pequeñas, ya que un solo participante puede hacerse con el control de la misma[20].

En un ataque del 51% uno o más mineros poseen más de la mitad del poder computacional de una red Blockchain. Esto les permite impedir de forma maliciosa el registro o validación de las transacciones incluidas en los bloques que están minando. También afecta al resto de usuarios pues se les impide participar o, directamente, se incluye en la cadena de bloques una transacción que no es real.

Un ejemplo podría ser Etherum classic, que sufrió este ataque en 2019. Este reorganizó 11 bloques y permitió a los atacantes gastar dos veces 1.1 M dólares, lo que supone un fraude de gran entidad para la plataforma y sus usuarios.

---

[19] Íd.
[20] NAWARI, N. O., & RAVINDRAN, S., "Blockchain technology and BIM process: review and potential applications". *J. Inf. Technol. Constr.*, vol. 24, nº 12, 2019, p. 216.

Por otro lado, Bitcoin sb, una bifurcación de la cadena Bitcoin, lo sufrió recientemente en el año 2021. Atacaron 100 bloques y borraron aproximadamente 10 horas de transacciones, una gran pérdida no solo de veracidad sino de inversión en coste computacional.

No parece que el legislador haya hecho ninguna referencia en la Ley o en jurisprudencia contra este tipo de ataques del 51%. Pero sus actos si parece que puedan generar responsabilidad penal en EEUU. Sin embargo, es innegable que comporta un fraude en casos en los que sea la mala fe la que promueva este tipo de actuaciones en lugar de ser el resultado natural de una prueba de consenso de Blockchain.

De todos modos, la red Blockchain se protege de este tipo de ataques por su propia naturaleza. El alto coste computacional que exige a sus nodos importantes inversiones monetarias no permite que estos ataques puedan darse de forma frecuente y les resta realmente sentido, ya que no compensa económicamente. Si se quisiera introducir un error de forma maliciosa es perfectamente posible, pero no prospera debido al coste que implica mantenerlo, es decir, el coste de validar constantemente antes que el resto de nodos todos los bloques y recibir apoyo del resto o conformar de forma individual un porcentaje superior a la mitad (51%).

3.6. Tipos de Blockchain según su privacidad

Las cadenas de bloques pueden variar entre sí en función de dos factores, según el nivel de apertura de la cadena y según nivel de permisos necesarios para agregar información[21]. Según el nivel de apertura de la cadena distinguiremos entre cadenas públicas y cadenas privadas. A la hora de analizar el nivel de permisos necesarios para agregar información, distinguiremos cadenas *permissioned* y cadenas *permissionless*.

Las Blockchain públicas se caracterizan por el hecho de que cualquiera puede acceder a ellas y a sus transacciones, lo que las dota de una innegable transparencia. Sus usuarios son anónimos y los nodos no tienen por qué identificarse. Aunque no pueda identificarse a los usuarios sí son rastreables las transacciones que realicen.

[21] VILALTA NICUESA, A. E., *Smart legal contracts y blockchain*, Wolters Kluwer, Madrid, 2019.

Además de públicas, pueden ser *permissionless* o *permissioned*. En las cadenas públicas *permissionless* cualquier usuario podrá crear bloques y realizar transacciones. Ejemplos de las mismas son Bitcoin y Ethereum. Las cadenas públicas *permissioned* reservan a un grupo concreto de usuarios la creación de bloques y el procesado de transacciones. Un ejemplo de estas serían las plataformas BigchainDB o Multichain.

Por otro lado, en las cadenas de bloques de corte privado los permisos de escritura corresponden a una sola organización y los de lectura serán centralizados o públicos[22]. Una posible aplicación sería en el sector de la auditoría y en otros mercados específicos. Solo pueden crearse redes privadas *permissioned* puesto que hacerlas *permisionless* sería contradictorio.[23]

3.7. Ethereum

Creada por Vitalik Buterin en 2015, Ethereum se presenta como una plataforma de código abierto que busca mediante el uso de la tecnología Blockchain el desarrollo de aplicaciones descentralizadas o DApps.

Basándose en su predecesora Bitcoin, la plataforma de Vitalik ofrece a sus usuarios la posibilidad de construir sus propias aplicaciones y operaciones. Deja a un lado las meras transacciones con las que trabajaba Bitcoin y amplía el espectro[24]. Podemos decir que Ethereum surge como una mejora del protocolo de Bitcoin, es decir, dota a su código de mayor inteligencia y simplifica su programación, de forma que queda accesible para cualquier desarrollador[25].

Esta es una de las plataformas más conocidas que utiliza la tecnología Blockchain. A diferencia de Bitcoin, que se centra únicamente en operaciones de transacciones monetarias sin necesidad de terceros ajenos involucrados, Ethereum es una plataforma que busca dar cabida a aplicaciones descentralizadas como son los Smart Contracts.

---

[22] PARRONDO, L., "Tecnología Blockchain, una nueva era para la empresa", *Revista de contabilidad*, vol. 27, 2018, p. 8.
[23] ROCO SALAS, Á., "Estudio sobre Smart Contracts en Ethereum", Trabajo fin de grado, Universidad Carlos III de Madrid, 2019, p.23.
[24] ROMERO SOLÍS, J., "Aplicaciones de contratos inteligentes en Ethereum", Trabajo fin de grado, Universidad Carlos III de Madrid, 2019, pp. 1-78.
[25] ROCO SALAS, Á., "Estudio sobre Smart Contracts en Ethereum", Trabajo fin de grado, Universidad Carlos III de Madrid, 2019, p.23

La plataforma Ethereum cuenta con su propia moneda, equivalente a la criptomoneda de Bitcoin, el Ether (ETH). Esta es utilizada tanto para realizar pagos y transacciones como para ser la retribución que la propia plataforma ofrece de forma interna a los mineros y programadores de la misma. Es un incentivo de calidad de su servicio[26].

El objetivo de Ethereum es garantizar la simplicidad, la universalidad, la modularidad, la agilidad y la permisividad. Para proporcionar todas y cada una de ellas, desde su protocolo busca dar la mayor simplicidad posible, permitiendo así que este al alcance de cualquiera la posibilidad de utilizar la app, dándole una mención social. De igual forma, a nivel interno utiliza un lenguaje informativo accesible para la mayoría de programadores, lo que la dota de universalidad.

La modularidad dota al sistema de la posibilidad de flexibilidad con respecto a los cambios que afecten a bloques individuales, además de permitir la retroalimentación de todo el sistema con respecto a estos cambios.

Su agilidad se ve reflejada en la simplicidad y la modularidad combinadas, es una plataforma que acepta la modificación y no la dificulta. Además, su permisividad otorga a sus usuarios la posibilidad de implementar infinitud de aplicaciones descentralizadas así como de modificarlas.

3.8. Ventajas y desventajas del uso de la tecnología Blockchain

Comenzaremos el presente apartado analizando las ventajas que ofrece el sistema y posteriormente serán comentados sus límites.

La cadena de bloques ofrece entre otras cosas seguridad. La encriptación que utiliza y sus sistemas de funcionamiento evitan en gran medida las posibilidades de ataque y manipulación, ya que todo está a la vista de todos y los cambios se realizan mediante los

[26] MIRANDA PALACIOS, V., "Explorando la Blockchain de Ethereum y el desarrollo de Smart Contracts", Tesis doctoral, Universitat Politècnica de Catalunya, 2018.

métodos de consenso preestablecidos. Cualquier modificación queda registrada y afecta a los elementos fundamentales del bloque, como puede ser su número hash.

Otra característica de la Blockchain es que, gracias a su metodología de transparencia total, dota a la plataforma que la incorpore de una confiabilidad muy fuerte por parte del usuario.

Además, la descentralización del sistema y su autoejecutabilidad supone la disminución y eliminación de los costes antes preceptivos de aquellos intermediarios necesarios para validar las operaciones. Esto no solo se percibe en un ahorro monetario, sino además, en un ahorro de tiempo considerable, pues elimina los tediosos tiempos de espera de tramitaciones. La digitalización de estos procesos aporta también la reducción de los posibles errores humanos a los que podían estar sometidas las operaciones, dotándolas así de una mejor calidad y mayor efectividad.

Por último, su autoejecutabilidad dota a los contratos inteligentes de integridad en cuanto a sus resultados. No cabe el incumplimiento, pues el cumplimiento queda garantizado y las partes se obligan en este sentido o asumen las consecuencias de la digitalización jurídica.

Pasando a aquellas características por las que la Blockchain y los Smart Contracts pueden verse limitados, destacaremos en primer lugar la poca transparencia de los mecanismos de consenso. Al no haber una figura centralizada en la que depositar de forma ciega la confianza en su buen funcionamiento, los usuarios de las plataformas que instauran Blockchain se ven sometidos al método de consenso elegido en cada cadena. La información dependerá del almacenamiento y capacidad de transmisión de los nodos y el procesamiento de las mismas será limitado en función de la saturación del sistema. Además, el método de consenso puede otorgar un poder de negociación desequilibrado.

Así mismos, los ataques de hackers siguen siendo posibles, además de aquellos que puedan iniciarse desde dentro de la propia plataforma. La seguridad del sistema está en parte en manos de que ningún nodo maligno goce de una capacidad computacional mayor a la que pueda tener la mitad de nodos y mineros. La Blockchain, además, debido a su

novedad habrá de invertir en procesos que le permitan detectar vulnerabilidades del sistema.

Por último, debido a la flexibilidad que ofrece cada tipo de cadena de bloques, los usuarios habrán de ver garantizado su derecho de protección de datos pese al carácter abierto del sistema. A día de hoy se apuesta por la indistinguibilidad en lugar de por la ofuscación, dado lo complicado de garantizar esta última de forma completa.

3.9. Otras disputas comunes

En este apartado vamos a analizar los principales problemas que el uso de este tipo de contractos está generando con respecto a los efectos entre sus partes y para con el resto de la comunidad. Habiendo analizado en el apartado anterior las principales ventajas y desventajas, los ejemplos que aquí se expondrán serán casos comunes a los usuarios.

Debido al carácter automático de los Smart Contracts y a su independencia con respecto a actuaciones de terceros intermediarios, se potencian los riesgos y consecuencias de que el objeto dispuesto en el mismo sea ilícito. Y es que a pesar del desconocimiento del funcionamiento de las plataformas como Ethereum o Bitcoin debido la poca información manejada por el ciudadano común, estos acuerdos siguen estando sometidos a las normas del tráfico regular de los contratos. Es por este carácter de desconocimiento generalizado por lo que algunos usuarios han utilizado la Blockchain para crear contratos inteligentes con objetos ilícitos. Un ejemplo de esto fue el caso de SilkRoad[27], donde a través de transacciones de Bitcoin se daba la compraventa de objetos ilegales. Estas compraventas incluían documentos falsificados, armas y drogas. La nota de anonimato de los usuarios y la protección de las operaciones realizadas dificultó mucho el rastreo.

Es por ello que, la validez de los contratos inteligentes ha de estar sometida a algún tipo de control jurídico que proteja al usuario e impida los actos ilícitos.

[27] MITRE ABUHAYAR, C., ALONSO ALLENDE, J., ESCAURIAZA, M., GONZALO, J., MÁRQUEZ, R., & MORENO GARCÍA, F. J., "Descifrando la blockchain", *Nuevas Tendencias,* nº 100, 2018, pp. 33-38.

Controversias como el caso fortuito o la fuerza mayor[28] afectan a los usuarios de los Smart Contracts y comportan serias dificultades con respecto al carácter autoejecutable de los contratos. Esto solo puede solventarse creando contratos inteligentes muy completos, que prevean toda clase de situaciones que puedan afectar a la viabilidad de consecución de su objeto y que establezcan pasos a seguir o consecuencias derivadas. Para lograrlo, se ha de investigar sobre la naturaleza del contrato así como la situación de las partes, para posteriormente plasmar en la versión digital todo aquello que sea pertinente.

El lenguaje binario por el que se rigen los Smart Contracts, dificulta además la verificación de cláusulas referentes a casos fortuitos o de fuerza mayor, ya que estos requieren de una cierta interpretación y no pueden enumerarse taxativamente por la infinitud de posibilidades. Esto elimina la independencia de los mismos y su autoejecutabilidad[29].

4. SMART CONTRACTS

4.1. Concepto

Aunque ya hemos venido utilizando el término Smart Contract en este apartado estableceremos más formalmente sus características.

Los Smart Contracts o contratos inteligentes son programas autónomos que se ejecutan en toda la red de Blockchain. Ejecutan los algoritmos que en ellos se codifiquen[30].

Sin embargo, la forma de definirlos difiere considerablemente según el enfoque de aquel que los estudie. Informáticos y juristas tienen percepciones considerablemente distintas de aquello que caracteriza de forma inmediata a los contratos inteligentes. Para un jurista no deja de ser un acuerdo de voluntades entre sujetos de derecho que se obligan ante una

[28] El Código Civil Español establece que nadie responderá de aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables, son los casos fortuitos o aquellos que suceden por fuerza mayor

[29] CATALÁN, J. C., "Los smart-contracts y el arbitraje. Una introducción.", *Ius et Tribunalis*, 2019, pp. 1-7.

[30] MORALES-MORALES, M., ROSERO-CORREA, L., & MORALES-CARDOSO, S., "Registro de títulos académicos mediante una aplicación basada en Blockchain y Smart Contracts", *Cátedra*, vol. 3, nº 2, 2020, pp. 73-98.

causa, sin embargo, todo él se expresa a través del lenguaje en código que le otorgue ejecutabilidad en una cadena de bloques.

Debemos aclarar que este tipo de contratos no conforma una nueva categoría o tipología de los mismos, sino que se diferencia por su soporte digital y lenguaje codificado, además de por su directa relación con la cadena de bloques [31]. En ningún caso conforma otro tipo negociable, por lo que su naturaleza jurídica no se verá modificada, solo afectada por la novedad digital[32].

Gracias a la oportunidad que Blockchain ofrece para ejecutar scripts autónomos, estas funcionalidades se han ido incorporando a todo tipo de aplicaciones descentralizadas. Un claro ejemplo de las ventajas que ha supuesto en el mundo jurídico la incorporación de los contratos a la cadena de bloques es la eliminación de terceros que antes eran necesarios para validar sus contenidos y garantizar su inmutabilidad.

Con este nuevo formato de contrato que ha aparecido gracias al avance de la tecnología, surgen nuevas necesidades jurídicas que el legislador habrá de solventar mediante la regulación de los nuevos supuestos que su uso provoque.

4.2. Orígenes

Sin embargo este concepto de contrato inteligente es previo al desarrollo de la Blockchain y a la creación de Bitcoin. Fue introducido por Nick Szabo, quien lo definió como "un protocolo de transacción computerizada que ejecuta los términos de un contrato"[33], en otras palabras la automatización de los efectos de los contratos mediante las técnicas digitales.

Tal digitalización comienza a través del modelo condicional "If… then…", es decir, si se da por cierta una condición entonces se producirá una consecuencia de forma automática. Entonces cumplida una condición, el contrato ejecuta el bloque de instrucciones

[31] VILALTA NICUESA, A. E., *Smart legal contracts y blockchain*, Wolters Kluwer, Madrid, 2019, pp. 28.
[32] Íd.
[33] SZABO, N., "Formalizing and securing relationships on public networks", *First Monday*, vol. 2., nº 9, 1997, p. 1.

siguiente[34]. Así un contrato que en la mayoría de casos habrá sido previamente redactado en lenguaje natural, podrá codificarse mediante el software adecuado[35]. El cumplimiento ya no dependería de las partes, sino que sería la propia red Blockchain la que autoejecutaría la consecuencia al cumplirse los requisitos requeridos.

Soluciones como el arbitraje quedarían obsoletas[36], ya que el cumplimiento forzoso dejaría de existir puesto que el contrato hace que se cumpla la pretensión de manera inmediata. Sin embargo, existen supuestos que aún precisan de aclaraciones legales con respecto a la complejidad de los mismos en el ámbito digital. Un ejemplo de esto podría ser el cumplimiento defectuoso de la obligación establecida.

4.3. Conexidad, contratos vinculados y contratos complementarios

4.3.1. Conexidad

Los contratos, a pesar de su independencia y autonomía, pueden estar vinculados a otros contratos que de igual forma serán independientes y válidos. Sin embargo, esta relación que viene dada por algún tipo de finalidad común, es susceptible de generar derechos y deberes interdependientes.

Podemos destacar entonces dos elementos necesarios[37]: la autonomía de los contratos y su finalidad compartida. Serán autónomos ya que sin autonomía no habrá validez y sin esta no podrá hablarse de efectos o conexidades respecto a otros contratos, pues no existiría ningún contrato. Por otro lado, la conexidad vendrá dada por la finalidad en común. Esta señalará que uno de los contratos ha de haber sido determinante para que el otro logre su fin.

Con respecto al modo en que habrán de ser interpretados, esto se hará de forma completa, es decir, uno a través del otro. Esto se debe a que se ha establecido una relación de interdependencia, que por mínima que sea, genera efectos de uno sobre otro.

---

[34] LUQUE RESTREPO, D., "Análisis de las obligaciones condicionales en la implementación de Smart Contracts en el ordenamiento jurídico colombiano", Tesis para obtener el título de Abogado, Escuela de Derecho y Ciencias Políticas de Medellín, 2020.
[35] SANZ BAYÓN, P., "Smart Contracts: la aplicación Blockchain que mejorará la eficiencia del mercado" *Diario Abierto*, 2018.
[36] Íd.
[37] SÁNCHEZ HERRERO A., "Contratos celebrados por adhesión a cláusulas generales predispuestas, en Tratado de Derecho Civil y Comercial", Ed. *Thompson Reuters La Ley*, vol. 3, 2016, p. 566.

Algunos autores establecen dos tipos de conexidades, la conexidad genética y la conexidad funcional.

La conexidad genética atiende a la formación del contrato, es decir, a su primer estadio de diseño y creación. Supone que uno se crea o establece a partir del otro. Un ejemplo podría ser el contrato preliminar y el contrato definitivo[38].

Por otro lado, la conexidad funcional será bilateral o unilateral[39]. La diferencia entre ambos tipos la establece el rango de los contratos. Esto hace referencia a la dependencia o interdependencia que pueda establecerse. Si existen dos contratos y uno de ellos puede considerarse accesorio al otro, es decir, que existe un contrato "principal", entonces la relación que se establecerá será de dependencia y todo lo que afecte al principal afectará al accesorio. Por el contrario, una relación de interdependencia entre dos o más contratos en la que no se distinguen por rango, es decir, no existe ni contrato principal ni contrato accesorio, será clasificada con una conexidad unilateral.

Para finalizar, si acudimos a la fuente que inspira el contrato, la conexidad podrá ser convencional si surge por acuerdo de las partes o, por otro lado, legal en caso de que haya sido el legislador quien lo haya establecido. También podrá ser objetiva en el caso de que sea el objeto al que se refieren aquello que les de la nota de conexidad[40].

4.3.2. Contratos vinculados

Se trata de un tipo de conexidad que únicamente hace referencia a contratos vinculados por operaciones de financiación y de adquisición.

Podemos destacar a tres partes que participan en los mismos. Dos de ellas se obligan mediante un contrato de compraventa. Dicha compraventa quedará inevitablemente sujeta a otro contrato de crédito por el cual una de las dos partes anteriores obtendrá financiación de un tercero. Este tercero participará también de la conexidad de los contratos puesto que se obligará mediante el préstamo monetario ante una de las partes sujetas al contrato

[38] BIANCA, M., *Derecho civil III: el contrato*, Universidad Externado, Colombia, 2007.
[39] SÁNCHEZ HERRERO A., "Contratos celebrados por adhesión a cláusulas generales predispuestas, en Tratado de Derecho Civil y Comercial", Ed. *Thompson Reuters La Ley*, vol. 3, 2016, p. 566.
[40] BERNAD, R., "A propósito de una pretendida teoría general de los contratos conexos", *Revista Crítica de Derecho Inmobiliario*, nº 720, 2010, pp.1447-1484.

de compraventa. Podrá realizarse de forma simultánea o sucesiva, lo que es determinante es la relación que se establece, no el momento temporal.

Con respecto a posible jurisprudencia referente a este tipo de conexidades, la Sección 16ª de la Audiencia Provincial de Barcelona dictó sentencia el 27 de marzo de 2018[41] analiza las excepciones procesales del consumidor en los contratos vinculados de venta de bienes y de financiación. Esta audiencia se basa en la doctrina fijada por la Sala 1ª del TS y en la sentencia de 24 de noviembre de 2016.[42]

Si bien, los Smart Contracts quedarán afectados de igual forma que los contratos tradicionales ante este tipo de vínculos. Son más susceptibles de uniones ya que la cadena de bloques tiende a interrelacionar todos sus componentes debido a su carácter de inflexibilidad y autoejecutabilidad.

4.3.3. Contratos complementarios

La Ley 9/2017 de Contratos del Sector Público[43], por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/24/UE[44] y 2014/23/UE,[45] de 26 de febrero de 2014, establece en su artículo 29.7 una definición para los contratos complementarios.

Según esta ley, los contratos complementarios serán "aquellos que tienen una relación de dependencia respecto de otro, el principal, y cuyo objeto se considere necesario para la correcta realización de la prestación o prestaciones a las que se refiera dicho contrato principal". Por esta definición los asemejamos a los contratos de conexidad funcional que hemos explicado anteriormente, sería equivalente a la conexidad unilateral.

El contrato accesorio quedará sujeto al principal y el desistimiento del segundo provocará la extinción automática del primero. Un ejemplo de esta relación llevada al campo de los

[41] Sentencia de la Audiencia Provincial núm. 2219/2018, de 27 de marzo.
[42] Sentencia del Tribunal Supremo núm. 5165/2016, de 24 de noviembre.
[43] Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (BOE 9 de noviembre de 2017), por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
[44] Unión Europea. Directiva (UE) 2014/24 del Parlamento Europeo y del Consejo, de 26 de febrero de 2014 sobre contratación pública y por la que se deroga la Directiva 2004/18/CE.
[45] Unión Europea. Directiva (UE) 2014/23/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014 relativa a la adjudicación de contratos de concesión.

Smart Contracts sería el contrato que se establece por el desarrollador con la plataforma Ethereum y el que a su vez firma con el usuario que solicita sus servicios. Hay una relación de tres partes y la relación con Ethereum no tiene funcionalidad si el usuario desistiera de su voluntad de contratar al desarrollador para sus fines privados.

4.4. Oráculos

Los oráculos conforman un servicio que proporciona a la Blockchain un suministro de información externa constante. La funcionalidad de los mismos reside en la conexión que establecen entre distintas interfaces de programación.

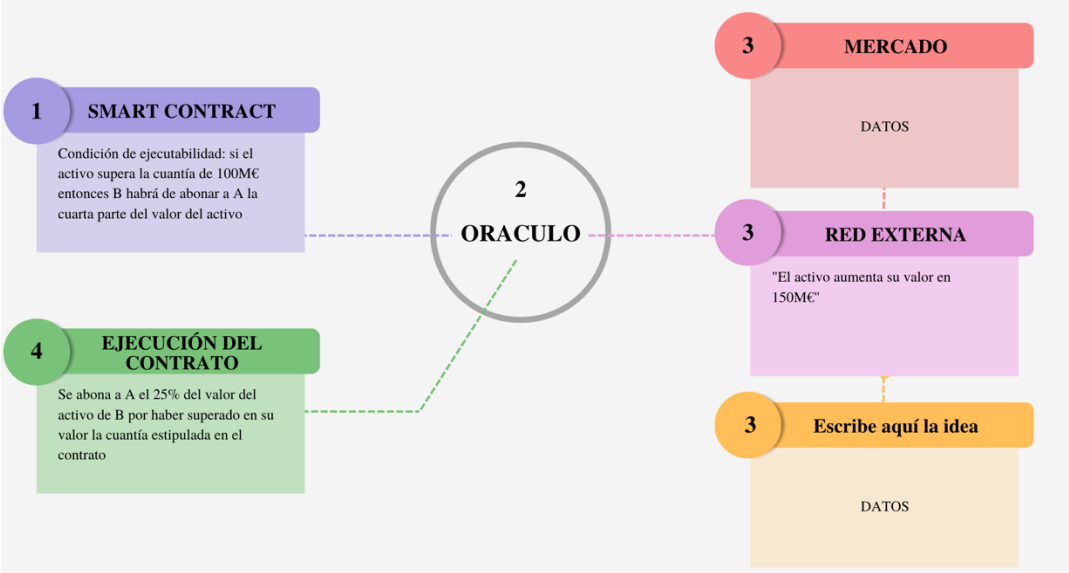
Principalmente están diseñados en la Blockchain para dar soporte a los Smart Contracts, aliviándola así de carga de trabajo. Los términos de los contratos pueden estar subordinados a cambios en variables externas a la Blockchain, como podría ser la subida de tipos de interés. Es por ello que los oráculos, mediante la consulta y verificación de la información, permiten que se ejecuten las consecuencias previstas en dichos Smart Contracts en caso de que los cambios detectados sean vinculantes según lo dispuesto en sus cláusulas.

Los contratos por sí solos están obligados a interactuar únicamente con la propia red de Blockchain, es decir, necesitan de la acción de los oráculos para obtener información de la red externa[46].

Sin embargo, puestos a analizar los objetivos básicos de los creadores de las plataformas Blockchain, los oráculos configuran un servicio provisto por terceros, ajenos a Bitcoin, Ethereum, etc. Es por ello que el sistema acaba necesitando de intermediarios en aquellos casos en los que las aplicaciones desarrolladas estén sujetas a datos externos cambiantes, perdiendo así parte de esa promesa de servicio descentralizado. Sería un añadido en costes e incluso en cuestiones de confianza[47].

[46] CAÑAR UYAGUARI, J. C., & JARA JARA, R. V., "Análisis y desarrollo de una aplicación de registro de permisos y ausentismos sobre una Blockchain mediante un Smart Contract desplegado en una testnet de Ethereum", Trabajo de titulación previo a la obtención del titulo de Ingeniero de Sistemas, 2022.
[47] ALGOVIA GARCÍA, Á., "Contratos Inteligentes sobre registros confiables de polución: una propuesta usando dispositivos IoT, entornos de ejecución seguro y oráculos Blockchain", Trabajo Fin de Máster, 2019.

FIGURA 6: PROCESO DE ACTUACIÓN DE LOS ORÁCULOS



Fuente: elaboración propia.

Si bien, es importante destacar que en múltiples ocasiones será necesario disponer de más de un oráculo. Ciertos contratos precisan de varios oráculos de forma que algunos de ellos verifiquen el cumplimiento de las condiciones y otros se encarguen de enviar la orden que ejecuta la respuesta del contrato a dicho evento. Es decir, uno verifica la causa y el otro inicia la respuesta contractual. Si bien cabe la posibilidad de que los oráculos devengan inoperativos, con lo cual también será recomendable que existan oráculos alternativos, de forma que las partes no queden indefensas ante posibles fallos técnicos[48].

4.5. Smart Contracts con elemento internacional

La figura de los contratos inteligentes, así como cualquier documento privado, esta sujeta a la posibilidad de contener elementos internacionales que obliguen a sus partes a regirse por las disposiciones del Derecho Internacional Privado.

En dichos casos en los que existe un elemento internacional dentro del Smart Contract, sus partes encontrarán la jurisdicción por la que habrán de regirse en lo dispuesto en el Reglamento (CE) 44/2001 o también conocido por el nombre de Reglamento Bruselas I y el Reglamento (UE) 1215/2012 o Reglamento Bruselas I bis, como así dicta el artículo

[48] VILALTA NICUESA, A. E., *Smart legal contracts y blockchain*, Wolters Kluwer, Madrid, 2019

26 de la Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico.

De igual forma, a la hora de determinar la ley aplicable al contrato inteligente en cuestión habremos de acudir al Reglamento de Roma I, a su regla general (art. 2) y al resto de disposiciones. Este Reglamento tratará de salvaguardar los intereses de las partes a la hora de resolver el conflicto. De este reglamento se extrae el contenido de su tercer artículo que dispone la posibilidad de las partes de elección de la ley a la que se someterá el contrato[49]. Por tanto, los Smart Contract de índole internacional, así como los contratos tradicionales internacionales podrán elegir el foro de aplicación, siempre evitando ilicitudes que se derivan de este derecho como puede ser el *fórum shopping*.

Para que quede determinada la ley aplicable por voluntad de las partes, habrá de estar contenida en el contrato una cláusula de sumisión expresa que así lo disponga. Podrá versar tanto de los aspectos materiales como de los formales

4.6. Arbitraje electrónico

Todos los acuerdos entre partes están sujetos a vicisitudes y necesitan en algunos casos de intervención cuando las partes entran en conflicto. Para los contratos inteligentes podemos prever dos caminos, el proceso judicial ordinario o el arbitraje.

Si bien, aunque ambos procesos son perfectamente válidos, podemos encontrar en el arbitraje un método que se adecúa al modus operandi de los Smart Contract ya que favorece muchas de sus garantías. Entre otras ventajas, el arbitraje presenta la posibilidad de mantener a ciencia cierta la confidencialidad del acuerdo y las actuaciones de las partes. Además, permite desde el primer momento seleccionar de entre los posibles árbitros uno especializado en el objeto del contrato y en la tecnología empleada. También dota de mayor flexibilidad y rapidez al proceso lo que lo dotaría de efectividad cuasi inmediata[50].

[49] El Artículo 3 sobre la Libertad de elección dicta que: El contrato se regirá por la ley elegida por las partes. Esta elección deberá manifestarse expresamente o resultar de manera inequívoca de los términos del contrato o de las circunstancias del caso. Por esta elección, las partes podrán designar la ley aplicable a la totalidad o solamente a una parte del contrato.
[50] CATALÁN, J. C., "Los smart-contracts y el arbitraje. Una introducción", Ius et Tribunalis, vol. 5, 2019, pp. 1-7.

Las partes habrán de incluir en el acuerdo procedimiento estándar de activación del convenio arbitral que les dote de seguridad y que sirva a posteriori para guiar el modo de actuar en caso de conflicto.

Analizando más concretamente el caso de los Smart Contracts, estos se encuentran en un sistema deslocalizado como es la Blockchain. Siendo esto así, el convenio o la cláusula que determine el arbitraje, podrá tener carácter internacional siempre que existan elementos esenciales que se encuentren vinculados al país a cuya jurisdicción se sometan. Este razonamiento se conoce como la *teoría de deslocalización del arbitraje* de los Smart Contracts. Podemos encontrar su motivación en que las partes al obligarse mediante la Blockchain realmente no han decidido someterse a la ley del lugar en el que se obligaban sino que han huido de lo convencional.

5. ÉTICA DE LOS SMART CONTRACTS

Como es natural y ocurre de forma generalizada, el derecho siempre va por detrás de la sociedad. El legislador no puede adelantarse a los acontecimientos que se puedan ir dando tanto en el campo social como en el del desarrollo de las tecnologías, es por ello que existirá un periodo de tiempo en el que dichos hechos no podrán estar cubiertos por una legislación completa. Además, para que se cree legislación o se provoque en el legislador la preocupación y necesidad de regular nuevas situaciones será necesario que las mismas se hayan asentado en la sociedad y afecten de forma generalizada. Las redes Blockchain son relativamente novedosas, ya que su tiempo de operación es escaso, sin embargo, en ellas se realizan movimientos monetarios de gran entidad y afectan a innumerables particulares y empresas, con lo cual, aunque no se utilicen de forma masiva sí necesitan hoy día una regulación específica.

La falta de legislación entorno a la Blockchain y a los Smart Contracts provoca que ciertos aspectos o bienes jurídicos puedan quedar desprotegidos. La ética creada entorno a ellos pretende señalar qué aspectos no han de quedar olvidados y deben ser protegidos tanto por el legislador cuando regule como por los usuarios en todo momento. En este apartado se señalarán algunos de los puntos más importantes.

La descentralización, característica clave de la cadena de bloques, protege a los individuos del robo de datos masivo y oculto llevado a cabo por la computerización y delegación de los procedimientos en terceros ajenos y poderosos.

David Chaum, uno de los mayores críticos de este robo de datos promovido por la automatización de los negocios, es considerado padre del dinero digital. En su obra "Security without Identification: Card Computers to make Big Brother Obsolete"[51], propone una alternativa al sistema de pagos actual buscando dotar al individuo de la capacidad necesaria para proteger su propia privacidad y seguridad. Además, no debemos olvidar, que el derecho a la intimidad queda consagrado en la Constitución española como fundamental y los desarrolladores de Smart Contracts han de garantizarlo mediante una perfecta confidencialidad.

Sin embargo, esta supuesta seguridad conseguida a través de la descentralización puede verse eclipsada considerablemente por los problemas que entraña la autonomía de la inteligencia artificial. Las limitaciones de los Smart Contract y su carácter inflexible puede provocar la creación en masa de los mismos cayendo en generalidades y perdiendo la clara necesidad del derecho de crear instrumentos específicos que protejan a las partes. Esto afectaría sobretodo a aquellas clases sociales que rechacen acudir a profesionales asesores por motivos económicos y que antepongan obtener el instrumento, aunque suponga perder en cierto modo plasmar su clara voluntad en el acuerdo. De esta forma quedarían obligados a contratos que realmente no constituyen lo que en un principio deseaban acordar ambas partes.

Por otro lado, las criptomonedas han sido objeto de blanqueamiento de capitales, lo cual ha provocado la acción directa del legislador en este nuevo campo tecnológico. Mediante la Directiva 2015/849 de lucha contra el blanqueo de capitales se ha buscado luchar contra todo el anonimato que otorgan las redes Blockchain que se escudan en la necesidad de transmitir confianza hacia el usuario. Si bien es completamente ética la defensa de la protección de datos de los usuarios, así como de las transacciones que realizan, se habrá

[51] CHAUM, D., "Security without identification: Transaction systems to make big brother obsolete", *Communications of the ACM*, vol. 28, nº10, 1985, pp. 1030-1044.

de ejercer un control regulatorio por parte de las autoridades para no favorecer actividades ilícitas financieras. Sin embargo, estas actuaciones han de ser financiadas por el sector público y, de momento, no se están llevando a cabo, lo que resulta natural debido a la gran complejidad, novedad y alto coste de inversión que suponen[52].

El carácter de completa transparencia de los contratos inteligentes trae consigo diversos beneficios para las partes que se someten a ellos. Esto habrá de quedar garantizado por los desarrolladores de los Smart Contract, quienes deberán evitar a toda costa la ofuscación y tratar de plasmar en ellos todas las posibles vicisitudes que puedan darse en el ciclo de vida de los mismos. Será clave la primera fase de diseño del contrato, previa a su desarrollo digital. De igual forma habrán de garantizar la funcionalidad y equilibrio del ecosistema tecnológico de la cadena de bloques y sus componentes[53]. Este carácter ético parte de un principio de transparencia y buen hacer. Algunos autores señalan que aportaría valor y seguridad la posibilidad de obtener informes descargables sobre la actividad de la red concreta.

Otro punto desde la ética a garantizar es el principio de fiabilidad. Este ha de garantizar la veracidad de los datos contenidos, así como la seguridad garantizada de acceso. Además, otros muchos procesos tendrán que estar minuciosamente regulados, un ejemplo sería la necesidad de auditabilidad y rendición de cuentas. De este modo se garantiza que las actividades que utilicen estas tecnologías sean eminentemente lícitas y deje de concebirse a la Blockchain o a los Smart Contracts como nidos de fraude.

También la precaución ha de estar presente en estas nuevas aplicaciones descentralizadas. El sistema y la ley deben prever medidas de precaución ajustadas tras análisis de los posibles riesgos, es decir, dotar de algún modo a la red de sistemas de control generalizados.

Por último, como todos los servicios que se ofrecen en el mundo jurídico, el fin ultimo habrá de ser social. La plataforma y sus aplicaciones habrán de garantizar que se da un

[52] PÉREZ LÓPEZ, X., "Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España", *Revista de derecho penal y criminología*, vol. 3, nº 18, 2017, pp. 141-187.
[53] VILALTA NICUESA, A. E., Smart legal contracts y blockchain, Wolters Kluwer, Madrid, 2019, p. 240.

trato igualitario hacia todos los usuarios y que no prevalezcan los derechos de unos sobre otros. Esto genera gran confusión en la Blockchain cuando hablamos de los métodos de consenso y de los ataques del 51%.

6. RETOS LEGALES, ASPECTOS NO CLAROS

En primer lugar, es necesario destacar que realmente no existe una regulación específica de los Smart Contracts, sino que se hace mención en distintos artículos de diferentes cuerpos normativos sobre el tratamiento legal de los documentos privados electrónicos. Un documento legislativo específico sobre esta materia aportaría una mayor claridad jurídica y con ello crecería la confianza con respecto a este tipo de nuevas formas de obligarse. Sin embargo, no parece que el legislador planee dicha codificación en el corto plazo.

También sugiere gran problemática la codificación digital. El lenguaje jurídico empleado en los contratos tiende a ser muy especifico y concreto, pues esto dota de seguridad y confianza a sus partes. Sin embargo, la codificación y los scripts diseñados para los Smart Contracts son realizados por ingenieros y técnicos profesionales del ámbito electrónico e informático, con lo cual el riesgo de que la traducción computacional no se ajuste en todo su contenido y significado a la versión escrita es bastante alto. Esto reduce considerablemente la seguridad jurídica y eficacia proporcionada por el documento y puede someter a las partes a situaciones de indefensión[54]. Esta sería sin duda un área a regular y proteger por el derecho en mayor medida pero que resulta incompatible en cierto modo con el carácter descentralizado y libre de intermediarios que caracteriza a la Blockchain. Así, no es solo el legislador el que puede mejorar este ámbito, sino también el propio sistema de Blockchain o de plataformas concretas como Ethereum.

Los errores informáticos tampoco quedan descartados y suponen parte del riesgo, puesto que la imposibilidad de retrotraer las consecuencias derivadas de la autoejecución de los contratos supone una situación de indefensión considerable para las partes, que necesitará de acción judicial para ser solventada. Es aquí donde vemos que a pesar de la

[54] PADILLA SÁNCHEZ, J. A., "Blockchain y contratos inteligentes: Aproximación a sus problemáticas y retos jurídicos", *Revista de Derecho Privado*, nº. 39, 2020, pp. 175-201.

independencia sugerida por este tipo de tecnologías, siguen necesitando de una regulación jurídica que cubra sus principales debilidades y proteja al consumidor en casos de error.

Otro reto que destaca dentro de las limitaciones de los contratos inteligentes son las consecuencias derivadas de su inmutabilidad. Como hemos explicado en apartados anteriores, gran parte del éxito de Ethereum, Bitcoin y, en general, de las plataformas que utilizan la tecnología Blockchain es la autenticidad de sus bloques. Estos bloques tienen asociados el código *hash* que los identifica y diferencia del resto de bloques y, sobretodo, es un código que vale únicamente para un bloque, es decir, cualquier cambio producido en dicho bloque conlleva una modificación inmediata de su código *hash* puesto que el bloque ya no es el mismo, ha cambiado. Esto se traduce en una preocupación para el legislador en el sentido de que un contrato inmutable ha de ser perfecto, puesto que goza de autoejecutabilidad y los errores que contenga no podrán ser modificados. Sin embargo, por el contrario, en los contratos tradicionales sus partes son susceptibles de poder añadir cláusulas de mutuo acuerdo que ajusten su contenido a su voluntad. También es común que las partes decidan no realizar un cumplimiento perfecto del contrato sin que quiera decir esto que se ha dado un incumplimiento. Todas estas opciones son imposibles en el área de los Smart Contracts debido a la rigidez de los mismos[55]. Esto realmente es un atraso, ya que impide realizar algo que los contratos tradicionales sí que permiten.

De igual modo, los Smart Contract están sujetos a la independencia de la Blockchain con respecto al "mundo real", es decir, las partes de los contratos pueden verse involucradas en otras muchas situaciones que podrían impedir el cumplimiento del contrato o permutar su fecha de cumplimiento. Un ejemplo podría ser el caso de que la parte deudora entrara en concurso de acreedores y, por tanto, el crédito en manos del acreedor habría de quedar sujeto a las normas del concurso. La autoejecutabilidad en este caso del contrato comportaría un retraso en el proceso además de los problemas de anulabilidad que podría enfrentar o incluso de responsabilidad que podrían afectar a la hora de clasificar el crédito.

[55] PADILLA SÁNCHEZ, J. A., "Blockchain y contratos inteligentes: Aproximación a sus problemáticas y retos jurídicos", *Revista de Derecho Privado*, nº. 39, 2020, pp. 175-201.

7. CONCLUSIONES

Tras el análisis planteado, queda demostrado el innegable potencial de la Blockchain, así como de una de sus aplicaciones descentralizadas como son los Smart Contracts. Este nuevo sistema electrónico tiene infinitud de posibilidades y parece que responde a necesidades presentes en ámbitos profesionales completamente distintos. Es por ello que la información de la que hoy disponemos se renueva de forma constante, ya que al ser un sector relativamente novedoso, sus usuarios y estudiosos constantemente tratan de mejorar el sistema y suplir debilidades.

Pese al potencial de la Blockchain y las claras ventajas y avances que trae consigo, existe un cierto miedo u oscuridad que la rodea. La vaga regulación de la misma deja desprotegidos ciertos bienes jurídicos que en otros ámbitos resultan fundamentales, y esto no aporta ni confianza ni seguridad a los posibles futuros usuarios. De igual forma, ha sido objeto, como otras tantas tecnologías y puestos profesionales, de fraude y blanqueo de capitales, su uso indebido puede eclipsar mediáticamente y de forma injusta la funcionalidad para la que realmente ha sido creada. Por último, todo este desconocimiento y escasez de regulación provoca que solo aquellos con conocimientos informáticos, científicos, jurídicos o personas con posibilidad de acceso a fuentes de información veraces sean los únicos que puedan beneficiarse de sus funcionalidades. Esto lo provoca la complejidad del funcionamiento de la cadena de bloques y la poca publicidad que desde el Estado se le pueda estar dando.

Si la Blockchain ofrece una versión mejorada de los procesos que hoy se dan y está siendo acogida por multitud de particulares, empresas privadas y entidades financieras de gran tamaño, desde el Gobierno se ha de establecer un plan de actuación con respecto a la misma. Esto quiere decir que comienza a ser una necesidad social, que afecta a un gran número de personas y que implica consecuencias de gran entidad.

Será necesario que el legislador analice tanto los Smart Contracts como otras muchas aplicaciones descentralizadas que ya están en uso. De esta forma podrá dotar al sistema de mayor seguridad y solventar aquellos fallos que pueda presentar o que desde los contratos tradicionales se esté abordando mejor. Para ello es sin duda necesaria una gran inversión de tiempo y recursos, ya que son innumerables los retos jurídicos que se

plantean. Sin embargo, esta regulación solo puede ser pospuesta, ya que habrá de darse necesariamente puesto que la cadena de bloques no cesa en su crecimiento.

Cooperación y coordinación serán necesarias también entre juristas y técnicos desarrolladores. Esto mejorará el sistema y las garantías hacia los usuarios, además lo dotará de sentido. Una ciencia necesita de la otra para que esta digitalización no resulte de menor utilidad que los contratos tradicionales. Habrán de garantizar que el contenido y consecuencias de los mismos queden plasmados para cumplir así con el principio de legalidad básico de nuestro ordenamiento jurídico.

Por último, no olvidar que la ética aplicada a los Smart Contracts señalará el camino por el que el legislador habrá de comenzar su estudio de la Blockchain. Como en el resto de ámbitos científicos y sociales, las cuestiones éticas nos muestran el por qué y para qué de las creaciones del hombre, que innumerables veces pierden su razón de ser al crecer de forma desmedida.

8. BIBLIOGRAFÍA

LEGISLACIÓN

[1] Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (BOE 9 de noviembre de 2017), por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

[2] Unión Europea. Directiva (UE) 2014/24 del Parlamento Europeo y del Consejo, de 26 de febrero de 2014 sobre contratación pública y por la que se deroga la Directiva 2004/18/CE.

[3] Unión Europea. Directiva (UE) 2014/23/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014 relativa a la adjudicación de contratos de concesión.

JURISPRUDENCIA

[4] Sentencia de la Audiencia Provincial núm. 2219/2018, de 27 de marzo.

[5] Sentencia del Tribunal Supremo núm. 5165/2016, de 24 de noviembre.

OBRAS DOCTRINALES

[6] ALGOVIA GARCÍA, Á., "Contratos Inteligentes sobre registros confiables de polución: una propuesta usando dispositivos IoT, entornos de ejecución seguro y oráculos Blockchain", Trabajo Fin de Máster, 2019.

[7] AMORES MARTÍNEZ, A., "Blockchain, algoritmos de consenso", Trabajo Fin de Máster, Universitat Oberta Catalunya, 2020.

[8] BERNAD, R., "A propósito de una pretendida teoría general de los contratos conexos", Revista Crítica de Derecho Inmobiliario, nº 720, 2010, pp.1447-1484.

[9] BIANCA, M, Derecho civil III: el contrato, Universidad Externado, Colombia, 2007.

[10] CAMPAÑA IZA, X. M., & ZUMBA SAMPEDRO, W. X., "Métodos de consenso sobre plataformas blockchain: Un enfoque comparativo", Tesis doctoral, Quito: Universidad Central del Ecuador, 2020.

[11] CAÑAR UYAGUARI, J. C., & JARA JARA, R. V., "Análisis y desarrollo de una aplicación de registro de permisos y ausentismos sobre una Blockchain mediante un Smart Contract desplegado en una testnet de Ethereum", Trabajo de titulación previo a la obtención del titulo de Ingeniero de Sistemas, 2022.

[12] CATALÁN, J. C., "Los smart-contracts y el arbitraje. Una introducción", Ius et Tribunalis, vol. 5, 2019, pp. 1-7.

[13] CHAUM, D., “Security without identification: Transaction systems to make big brother obsolete”, Communications of the ACM, vol. 28, nº10, 1985, pp. 1030-1044.

[14] FORERO FORERO, E. A., & MOYANO SOTO, S. D., “Pasos a tener en cuenta para un proceso de implementación del Blockchain en el sector cafetero colombiano”, Trabajo fin de grado, 2020.

[15] HOLGUÍN MENDOZA, J. D., “Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática”, Trabajo de fin de grado, 2021, p.7.

[16] IZA, X. C., SAMPEDRO, X. Z., MORALES, M. M., & CARDOSO, S. M., “Análisis Comparativo de Métodos de Consenso sobre Plataformas Blockchain”, Revista Tecnológica-ESPOL, vol. 33, nº 2, 2021, p. 29.

[17] LUQUE RESTREPO, D., “Análisis de las obligaciones condicionales en la implementación de Smart Contracts en el ordenamiento jurídico colombiano”, Tesis para obtener el título de Abogado, Escuela de Derecho y Ciencias Políticas de Medellín, 2020.

[18] MELA, J. L., & HERRERA, E. J. C., “Tecnologías Blockchain y sus aplicaciones”, Visión Antataura, vol 3, nº 2, 2019, pp. 110-126.

[19] MIRANDA PALACIOS, V., “Explorando la Blockchain de Ethereum y el desarrollo de Smart Contracts”, Tesis doctoral, Universitat Politècnica de Catalunya, 2018.

[20] MITRE ABUHAYAR, C., ALONSO ALLENDE, J., ESCAURIAZA, M., GONZALO, J., MÁRQUEZ, R., & MORENO GARCÍA, F. J., “Descifrando la blockchain”, Nuevas Tendencias, nº 100, 2018, pp. 33-38.

[21] MORALES-MORALES, M., ROSERO-CORREA, L., & MORALES-CARDOSO, S., “Registro de títulos académicos mediante una aplicación basada en Blockchain y Smart Contracts”, Cátedra, vol. 3, nº 2, 2020, p. 81.

[22] MORALES-MORALES, M., ROSERO-CORREA, L., & MORALES-CARDOSO, S., “Registro de títulos académicos mediante una aplicación basada en Blockchain y Smart Contracts”, Cátedra, vol. 3, nº 2, 2020, pp. 73-98.

[23] NAKAMOTO, S., Bitcoin: A Peer-to-Peer Electronic Cash System, Lista de correo de criptografía metzdowd, 2008.

[24] NAKAMOTO, S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, Decentralized Business Review, 2008, pp.1-9.

[25] NAWARI, N. O., & RAVINDRAN, S., “Blockchain technology and BIM process: review and potential applications”, J. Inf. Technol. Constr., vol. 24, nº 12, 2019, p. 216.

[26] PADILLA SÁNCHEZ, J. A., “Blockchain y contratos inteligentes: Aproximación a sus problemáticas y retos jurídicos”, Revista de Derecho Privado, nº. 39, 2020, pp. 175-201.

[27] PARRONDO, L., “Tecnología blockchain, una nueva era para la empresa”, Revista de Contabilidad y Dirección, vol. 27, 2018, pp. 11-31.

[28] PARRONDO, L., “Tecnología Blockchain, una nueva era para la empresa”, Revista de contabilidad, vol. 27, 2018, p. 8.

[29] PÉREZ LÓPEZ, X., “Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España”, Revista de derecho penal y criminología, vol. 3, nº 18, 2017, pp. 141-187.

[30] ROCO SALAS, Á., “Estudio sobre Smart Contracts en Ethereum”, Trabajo fin de grado, Universidad Carlos III de Madrid, 2019, p.23.

[31] ROMERO SOLÍS, J., “Aplicaciones de contratos inteligentes en Ethereum”, Trabajo fin de grado, Universidad Carlos III de Madrid, 2019, pp. 1-78.

[32] SÁNCHEZ HERRERO A., “Contratos celebrados por adhesión a cláusulas generales predispuestas, en Tratado de Derecho Civil y Comercial”, Ed. Thompson Reuters La Ley, vol. 3, 2016, p. 566.

[33] SANZ BAYÓN, P., “Smart Contracts: la aplicación Blockchain que mejorará la eficiencia del mercado” Diario Abierto, 2018.

[34] SZABO, N., “Formalizing and securing relationships on public networks”, First Monday, vol. 2., nº 9, 1997, p. 1.

[35] VILALTA NICUESA, A. E., Smart legal contracts y blockchain, Wolters Kluwer, Madrid, 2019, p. 24.

[36] VIRIYASITAVAT, W., & HOONSOPON, D., “Blockchain characteristics and consensus in modern business processes”, Journal of Industrial Information Integration, vol. 13, 2019, pp. 32-39.

[37] ZOZAYA, C., INCERA, J., & FRANZONI, A. L., “Blockchain: un tutorial”, Estudios, vol 17, nº 129, 2019, pp. 113-126.

RECURSOS DE INTERNET

[38] SANTANA VEGA C., "QUÉ es el BLOCKCHAIN - (Bitcoin, Cryptos, NFTs y más)", 2022 (disponible en https://www.youtube.com/watch?v=V9Kr2SujqHw&t=1054s&ab_channel=DotCSV última consulta el 9 junio 2021)