

# informática **Y** **DERECHO**

**2<sup>A</sup>**  
Época



Revista Iberoamericana de Derecho Informático  
(Segunda Época - Primer Semestre 2020 - Número 8)





# informática **Y** **DERECHO** 2<sup>A</sup> Época

Revista Iberoamericana de Derecho Informático  
(Segunda Época - Primer Semestre 2020 - Número 8)



***DIRECTOR ACADÉMICO***

PROF. MG. BIBIANA BEATRIZ LUZ CLARA

***EDITOR GENERAL***

PROF. DR. JOSE HERIBERTO GARCIA PEÑA

***CONSEJO ASESOR***

***PRESIDENTE DEL CONSEJO ASESOR***

PROF. DR. FEDERICO BUENO DE MATA

PROF. MÁSTER. AUGUSTO HO SÁNCHEZ

PROF. HORACIO FERNÁNDEZ DELPECH

PROF. DRA. MARILIANA RICO CARRILLO

PROF. DRA. MYRNA ELIA GARCÍA BARRERA

PROF. DR. VALENTÍN CARRASCOSA LÓPEZ

***REPRESENTANTE LEGAL***

PROF. MARCELO BAUZA RELLY

*Presidente de la Federación Iberoamericana de Asociaciones de Derecho e Informática*

***COORDINADORES***

LIC. ERNESTO IBARRA SÁNCHEZ

LIC. HUMBERTO MARTÍN RUANI

PROF. DRA. JACQUELINE GUERRERO CARRERA

PROF. DRA. NAYIBE CHACÓN GÓMEZ

PROF. MÁSTER. YOSSELIN VOS CASTRO

## **COMITÉ EDITORIAL**

PROF. DR. FELIPE MIGUEL CARRASCO FERNÁNDEZ

*Profesor de Derecho del Trabajo en la Universidad Popular Autónoma del Estado de Puebla. Doctor en Estudios Legales por la Atlantic International University. México.*

PROF. DR. FERNANDO CARBAJO CASCÓN

*Profesor de Derecho Mercantil de la Universidad de Salamanca. Doctor en Derecho por la Universidad de Salamanca. España.*

PROF. DR. HORACIO ROBERTO GRANERO

*Profesor Titular de Derecho Procesal de la Pontificia Universidad Católica Argentina. Doctor en Ciencias Jurídicas por la Pontificia Universidad Católica Argentina. Argentina.*

PROF. DRA. LAURA NAHABETIÁN BRUNET

*Profesora de Derecho Constitucional de la Universidad Católica del Uruguay. Doctora en Derecho y Ciencias Sociales por la Universidad de la República. Uruguay.*

PROF. DR. LORENZO COTINO HUESO

*Profesor Titular de Derecho Constitucional de la Universitat de València. Doctor en Derecho por la Universitat de València. España.*

PROF. DR. LORENZO MATEO BUJOSA VADELL

*Catedrático de Derecho Procesal de la Universidad de Salamanca. Doctor en Derecho por la Universidad de Salamanca. España.*

PROF. DRA. MÓNICA LASTIRI SANTIAGO

*Profesora de Derecho Mercantil de la Universidad Carlos III. Doctora en Derecho por la Universidad Carlos III. España.*

PROF. DR. NELSON REMOLINA ANGARITA

*Profesor de Derecho Comercial de la Universidad de los Andes. Doctor en Ciencias Jurídicas por la Pontificia Universidad Javeriana. Colombia.*

PROF. DR. RUPERTO PINOCHET OLAVE

*Profesor de Derecho Civil de la Universidad de Talca. Doctor en Derecho por la Universidad de Barcelona. Chile.*

PROF. DRA. TERESA RODRÍGUEZ DE HERAS BALLEL

*Profesora Titular de Derecho Mercantil de la Universidad Carlos III de Madrid. Doctora en Derecho por la Universidad Carlos III de Madrid. España.*

DRA. VILMA SÁNCHEZ DEL CASTILLO

*Letrada de la Corte Suprema de Justicia de Costa Rica. Doctora en Derecho por la Universidad Carlos III de Madrid. Costa Rica.*

**INFORMÁTICA Y DERECHO**  
**REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA)**  
**PRIMER SEMESTRE 2020 - NÚMERO 8**

PRESENTACIÓN .....	9
PRÓLOGO .....	11
MANUEL FERNÁNDEZ MORALES y RODRIGO FRANCO PÉREZ	
<i>Bitcoin no blockchain: censura y centralismo.</i> .....	19
ANAHIBY BECERRIL	
Breve historia de los <i>smart contracts</i> .....	35
DAVID AMADO MONROY	
Entendiendo <i>blockchain</i> , su aplicación y sus implicaciones legales y técnicas .....	53
CLAUDIA ALIN ESCOTO VELÁZQUEZ	
El uso de <i>blockchain</i> para la valoración documental con miras a la conformación de la memoria histórica en México .....	71
MANFRY RAFAEL SIERRA ALEMÁN	
FÉLIX JUAN RIVERA AQUINO	
ALEXIS GERMAN ANTONIUCCI L.C.	
<i>Blockchain: teoría y práctica. Aplicaciones legales y técnicas.</i>	
Los casos de Colombia y República Dominicana .....	83
MARILIANA RICO CARRILLO	
El impacto de <i>blockchain</i> y el COVID-19 en la digitalización de los sistemas de pago. ....	91
OLIVIA ANDREA MENDOZA ENRÍQUEZ	
<i>Blockchain</i> y protección de datos personales.....	107



**PRESENTACIÓN**  
**REVISTA FIADI SEGUNDA ÉPOCA. N° 8**

Estimados lectores de la Revista FIADI 2<sup>da</sup>. Época, nos toca presentar esta nueva edición fruto de un arduo trabajo realizado en situación de plena pandemia, que nos ha golpeado fuerte a todos este año, pero lo hemos logrado y tenemos el gusto de acercarles un tema que pensamos concita el interés de muchos de ustedes que así lo han manifestado y por ello decidimos incorporarlo, referido a Blockchain teoría y práctica, aspectos legales y técnicos.

Nuestro mundo, ya digital, se encuentra en momentos de profundos cambios, donde el uso de las tecnologías y sus posibilidades se han acentuado y multiplicado con motivo del aislamiento obligatorio al que nos vimos sometidos, y que en muchos lugares aún continúa. Por tal razón, fue necesario recurrir a estrategias de trabajo, comercio, educación, medicina y justicia entre otros, por medios digitales algunos muy seguros y otros no tanto.

Hemos tomado conciencia de la importancia de contar con mecanismos que permitan agilizar las transacciones electrónicas de todo tipo en un marco seguro y legal. Es aquí donde ponemos la mirada en Blockchain, por la posibilidad que implica de facilitar las contrataciones, brindándonos una oportunidad para el avance hacia nuevos horizontes.

Espero disfruten de estos artículos seleccionados, y les permitan profundizar en sus conocimientos.

Agradecemos a nuestros lectores, colaboradores autores de artículos y a los evaluadores que nos ayudan con la selección para poder brindar los mejores trabajos en busca de la excelencia.

Saludos cordiales

*Mg. Bibiana B. Luz Clara*  
*Directora*

*Informática y Derecho*  
*Revista Iberoamericana de Derecho Informático*  
(segunda época)

*Domicilio Electrónico en España*  
revista@fiadi.org

*Domicilio Postal en Chile*  
Huérfanos 979, oficina 609  
8320182 Santiago de Chile

*Edita:*

Ratio Legis  
Paseo de Francisco Tomás y Valiente, n.º 14, local 3  
Tel.: (34) 923 227 037  
37007 Salamanca  
www.ratiolegis.net



RATIO LEGIS

ISSN:  
2530-4496

*Informática y Derecho, Revista Iberoamericana de Derecho Informático*, es publicada en los meses de noviembre y mayo de cada año en formatos electrónicos (pdf, epub y mobi) que están disponibles para descarga en la página web:  
<http://www.informaticayderecho.org/>

Una guía para la presentación de manuscritos está disponible en el enlace:  
<http://www.informaticayderecho.org/manuscritos/>

Algunos derechos reservados. Publicada bajo los términos de la licencia:  
Reconocimiento-No comercial-Sin obra derivada.

**PRÓLOGO**  
**REVISTA FIADI SEGUNDA ÉPOCA. N° 8**

*Dr. Carlos De Cores<sup>1</sup>*

Es con mucho gusto que me dispongo a escribir el prólogo del presente número de la Revista de la Federación Iberoamericana de Derecho e Informática. Creo que es muy atinado que la dirección de la Revista haya decidido dedicar este número a estudios sobre *Blockchain*, para contribuir a la descripción y narración de un aspecto sumamente actual de una realidad tan atravesada por la tecnología, tarea que es esencial para derivar de ella reflexiones que orienten un derecho *in fieri*, un ordenamiento en construcción, que no está para nada configurado ni cristalizado.

Es que estamos reflexionando sobre un fenómeno que existe desde hace apenas algo más de una década. En la literatura especializada hay consenso en el sentido de que la fórmula de esta tecnología fue inventada por un sujeto de nombre (real o ficticio) Satoshi Nakamoto y consta en un documento concreto, difundido el 31 de octubre de 2008 (a las 6.10.00 PM (UTC), precisa Anahiby Becerril, de la UNAM, en su artículo “Breve historia de los *smart contracts*”). Por su parte, la idea de “*smart contracts*” tampoco es tan antigua: data de fines de la década de los 90, siendo atribuida a Nick Szabo la paternidad del término, aludiendo a un contrato cuyos términos se vuelcan en un programa de computación y por tanto son cumplidos en forma automática, tal como ocurre – en el ejemplo que utiliza el mismo autor – en una máquina expendedora (*vending machine*), que “vende” una bebida cuando el “comprador” introduce una moneda en la ranura correspondiente. Aquella idea inicial asume una enorme proyección al pensarse en un “*smart contract*” registrado en una “*blockchain*”.

No obstante esta absoluta novedad, el volumen de información a manejar es inmenso, tal vez – en proporción - mayor que el que estaba disponible para la investigación académica tradicional, en soporte papel; esta última implicaba costosos relevamientos bibliográficos y muchas veces largas estadías de estudio en bibliotecas y universidades. Es interesante comprobar que el aparato crítico que respalda toda esa literatura está constituido casi exclusivamente por artículos en formato digital (no en soporte papel, como las investigaciones académicas precedentes) y que están a libre disposición del público en Internet en tiempo real cualquiera sea el lugar del mundo donde hayan sido escritos.

Fenómenos tan recientes adolecen de falta de una disciplina jurídica, por lo que es muy oportuna la iniciativa de reunir en este volumen un conjunto de estudios sobre el tema.

Aparece en primer lugar un artículo de Darío Rivera, Jesús Olivares, Gabriel Sánchez, Karina Toscano y Víctor Sánchez, titulado “Modelo de votación electrónica basada en la tercera generación de *blockchain: Proof Of Stake*”, que contiene un análisis técnico de la evolución de *blockchain* y estudio de la tercera generación. Por su parte Manuel Fernández Morales y Rodrigo Franco Pérez escriben el trabajo titulado “Bitcoin no *blockchain*: censura y centralismo”, cuestionando la posibilidad de que la tecnología *blockchain* sea utilizada más allá de su uso originario en el sistema Bitcoin. El artículo de Anahiby Becerril, “Breve historia de los *smart contracts*”, contiene una exhaustiva recopilación de la evolución del fenómeno. “Entendiendo *blockchain*, su aplicación y sus implicaciones legales y técnicas”, es el título del artículo de David Amado Monroy, en el que describe en forma precisa la tecnología de base del sistema *blockchain*. Claudia Alin Escoto Velázquez en su obra “El uso de

---

<sup>1</sup> Doctor en Derecho por la Universidad Pontificia Comillas de Madrid, Miembro fundador de la Academia Nacional de Derecho del Uruguay, Miembro de la Asociación Iberoamericana de Derecho Privado y Miembro e integrante del Senado Académico de la Academia de Ius Privatistas Europeos. Ocupó el cargo de Vice Rector Académico de la Universidad Claeh.

*blockchain* para la valoración documental con miras a la conformación de la memoria histórica en México”, aporta un ejemplo concreto de uso de la tecnología *blockchain* que va mucho más allá de los usos financieros y monetarios. Manfry Rafael Sierra Alemán, Félix Juan Rivera Aquino y Alexis German Antonucci L.C. han elaborado el trabajo titulado “*Blockchain: teoría y práctica. Aplicaciones legales y técnicas. Los casos de Colombia y República Dominicana*”. Por su parte Mariliana Rico Carrillo nos informa sobre “El impacto de *blockchain* y el covid-19 en la digitalización de los sistemas de pago”, y finalmente Olivia Andrea Mendoza Enríquez refiere a la temática de “*Blockchain y protección de datos personales*”. De modo que se trata de un conjunto de artículos centrados en un mismo tópico: el invento de la tecnología *blockchain*, su uso en la actual sociedad de la información y sus perfiles jurídicos.

Representa para mí un gran honor haber recibido de la FIADI y en particular de su Presidente, mi querido amigo Marcelo Bauzá, a quienes agradezco, el cometido de escribir un prólogo para tan sustanciosos aportes. Soy consciente de que la expresión “prólogo” significa literalmente “palabra que va adelante”, y ello me impone colocarme a la vanguardia de los que ya están en la vanguardia, lugar que lleva consigo una gran responsabilidad.

### ***Blockchain & smart contracts “in a nutshell”***

Entrando en materia, adelantamos que no hablaremos sobre *blockchain* y *smart contracts* más allá de hacer somera referencia a una idea general, porque los artículos son excelentes y el lector podrá encontrar en ellos amplia información sobre el estado del arte.

Sí conviene tener en cuenta desde el comienzo que el contexto en el que nos movemos es el de la sociedad de la información, cuyos elementos esenciales pueden ser deducidos de la Directiva Europea 98/34/CE. La sociedad de la información es caracterizada en esa disposición por una forma especial que asumen las comunicaciones o mensajes entre las personas, consistente en que los mismos son “enviados en el origen y recibidos en el destino mediante aparatos electrónicos de tratamiento (comprendida la compresión digital) y de memorización de datos, y que son enteramente transmitidos, enviados y recibidos mediante cables, medios de radiodifusión, medios ópticos u otros medios electromagnéticos”. Nicolás Negroponte, en su explicativo libro “*Being digital*”, habla de la transformación de los “átomos” en “*bytes*”. Ello connota la idea de un mundo virtual o digital, paralelo al real, que lo refleja y que se vuelve fuente de infinitas relaciones entre ambos mundos, hasta hoy inexistentes.

En ese contexto y en un intento casi irrespetuoso de sintetizar el tema del discurso, puede decirse que *blockchain* o cadena de bloques es un registro (*ledger*) de comunicaciones o mensajes que son generados y transmitidos en una red descentralizada (*distributed*) en base a tecnologías de la sociedad de la información (*technology*). De ahí la sigla DLT (*Distributed Ledger Technology*).

Este sistema permite que esos mensajes digitales transmitidos entre los nodos de la red queden registrados algorítmicamente en forma indeleble y con fecha cierta, no mediante la intervención de un tercero de confianza, como el Estado, un Banco o un profesional habilitado, sino mediante el consenso de una red de nodos coordinados mediante protocolos de base matemática. De modo que el registro no opera bajo el control de un sujeto ubicado en posición central, del cual todos los operadores dependen, llamado en las leyes modelo de CNUDMI sobre comercio electrónico “tercero de confianza”, sino que se constituye en todos y cada uno de los servidores o nodos de la red que participan de la organización que provee el servicio de *blockchain*.

Un registro confiable permite impedir que alguien que figura como titular de un derecho, disponga de él dos veces, que es el principal problema de la circulación jurídica, llamado “doble venta sucesiva” o “*double spending*”. Ello está en la base, por ejemplo, de los registros estatales de la propiedad y de

todos los sistemas de publicidad jurídica. Pero este sistema implica un “tercero de confianza”, en este caso, el Estado. En efecto, la concepción que subyace a las leyes modelo de CNUDMI sobre el comercio electrónico, implica precisamente que es necesario un tercero de confianza que neutralice el peligro de doble enajenación (*double spending*), que en el mundo real se dificulta porque el documento original que contiene la referencia a la titularidad del derecho que se quiere transferir no puede ser falsificado fácilmente, mientras que por el contrario, los documentos digitales, que son los que circulan por Internet y sirven de base al comercio electrónico, son fácilmente copiables hasta el punto que no puede distinguirse una copia de un original. La solución de la CNUDMI se funda pues en la participación de un tercero de confianza que centralice las operaciones, de modo que una vez transferido un derecho registrado, el agente central no volverá a transferirlo, ya que ha registrado la primera transferencia.

En cambio el sistema “*blockchain*” está basado en una técnica de registro descentralizado, “*decentralized ledger technology*”, que ahorra los costos (y los riesgos) de confiar en un agente centralizado. Antes de ser agregado a la cadena, cada bloque conteniendo información digital es controlado, validado y criptografiado por algunos de los nodos (llamados “mineros”), por medio de la solución de una operación matemática, lo que resulta prueba de la operación (*proof of work*). La tecnología *blockchain* permite verificar, aprobar y archivar en todos los nodos de la red, de manera indeleble e inmodificable, los datos de las transacciones en ellos registradas, utilizando una clave criptográfica que se origina a través de la resolución de un problema matemático, sin la necesidad de recurrir a un tercero o a una autoridad central. Se excluye al intermediario (sistema *peer to peer*).

Ello significa que se ha creado un sistema informático basado en Internet, por medio del cual se puede registrar en forma sumamente rápida, barata y segura transacciones sobre bienes, pero no solamente informáticos, sino reales, incluso identificados por medio de la llamada “RFID”, “*Radio Frequency Identification*”, representados por datos digitales. Lo que significa que esta tecnología que subyace al *bitcoin* y en general a las criptomonedas, puede ser utilizada hoy día en forma general para registrar transacciones relativas a todo tipo de bienes.

En un estudio realizado por la Universidad de Cambridge, se enumeran los casos de uso (“*use cases*”) de la tecnología *blockchain*, subyacentes a las criptomonedas. Ellos se clasifican en cuatro categorías: inversión digital especulativa, medio de cambio, medio de pago y “usos no monetarios”, donde “uso no monetario” significa que un sistema propio de la sociedad de la información, como en efecto es el basado en la tecnología *blockchain*, puede ser utilizado para la transferencia de todo tipo de bienes del mundo real, por medio de su representación virtual.

Lo que estamos poniendo de manifiesto es que, así como en el mundo real, la circulación opera a menudo por medio de documentos escritos, la transferencia o el gravamen pueden a partir de la tecnología *blockchain* operar por medio de la representación de los bienes por expresiones alfanuméricas y el registro de la transferencia o gravamen en un registro distribuido, generando una publicidad de la operación que la hace oponible a terceros. Se habla en efecto de los “*tokens*”, representaciones digitales y criptográficas de derechos patrimoniales, que permiten la circulación de los mismos por medio de Internet en una forma segura, fácil, económica y en tiempo real, sirviendo de interfase entre la economía real y la economía digital en forma mucho más radical que la que funcionó en la primera generación del comercio electrónico, que, como vimos, se limitaba a servir de medio de comunicación para el encuentro de la propuesta y la aceptación que perfeccionaban el contrato. Tomando en cuenta la cada vez mayor posibilidad de identificación y registro telemático de los bienes por medio del llamado “Internet de las cosas” (Internet of Things), se percibe que estamos frente a una probable generalización del empleo de esta tecnología para la circulación o el gravamen de cualquier tipo de bien, aun de escaso valor.

En virtud de que la doble enajenación resulta controlada por medio de la tecnología *blockchain*, que

no es otra cosa que un sistema que provee de fecha cierta a las transacciones, impidiendo así la posibilidad de una doble venta sucesiva, es previsible un desarrollo creciente de esta tecnología de circulación jurídica. Es por ello que se habla de los *Smart Contracts*, que connotan operaciones informáticas consiguientes a contratos del mundo real, por medio de las cuales se transfieren derechos por vía de Internet en forma automática.

Diversos autores italianos han afirmado que la tecnología *blockchain* tiene la potencialidad de modificar en tiempos breves, las modalidades tradicionales de estipulación y cumplimiento de muchos contratos comerciales, señalando que es una tecnología destinada a la gestión de transacciones a través de la creación de una base de datos distribuida entre los usuarios de la red.<sup>2</sup>

Originalmente pensada para crear una moneda (*bitcoin*) que no dependiera de ningún Estado ni de ningún Banco, la tecnología *blockchain* ha proyectado entonces su funcionalidad mucho más allá, constituyendo una alternativa para muchos sistemas de circulación de bienes o servicios. El sistema se difunde cada vez más rápidamente desde el sector financiero, donde nació, al energético (para el pago de energía), automovilístico (habilitación del funcionamiento del motor del vehículo contra el pago de cuotas del precio de compra o de leasing), agroalimentario, educativo, etc.

Como se dijo, el “*smart contract*” implica un contrato (esto es, un acuerdo libre de voluntades para intercambiar bienes y servicios sobre la base de la idea de lo justo) cuyos términos se han volcado a un programa informático, o sea, en un código de computación, y en determinadas condiciones, se producirán determinadas consecuencias en forma automática. Este supuesto – y no es ciertamente el lugar para profundizar en ello – pone sobre el tapete uno de los grandes problemas de nuestra materia: la ambivalencia de los términos. Porque la palabra código, en este contexto, significa un conjunto de instrucciones contenidas en un programa de computación que en determinadas hipótesis provocarán determinado resultado. Por ejemplo, al vencimiento de un plazo, generarán una orden de pago o desbloquearán o bloquearán una determinada cuenta, o cualquier otra situación imaginable. Cosa muy distinta al significado del término “código” cuando se emplea intentando denotar la idea de norma jurídica, que establece un deber ser, una regla que orienta una conducta que “debe” conformarse a la misma, pero que no necesariamente lo hará.

Por eso la expresión de Lawrence Lessig, “*code is the law*”,<sup>3</sup> representa un paradigma de esta confusión. La idea de *smart contract* implica que el contrato se cumplirá automáticamente, o incluso que se perfeccionará automáticamente, como ocurre con los contratos celebrados entre computadoras dotadas de inteligencia artificial; pero no que el Derecho se reduce a un programa informático. El Derecho siempre estará fuera, mirando en forma heterónoma, por lo que siempre se podrá hacer un juicio de juridicidad, aunque sea sobre un *smart contract* sometido a un programa informático. El derecho no puede ser reducido a un programa de computación.

### ***Posibilidad de un “Derecho de blockchain”***

Partiendo de estas ideas básicas, podría ser razonable deducir que - como se señala en el artículo de Manuel Fernández Morales y Rodrigo Franco Pérez, del Centro de Estudios Garrigues y Tecnológico de Monterrey, titulado “Bitcoin no *blockchain*: censura y centralismo” - el fenómeno originario de *blockchain* parece incompatible con la idea de Derecho. Por el contrario: parece haber sido creado para soslayar el Derecho o para crear un sistema al margen del Derecho, porque consiste en una red que se encuentra por encima de los Estados nacionales, que serían los que elaboran el Derecho. En efecto, mientras que el sistema jurídico estatal es centralizado, ya que implica una autoridad soberana

---

<sup>2</sup> PAROLA, Lorenzo, MERATI, Paola, GAVOTTI, Giacomo, (2018), “Blockchain e Smart contracts; questione giuridiche aperte”, *Contratti* 2/2018, IPSOA Wolters Kluwer Italia s.r.l., diciembre 2018, p. 681-688.

<sup>3</sup> LESSIG, Lawrence, (2006), *Code version 2.0*, Nueva York, Basic Books, capítulo 1.

desde la cual desciende el ordenamiento jurídico, los sistemas *blockchain* basan su fuerza en la confianza de todos los participantes en una red paritaria donde nadie ejerce poder, sino que todos se rigen por el respeto de un protocolo matemático que se cumple siempre.

Según ese entendimiento, el sintagma “Derecho de blockchain” - acuñado por el apreciado amigo Javier Ibañez para título de su reciente libro, editado en 2018 por Comillas/Aranzadi - contendría en sí mismo una contradicción insalvable.

Sin embargo, esta conclusión no se revela, a mi criterio, verdadera, por un doble orden de consideraciones, que constituirán el modesto aporte que puede proporcionar este prólogo a la importante contribución sobre el tópico hecha en verdad por los autores de los artículos publicados en este número de la Revista de FIADI.

En primer lugar, es una realidad incontestable que el sistema *blockchain*, pensado para funcionar *ad extra*, esto es al margen de los Estados y los Derechos y de las organizaciones que operan bajo su imperio, puede ser utilizado *ad intra*, o sea en el marco de los ordenamientos jurídicos nacionales o internacionales. En consecuencia, nada de extraño hay en que se hable de *blockchains* permisionadas, es decir, del uso de la tecnología *blockchain* sometida a normas, ya sean normas meramente convencionales, o normas sometidas al ordenamiento jurídico de un estado u organización. En ese marco, la tecnología ofrece una gran utilidad, porque permite lograr los resultados técnicos que son naturales a su funcionalidad (registro de información, verificación de su autenticidad y fecha cierta de los actos) en forma sumamente barata y eficiente, por lo que no hay razón para que ella no sea utilizada en el interior de los ordenamientos nacionales.

Pero aun cuando consideremos a las *blockchains* y a los *smart contracts* en su lugar original, es a saber, en el mundo global, que está por fuera o por encima de cualquier ordenamiento nacional o internacional, su advenimiento no significa que se trate de un hecho ajeno a la juridicidad, siempre que nos pongamos de acuerdo en el sentido del concepto de Derecho.

Por cierto, *prima facie*, la tecnología *blockchain*, utilizada por organizaciones sometidas al Derecho nacional o internacional, dejaría de connotar esa actitud de originaria anarquía (la “criptoanarquía”, como se ha denominado) y democracia directa que caracteriza el pensamiento original de los “*hackers*”. En efecto, la tecnología *blockchain* y los *smart contracts*, como la misma Internet, reconoció un origen en el cual floreció un pensamiento profundamente democrático e igualitario, centrado en la colaboración altruista de toda la humanidad en la construcción del conocimiento y en la cooperación para la vida en sociedad. La creación de Internet como red global significó un enorme reservorio de conocimiento puesto libremente a disposición de todos, una enorme ampliación de la información disponible, una mayor transparencia de los mercados económicos y una posibilidad inédita de libre difusión del pensamiento y superación de la censura, lo cual arropó la idea de un mundo de relaciones emancipadas de los poderosos.

Pero ello no condujo linealmente a un mundo basado en esos paradigmas, porque Internet fue y es también utilizado como medio de control y de censura, como instrumento de manejo comportamental y de centralización de información, y como base para nuevos y disruptivos modelos de negocio que están contribuyendo a una concentración de riqueza como jamás existió en la historia de la humanidad. Las empresas de tecnología como el quinteto llamado “GAFAM” (Google, Apple, Facebook, Amazon y Microsoft) constituyen actualmente el desmesurado oligopolio de la sociedad de la información. Aspectos éstos que nos confirman la tesis de que la tecnología por sí sola no puede dar garantías de un orden justo. Esto significa que la tecnología no es buena ni mala, puede usarse para el mal o para el bien o para fines indiferentes al mal o al bien. Y ahí es donde tiene que estar el Derecho.

Resulta sí cierto - como señalan Manuel Fernández Morales y Rodrigo Franco Pérez – que el sistema en estudio parece incompatible con los ordenamientos estatales. Tomando un caso de conflicto en el marco de la red Bitcoin o Ethereum: cuál sería el ordenamiento aplicable? La respuesta es que no

habría ni podría haber ninguno, porque el asiento de estos hechos es el mundo global. O sea: si reducimos el sentido de lo jurídico a la ley emanada de los órganos estatales, o en otros términos, si identificamos el Derecho con la Ley, efectivamente es posible concluir que el fenómeno de la *blockchain* y los *smart contracts* es ingobernable por el derecho.

Pero – reitero – eso es así si identificamos el Derecho con la Ley estatal, si reducimos el Derecho a la Ley emanada del órgano político del Estado. Y esa identificación, pese a estar profundamente grabada en la formación positivista que hemos recibido durante generaciones, está en la actualidad bajo cuestión. Me limito a citar la frase que puede encontrarse en el documento de Fundamentos del Anteproyecto de Código Civil y Comercial de la Nación Argentina recientemente aprobado en el 2015: “ ... proponemos distinguir normativamente el derecho de la ley. Una identificación entre ambos no es admisible en el estadio actual de la evolución jurídico-filosófica.”

En efecto, Ley y Derecho vienen identificados no en su naturaleza necesaria, sino en una concepción contingente históricamente situada, que se origina en el iluminismo absolutista que cumple la función ideológica de legitimación de las monarquías absolutas que están en el origen de los estados nacionales europeos en los siglos XVII y XVIII, que fue asumida por el modelo jacobinista de la revolución francesa, luego empleada con fruto para el logro de los intereses de la burguesía dominante en el período napoleónico, y finalmente exportada a los países que nacieron a la vida independiente en el siglo XIX, entre ellos todos los latinoamericanos.

La identificación entre Ley y Derecho, o mejor dicho, la reducción del Derecho a la Ley, con la consiguiente exclusión o subordinación a la legislación de toda otra fuente de derecho, es un producto histórico de la modernidad, no un dato necesario de la naturaleza. En consecuencia, cuando los tiempos ya no pueden seguir siendo llamados modernos y los definimos aludiendo a la “postmodernidad” - porque es indiscutible que los caracteres de la sociedad actual difieren notoriamente de los de la sociedad decimonónica - el hecho de que resulte imposible tener una ley estatal sobre la *blockchain* que opera en el mundo global no significa que un conflicto de intereses surgido a su respecto no pueda ser resuelto conforme al Derecho; no implica que nosotros los juristas tengamos que renunciar a pensar y formular el Derecho aplicable a la *blockchain*.

Lo que ocurre es que - como consecuencia de nuestra cultura positivista - no hemos desarrollado las competencias para percibir y descubrir el Derecho fuera de un texto legal. Y nos hemos olvidado de que tarea esencial del jurista cabal es ante todo mirar la realidad, y captar en ella los signos de un orden justo. No es imprescindible para ello contar con una ley aprobada por ambas Cámaras del Parlamento, promulgada por el Poder Ejecutivo y publicada en el Diario Oficial de un mundo global que no tiene – ni por el momento es previsible que pueda tener - nada de eso. Para resolver los conflictos que no se hacen esperar, el jurista debe buscar los lineamientos de orden justo que subyacen a los fenómenos de la realidad social, expresados en la forma en que usualmente ella se manifiesta: las costumbres, los usos, las reglas técnicas, las convenciones de los que saben sobre la materia.

Esta fue, por otra parte, desde siempre, históricamente, la función del jurista. No la aplicación ciega de un texto imperativo a una realidad que muchas veces muestra su inadecuación y la inconveniencia de las soluciones, sino la atenta consideración de la tensión entre norma y realidad, y la actitud crítica de preguntarse si la solución dada es la que representa el sentido de justicia que predomina en la comunidad.

Por cierto, la modernidad jurídica trajo vientos de certeza y precisión, de igualdad y de origen democrático de la legislación. Pero ello no es suficiente para resumir el fenómeno jurídico, y demostración de ello es este fenómeno de *blockchain*, imposible de regular si se busca la norma legal, pero que clama por un orden justo que seguramente es necesario encontrar mediante el recurso a otras fuentes.

Ello significa que entramos en el campo de la absoluta libertad individual para sostener lo que es jurídico y lo que lo separa de lo antijurídico? El mundo global de *blockchain* es el mundo de la libertad de cada uno de sostener que es derecho lo que a él se le antoje?

En nuestra opinión ello no es así, porque el Derecho no es obra de una mente individual o de una voluntad arbitraria, sino un producto colectivo y consensuado. Las señas del ordenamiento justo deben partir de un esmerado estudio de la realidad, en este caso de la tecnología, y de lo que la comunidad ha ido asentando como Derecho, es decir, como idea de un ordenamiento que por un lado responde a las necesidades del tráfico, y por otro, a la idea de justicia.

De fundamental importancia aparece entonces el conocimiento de la tecnología, y de ahí el valor de esta revista, que contiene descripciones variadas y precisas de los elementos técnicos en los que se basa el fenómeno *blockchain*. Se ha hablado de la necesidad de tener una idea de la tecnología, hasta el punto de que es necesaria una verdadera campaña de alfabetización digital: “*digital literacy*”, como sostiene Shoshana Zuboff en su libro “*The age of surveillance capitalism*”.

Por otra parte, el jurista, aunque esté desprovisto de leyes globales, aunque no tenga un mapa en el desconocido mundo global de *blockchain*, no está desprovisto de brújula. Hay un norte que seguir y es posible encontrar manifestaciones de consenso a partir de las cuales se puede construir un derecho de *blockchain*, aun en ausencia total de leyes estatales aplicables.

Anahiby Becerril en su trabajo “Breve historia de los *smart contracts*” alude precisamente a ese “marco jurídico contractual para los “0” y los “1”, sistematizando varios principios jurídicos generales a partir de la ley modelo de CNUDMI sobre Comercio Electrónico. Esta norma, que no reviste el valor formal de ley para regular fenómenos globales - aunque haya sido seguida en el proceso legislativo de muchos países y por tanto sea aplicable en su fuero nacional - expresa un esquema básico de principios generales de neto carácter jurídico, aplicables directamente en la resolución de conflictos globales que pudieran generarse en relación con el fenómeno *blockchain*.

Tal vez la idea más trascendente sea la de que el derecho de la tecnología no altera el derecho preexistente en materia de obligaciones y contratos privados. El artículo 1 de la ley uruguaya 18.600 sobre firma electrónica establece que “las disposiciones de esta ley no alteran el derecho preexistente respecto a la celebración, perfeccionamiento, validez y eficacia de los actos y negocios jurídicos”. Esto permite conectar las realidades tecnológicas, por más novedosas que sean, con la tradición jurídica preexistente, de modo que en definitiva se tiene una continuidad y una estabilidad en el derecho. Aún en ausencia de ley, cualquier desarrollo doctrinario anterior puede ser de aplicación en un conflicto generado por la tecnología.

En segundo lugar, y a mi criterio se conecta con el primero, el principio de equivalencia funcional; las herramientas que proporciona la informática cumplen funciones homogéneas con las que otras herramientas no digitales cumplen en el campo analógico. Una clave critpográfica simple equivale al documento privado, una clave avanzada sirve como si fuera un instrumento público. Por tanto la reinención de sistemas de autenticación no afecta la función, que es autenticar. Expresa el artículo 5 de la ley modelo: “No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos.”

Por otra parte, el principio de neutralidad tecnológica; la tecnología está en constante evolución y el Derecho no puede quedar prisionero de artefactos que hoy pueden ser útiles pero que mañana estarán totalmente obsoletos.

Y por último, los dos grandes principios de libertad contractual y de buena fe, que nos ponen de lleno en el surco de la tradición jurídica privatista, indicando claramente que el uso de la tecnología no quita la humanidad de las realidades.

## **Conclusión**

En conclusión: en un escenario de este tipo, el jurista debe - como pedía Cesare Vivante en relación con las prácticas mercantiles - recoger sistemáticamente los hechos para reconducirlos a los institutos jurídicos existentes y deducir, de tal modo, a la disciplina aplicable. <sup>4</sup> Esto propone la necesidad de agudizar el sentido jurídico de los profesionales del Derecho, que es no otra cosa que mirar atentamente la realidad, narrar, describir y explicar racionalmente los modelos conductuales propios de la nueva sociedad de la información e individualizar las normas de base para una justa composición de los conflictos de intereses implicados. Porque es deber del jurista “tomar posesión del rol que siempre ha sido suyo, y que siempre ha calificado, en el tiempo, su perfil profesional, es a saber: el desarrollo de una hermenéutica sapiente de la realidad, la atribución al complejo de los acontecimientos de un significado, no cualquiera, sino uno que sea coherente con el cuadro regulatorio ofrecido por el contexto y que sea idóneo para colocar esos acontecimientos en unas coordenadas que permitan definir una organización de los intereses lo más próxima posible a una justa definición de las relaciones entre los hombres, y de éstos con las cosas”. <sup>5</sup>

Fiadi desde el punto de vista institucional y su Revista en particular forman ciertamente parte de este imprescindible esfuerzo por crear un cuerpo de pensamiento que vaya haciendo emerger el Derecho que está en la naturaleza de las cosas, incluyendo la informática. Y los trabajos que contiene son prueba de ello.

---

<sup>4</sup> PAROLA, Lorenzo, MERATI, Paola, GAVOTTI, Giacomo, (2018), cit., p. 682.

<sup>5</sup> SCIUMÈ, Alberto, (2018), Prólogo del libro de Carlos de Cores, “La teoría general del contrato a la luz de la historia”, Buenos Aires, IJ Editores, p. 21.

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).  
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.  
ISSN 2530-4496 – AÑO 1, N° 8, 2020, PÁGS. 19-34

**BITCOIN NO BLOCKCHAIN: CENSURA Y CENTRALISMO**

BITCOIN NOT BLOCKCHAIN: CENSORSHIP AND CENTRALISM

**Manuel Fernández Morales y Rodrigo Franco Pérez**  
Centro de Estudios Garrigues y Tecnológico de Monterrey



**RESUMEN:**

El presente artículo analiza a través del desarrollo histórico de la criptomoneda *Bitcoin* (BTC), cómo la tecnología de cadena de bloques (*blockchain*), siguiendo los propios principios bajo los cuales ha sido desarrollada, específicamente el de descentralización de la información y resistencia pública a la censura, hace indeseable la utilización de la misma por parte de autoridades estatales y gubernamentales para garantizar la trazabilidad de transacciones como contratos, transparencia y acceso a la información o tractos registrales.

**PALABRAS CLAVE:**

Estado, BTC, *blockchain*, descentralización, censura.

**ABSTRACT:**

The following paper analyzes Bitcoin's historical development, as a cryptocurrency backed up by *blockchain* technology and how after its own core principles, specifically information decentralization, and open resistance to censorship, makes usage by governmental authorities to guarantee traceability of transactions, such as contracts, transparency, information access and registry undesirable.

**KEYWORDS:**

State, BTC, *blockchain*, decentralization, censorship.

## I. INTRODUCCIÓN

El presente artículo desarrolla de modo secuencial y didáctico la historia de la red *Bitcoin* y la forma en la que dicha red opera, así como las propiedades inherentes a la misma. Posteriormente, revisa algunas de las aplicaciones actuales que tiene la tecnología derivada de *Bitcoin* denominada *blockchain* en otros activos similares.

A partir de los elementos anteriores, los autores resumen el análisis sobre la naturaleza jurídica que tiene Bitcoin en términos generales como un activo, bien o propiedad, descartando su naturaleza de divisa y la equiparándola mayormente a otros activos con valor intrínseco como el oro.

En paralelo, se explica cómo opera un sistema jurídico a través del enfoque del realismo, cerrando con una convergencia de la tecnología *blockchain* con el sistema jurídico y su enfoque de control, que colisiona directamente con los objetivos de la red *Bitcoin*, exponiendo finalmente las conclusiones de los autores, que afirman la imposibilidad de los Estados de extender la regulación existente o aplicar la tecnología *blockchain* de forma exitosa.

### 1. Origen de Bitcoin y la Cadena de Bloques

Resulta imposible hablar de la tecnología *blockchain* sin hablar de *Bitcoin*, ya que tienen una historia de origen conjunta: El documento escrito y publicado por quien dijo ser Satoshi Nakamoto el 31 de octubre de 2008.<sup>1</sup>

Antes de la existencia de la red *Bitcoin*, la humanidad no podía validar una transacción financiera sin la existencia de al menos un intermediario de confianza al cual las partes confían sus activos financieros y que evitase el doble gasto, concepto que se describe cómo usar más de una vez el mismo recurso en diferentes transacciones.<sup>2</sup>

Lo anteriormente descrito se puede definir en el problema de los generales bizantinos el cual parte de una premisa en la cual se busca hallar una forma de asegurar que en una organización jerárquica pueda seguir una orden teniendo en cuenta que algunos de sus miembros pueden ser desleales o actúen bajo interés propio.<sup>3</sup>

De acuerdo con el propio Nakamoto, existe una propuesta de solución al problema de validación de transacciones electrónicas carentes de intermediario.<sup>4</sup> Dicha intermediación había sido tradicionalmente atribuida a autoridades Estatales que componen el sistema financiero de un país tales como los bancos centrales, instituciones financieras y entidades reguladas que participan de los mismos.<sup>5</sup>

La solución propuesta para el problema consiste en una red *peer-to-peer*; es decir, que opera entre sus miembros, registrando un conjunto de bloques de transacciones ligados uno a otro para conformar un libro contable distintivo de la red denominada *Bitcoin* conocido como *ledger*.

Dichas transacciones son validadas por nodos existentes en la red que actúan como ‘mineros’ (figura que se explora más adelante) y realizan la denominada *proof of work* requerida para obtener una contraprestación en forma de *Bitcoin* después de que cada bloque es validado.

1 BERNARD, Zoë, *Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator*, disponible en el sitio web: <https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12?r=MX&IR=T> (consultado el 10 de mayo de 2020).

2 HOEPMAN, Jaap-Henk, *Distributed Double Spending Prevention*, disponible en el sitio web: <https://arxiv.org/pdf/0802.0832v1.pdf> (consultado el 10 de mayo de 2020).

3 KIRRMANN, Hubert, *Fault Tolerant Computing in Industrial Automation*, disponible en el sitio web: [https://web.archive.org/web/20140326192930/http://lamspeople.epfl.ch/kirrmann/Pubs/FaultTolerance/Fault\\_Tolerance\\_Tutorial\\_HK.pdf#page=94#page=94](https://web.archive.org/web/20140326192930/http://lamspeople.epfl.ch/kirrmann/Pubs/FaultTolerance/Fault_Tolerance_Tutorial_HK.pdf#page=94#page=94) (consultado el 10 de mayo de 2020).

4 NAKAMOTO, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponible en el sitio web: <https://bitcoin.org/bitcoin.pdf> (consultado el 10 de mayo de 2020).

5 *Ídem*.

Después de la publicación de Nakamoto, la red *Bitcoin* empezó a operar con el bloque 0 o génesis en 2009, que incluía el encabezado del periódico *The Times* del 3 de enero de 2009 de la siguiente manera:

*“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”*<sup>6</sup>

Es importante mencionar esto pues la tecnología *blockchain* y *Bitcoin* tienen su origen en la propuesta de una misma ‘persona’<sup>7</sup>, sino porque *Bitcoin* nace como una llamada de atención a la respuesta de las instituciones gubernamentales y monetarias ante la crisis financiera que sufrieron los mercados en 2008, cuyas consecuencias fueron globales.<sup>8</sup> Dichas respuestas, consistían en rescates financieros para bancos y empresas en la forma de expansión cuantitativa que en términos generales se tradujo en la pérdida del valor adquisitivo de las divisas con las cuales se produjeron dichos rescates, y la atomización del poder de compra de los particulares, en muchas ocasiones colocándolos en situación vulnerable o de pobreza.

Dicha propuesta solamente tuvo resonancia al inicio dentro de las subculturas del Internet, y poco a poco fue adquiriendo adeptos, quienes observaron ventajas en el carácter de activo de resguardo de valor similar al oro sin tener la dificultad de almacenamiento, acuñación centralizada, falta de transparencia e imposibilidad de respaldo de valor de divisa por la naturaleza jurídica del oro.<sup>9</sup>

## 2. Modo de operación de la red Bitcoin

Habiendo realizado una breve introducción a la aparición de *Bitcoin* y por qué se considera que tiene valor intrínseco; pareciere importante abordar una introducción técnica a la red *Bitcoin*, ya que este invento no es únicamente el resultado de un avance social sino también tecnológico y, como tal, es condición *sine qua non* para su comprensión.

Así las cosas, es menester mencionar algunos de los elementos que distintivos<sup>10</sup> de esta tecnología que se desarrollan a continuación:

**Participantes:** Son todos los nodos de la red BTC, es decir, quienes mantienen una copia del *ledger* y deciden de forma contingente si se agrega o no un bloque de transacciones, para en consecuencia considerar la validez de ésta.

**Activos:** En el lenguaje laico se denomina comúnmente como criptomoneda, que en el caso de la red *Bitcoin*, son las *Bitcoin*, mismas que tienen posibilidad de fraccionarse hasta por cien millones. La unidad mínima de *Bitcoin* es un Satoshi, que tiene equivalencia a 0.00000001 BTC.

**Transacciones:** Son operaciones que se ejecutan dentro de la red *Bitcoin* dentro de las cuales existe un agente denominado emisor, un agente denominado receptor y una cantidad de activos determinados enviada en cada una.

La manera en que la red *Bitcoin* opera es la siguiente: Los emisores, quienes son diferenciados con direcciones establecidas por la red BTC envían una transacción la cual se ‘firma’ con un código alfanumérico de cadena de caracteres encriptados denominada *llave privada*.

Esto, bajo la hermenéutica analógica para un sistema jurídico no es más que un símil a la figura de

6 NAKAMOTO, Satoshi, *Bitcoin v0.1 released*, disponible en el sitio web: <https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html> (consultado el 10 de mayo de 2020).

7 A la fecha de redacción la identidad de Satoshi Nakamoto no ha podido ser corroborada. ROBERTS, Daniel, *Who Is Satoshi Nakamoto, Inventor of Bitcoin? It Doesn't Matter*, disponible en el sitio web: <https://fortune.com/2015/12/09/bitcoin-satoshi-identity/> (consultado el 10 de mayo de 2020).

8 HERSZENHORN, David M., *Congress approves \$700 billion Wall Street bailout*, disponible en el sitio web: <https://www.nytimes.com/2008/10/03/business/worldbusiness/03iht-bailout.4.16679355.html> (consultado el 10 de mayo de 2020).

9 Ejecutivo Federal de los Estados Unidos Mexicanos, *Ley Del Banco De México*, México, Ciudad de México.

10 PRITZKER, Y., *Inventing Bitcoin*, sin editorial, 2019.

‘firma’ como elemento de reconocimiento de validez a un acto. Estas transacciones entran al *mempool*, lugar virtual hacia dónde se dirigen las operaciones que esperan a ser validadas por los nodos denominados “mineros” quienes realizan la *proof of work* resolviendo un problema matemático que ocupa mucho poder computacional en su resolución, pero es fácil de verificar, más adelante explicaremos que el poder computacional inherente al *blockchain* resulta inadecuado para resolver problemas de gobernanza digital o de trazabilidad en general.

La contraprestación que resulta de la realización del trabajo requerido para la verificación de un bloque de transacciones es un subsidio a la dirección del nodo, que en es una suerte de ‘pago’ por la ejecución del trabajo de verificación. De allí que se les denomine ‘mineros’ pues es la única manera de obtener activos de la red *Bitcoin* sin que provengan de otra dirección o exista duplicidad de transacción y es como se crean los *Bitcoins*.

Algo importante a destacar es que cada 2016 bloques, la propia red *Bitcoin* ajusta la dificultad de las pruebas de trabajo dependiendo de cuántos nodos existan en un momento dado en la red y cuánto poder de procesamiento se calcula que estos nodos tienen. Esto se realiza para prevenir que alguien o alguna entidad tenga el control mayoritario, es decir, mayor al 50% de los nodos de la red, pues de ser así, podría cambiar las transacciones a su conveniencia, ya que tendría la mayoría de las confirmaciones aseguradas, peligrando así la integridad y publicidad que otorga la certeza de un activo virtual como lo es *Bitcoin*.<sup>11</sup>

Otro punto para tomar en cuenta es que cada 210,000 bloques, la cadena ejecuta un ajuste a la contraprestación que se le da al nodo que valida las transacciones a la mitad de uno inicial de 50. El primer ajuste se dio en 2012, el segundo en 2016 y el tercero se espera en mayo de 2020 y es comúnmente conocido como ‘*halving*’.<sup>12</sup> Esto significa que, en 2140, las 21 millones de *Bitcoins* en existencia terminarán de ser minadas, ya que estos eventos se repetirán aproximadamente cada 4 años haciendo que el límite de *Bitcoin* en existencia sea de un poco menos de 21 millones pues el *halving* tiene una tendencia aritmética a 0.

## II. LAS PROPIEDADES DE BITCOIN

Para entender la particularidad de *Bitcoin* como activo inmaterial, es deseable que exista un consenso sobre los principales principios que le dotan de una naturaleza única como criptomoneda.

De acuerdo con Andreas Antonopoulos<sup>13</sup>, las cinco propiedades que definen a la red *Bitcoin* son las siguientes:

**Descentralizada:** Ninguna organización o individuo tienen el control relativo o absoluto de la red *Bitcoin*. Esto incluye, por supuesto, a organizaciones del sector privado o público que pretendan tener un control operativo o relevante de la misma y tienen un claro tinte antisistema puesto que busca que no existan individuos que puedan comprometer la integridad de la red BTC.

**Sin fronteras:** Ningún Estado u Organismo Internacional puede controlar la red *Bitcoin* por razón de su poder jurisdiccional, pues de lo contrario la misma rápidamente puede retirar sus nodos de dicha

11 WALKER, Greg, *Difficulty. A mechanism for regulating the time it takes to mine a block*, disponible en el sitio web: <https://learnmeabitcoin.com/beginners/difficulty> (consultado el 11 de mayo de 2020).

12 O’NEAL, Stephen, *Bitcoin Halving, Explained*, disponible en el sitio web: <https://cointelegraph.com/explained/bitcoin-halving-explained> (consultado el 10 de mayo de 2020).

13 Antonopolpus es uno de los voceros más importantes de Bitcoin a nivel mundial y quien ha escrito varios libros al respecto e incluso fue convocado por el gobierno de Canadá como consultor del Senado en 2014. SOUTHURTS, John, ‘*Bitcoin Guru*’ Andreas Antonopoulos Appears Before Canadian Senate, disponible en el sitio web: <https://www.coindesk.com/bitcoin-guru-andreas-antonopoulos-appears-canadian-senate> (consultado el 11 de mayo de 2020).

ARAYA, Daniel, *The Promise of Bitcoin: An Interview With Andreas M. Antonopoulos*, disponible en el sitio web: <https://futurism.com/promise-bitcoin-interview-andreas-m-antonopoulos> (consultado el 11 de mayo de 2020).

jurisdicción de manera casi instantánea. Esto hace, que las jurisdicciones que han intentado prohibir o restringir las operaciones en criptomoneda hayan fracasado o tenido que ajustar su marco jurídico, como pasó con la India y como después hubiere de definir el Reino Unido.

Resistente a la censura: Ninguna autoridad puede establecer de forma unilateral restricción alguna respecto del *modus operandi* de la red *Bitcoin*. La red *Bitcoin* opera como un flujo ininterrumpido sin la posibilidad, por su propia arquitectura, de que un Gobierno pueda restringir su operación en forma eficaz.

Abierta: Cualquier persona puede acceder y modificar el código fuente sobre el cual se ejecuta *Bitcoin*, siempre y cuando los desarrolladores lleguen a un consenso sobre que el cambio propuesto es válido y útil para la mejora de dicho código fuente.

Pública: La idea de un libro público y contable de transacciones, conocido como *ledger* es una herramienta pública para cualquier persona que quiera consultarlo, transparentando así las operaciones e impidiendo la duplicidad de estas.

En un segundo punto, este carácter público a menudo se ha teorizado como la herramienta práctica para la figura hipotética de los *smart contracts*, considerando que la publicidad es una trazabilidad de forma errónea, pues no existe un elemento distintivo a otros contratos celebrados por la vía web y/o con instrumentos de ejecución de garantía automática en las jurisdicciones donde es válido.

Estos puntos nos llevan a concluir preliminarmente que, para un Estado, aunque es posible legislar esta tecnología limitando privilegios operativos como la anonimidad en la enajenación del activo, es decir, de divisa a criptomoneda, es virtualmente imposible vigilar y taxar la operación hasta la reconversión del activo en FIAT o divisa de curso en el Estado donde se ejecute la transacción y para su uso en aplicaciones centralizadas.

### III. APLICACIONES ACTUALES DEL BLOCKCHAIN

Habiendo mencionado las características de *Bitcoin*, habremos de compararla con otras redes de “*blockchain*” existentes y explicar por qué éstas no cumplen con todas las características descritas anteriormente para acreditar plena existencia de un *blockchain*.

#### 1.1 Ethereum

La red Ethereum es considerada popularmente como la segunda red de criptomoneda más exitosa después de *Bitcoin*. Creada con la pretensión de permitir la creación y ejecución de aplicaciones descentralizadas y contratos inteligentes, denominados *smart contracts*. Fue propuesta por Vitalik Buterin en 2013 ya que tenía la idea de implementar este tipo de aplicativos en la red *Bitcoin*, pero al no llegar a consenso con la comunidad, decidió crear una nueva red. Junto con la red, se creó también la Ethereum Foundation, organización encargada para apoyar el desarrollo de la red.<sup>14</sup>

Dado que Ethereum tiene un “líder”, no puede cumplir con el principio de descentralización. Vitalik como titular proyecto ya ha causado estragos en el mismo. La falsa noticia en la que se le declaró muerto en 2017 causó un declive en el valor de la cadena con un total de cuatro mil millones de dólares.<sup>15</sup>

Empero, este no es el único problema inherente de Ethereum. En 2016 tuvo que hacerse un *hard fork*,

14 BUTERLINK, Vitalik, *Ethereum White Paper A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM*, disponible en el sitio web: [https://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf) (consultado el 11 de mayo de 2020).

15 WONG, Ian Joon, *Fake news of a fatal car crash wiped out \$4 billion in ethereum's market value yesterday*, disponible en el sitio web: <https://qz.com/1014559/vitalik-buterin-dead-a-hoax-on-4chan-crashed-ethereums-price/> (consultado el 11 de mayo de 2020).

una invalidación de ciertas transacciones dentro de la red, debido a un ciberataque en el cual se desviaron 50 millones de dólares en activos que fueron tomados de la primera organización descentralizada desarrollada sobre Ethereum, la DAO.<sup>16</sup>

Actualmente, las aplicaciones DeFi o de finanzas descentralizadas son la mayoría de los proyectos desarrollados por empresas sobre la red Ethereum y se centran en ejecutar contratos inteligentes que adquieren sus usuarios y que a la fecha no otorgan una ventaja sobre la ejecución de garantías sin declaración judicial que pueden existir en instituciones como el *escrow* de los Estados Unidos de América.

## 1.2 Libra

Libra es el proyecto que se desarrolla sobre la tecnología de cadena de bloques y propuesto por Facebook. Si bien no se ha desarrollado y simplemente se anunció la creación de un documento inicial de propuesta, es interesante comentar que, al ser creado por Facebook; Libra falla en la resistencia a la censura y a la descentralización, pues en reiteradas ocasiones se ha demostrado la enajenación de datos de privados y el constante monitoreo de datos sensibles por parte de la empresa para propósitos comerciales y de seguridad.<sup>17</sup>

Este proyecto llamó la atención de las autoridades de los Estados Unidos quienes convocaron al director de Facebook, Mark Zuckerberg, al Congreso para explicar su nueva propuesta.<sup>18</sup>

Al ser Facebook una empresa bajo las leyes de los Estados Unidos de América parece difícil que un proyecto en *blockchain* cumpla con las cinco propiedades antes mencionadas. Esto es algo que Andreas Antonopoulos también aborda en una conferencia denominada “Libre, not Libra”. Frase que resume el absurdo del proyecto.<sup>19</sup>

## 1.3 XRP/Ripple

Ripple es la empresa creadora del token XRP, el cuál es la tercera criptomoneda con mayor valor en el mercado. La empresa se dedica al envío de pagos de manera instantánea alrededor del mundo a través de los tokens XRP. Pero esta red genera problemas con los principios al ser controlada por un privado, el token XRP no es descentralizado y Ripple controla quienes pueden o no validar transacciones.<sup>20</sup>

Todo lo anterior refrendaría que, en un estudio preliminar, es complicado ajustar la tecnología de *blockchain* de forma plena a plataformas, redes o usos alternativos que no sea la red BTC.

## IV. NATURALEZA JURÍDICA DE BITCOIN

Es mandatorio que, si se cumple con el doble rasero, *consuetudo vel longa inveterata* (como costumbre repetida de forma reiterada) así como el *opinio iuris seu necessitatis* (como necesidad de aplicar una opinión jurídica al caso), habrá de integrarse al sistema jurídico la red *Bitcoin* por su relevancia e

16 POPPER, Nathaniel, *A Hacking of More Than \$50 Million Dashes Hopes in the World of Virtual Currency*, disponible en el sitio web: <https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html> (consultado el 11 de mayo de 2020).

17 The Libra Association, *Libra White Paper*, disponible en el sitio web: <https://libra.org/en-US/white-paper/> (consultado el 11 de mayo de 2020).

18 ROM, Tony, *Facebook's Zuckerberg takes broad lashing on Libra, 2020 election and civil rights at congressional hearing*, disponible en el sitio web: <https://www.washingtonpost.com/technology/2019/10/23/facebook-mark-zuckerberg-testifies-congress-election-libra/> (consultado el 11 de mayo de 2020).

19 ANTONOPOULOS, Andreas, *Libre Not Libra: Facebook's Blockchain Project*, disponible en el sitio web: <https://www.youtube.com/watch?v=7S6506vkth4> (consultado el 11 de mayo de 2020).

20 ZILKJAER, Thomas, *14 Common Misunderstandings About Ripple And XRP*, disponible en el sitio web: <https://www.forbes.com/sites/thomassilkjaer/2019/03/07/14-common-misunderstandings-about-ripple-and-xrp/#31bdd8f571d0> (consultado el 11 de mayo de 2020).

impacto creciente en diversas jurisdicciones donde se empezaron a realizar transacciones de divisa nacional a activo inmaterial.

Diversos tribunales, entre los cuales se resalta a la Alta Corte de Inglaterra y Gales, debieron definir en sus fallos la naturaleza que tiene BTC, si era un bien para efectos de la ley, y si el mismo gozaba de una integración en su sistema jurídico.

Existió un caso sonado en Gran Bretaña donde se cobró un rescate de una plataforma por un ciberataque a través de *Bitcoin*<sup>21</sup> y como consecuencia se reclamó un seguro y una orden de congelamiento de bienes para garantizar que no se dilapidaran dentro de un mercado virtual. a través de dicho estudio en el caso *AA v Persons Unknown*, se determinó que el *Bitcoin* era susceptible de ser tratado como una propiedad bajo el estudio del caso *National Provincial Bank v Ainsworth*, donde se definió la propiedad como definible, identificable por terceros, capaz de ser asumido por terceros y un grado de permanencia, sin embargo, no lo dotó de características de divisa.

Lo mismo aconteció con el gobierno de la India, que en principio había prohibido la criptomoneda BTC, y en un fallo reciente en 2018 revirtió la decisión ante la imposibilidad de controlar con prohibiciones.

## V. LOS SISTEMAS JURÍDICOS COMO INSTRUMENTO DE CONTROL

Tanto Talcott Parsons como Nicklas Luhman, desarrollaron una descripción de los modelos de gobernanza a través de la teoría de sistemas.<sup>22</sup> De acuerdo con Merriam Webster un sistema es ‘un grupo de entidades que interactúan para formar un todo unificado’<sup>23</sup>. Por ello, las sociedades humanas pueden ser descritas bajo este modelo, siempre que se asuma que dicha representación tiene un carácter dinámico con elementos de permanencia que permiten la descripción analítica de las mismas.

El Derecho ha sido estudiado como un sistema social desde las teorías Luhmanianas, ya que es un sistema particularizado que goza de un metalenguaje<sup>24</sup> y estructura distintiva que facilita su análisis.

Bajo la concepción tradicional bajo la idea Kelseniana en donde el Derecho es estudiado de forma ‘metodológicamente pura’<sup>25</sup>, encontraremos la unidad esencial es un enunciado conocido como norma, cuya particularidad sería su carácter ‘jurídico’.

Una norma jurídica, es un enunciado prescriptivo dotado de eficacia a través de los criterios de validez formal y material, mismos que garantizan que la forma de su producción sea a través de un proceso designado por un consentimiento válido del cual emanan normas subsecuentes<sup>26</sup>, y que se cumple con un estándar de corrección ética dentro del canon del consentimiento originario.

Cuando hablamos de un acuerdo primigenio o consentimiento originario estamos evocando la concepción gnoseológica que autores como Kelsen Tamayo y discutiblemente Hart han definido como una suerte de norma fundante<sup>27</sup>, a través de la cual se genera una subsecuencia de normas.

---

21 White and Case, *Cybersecurity: Legal implications and risk management*, disponible en el sitio web: <https://www.whitecase.com/publications/alert/recovering-ransom-high-court-confirms-bitcoin-status-property> (consultado el 11 de mayo de 2020).

22 PARSONS, Talcott, *The Structure of Social Action*. Free Press, Estados Unidos 2018. & LUHMANN, Niklas, *Law as a Social System*, 3.a edición., Inglaterra, 2004.

23 Merriam Webster dictionary, disponible en el sitio web: <https://www.merriam-webster.com/dictionary/systems> (consultado el 11 de mayo de 2020).

24 La idea del Derecho como concepción de un metalenguaje en los ámbitos académicos es prevalente dentro de los filósofos analíticos, como de los que abordan las escuelas realistas. Concretamente Rolando Tamayo en *Introducción Analítica al estudio del Derecho* afirma la condición del Derecho como metalenguaje.

25 KELSEN, Hans, *La Teoría Pura del Derecho*, 16.a edición, trad. de Roberto J. Vernengo, México, 2015.

26 HART, Herbert Lionel Adolphus, *The Concept of Law*, 18.a edición, Inglaterra, 2016.

27 *Ídem*.

De la referida subsecuencia a dichos enunciados se construye la jerarquía normativa, que significa en doble vía que existe una cadena ordinal de premisas dentro de las normas jurídicas, y que dichos enunciados se encuentran siempre sujetos por su propia y especial naturaleza a una comprobación basada en verificación si se cumplen con los contenidos primigenios de las cadenas de jerarquía, lo cual es visible en la práctica cuando ocurre que una autoridad realiza estudios de legalidad y constitucionalidad de un acto o de una norma dentro de un orden jurídico cualquiera.<sup>28</sup>

De forma adicional, las doctrinas *iusrealistas* y los *critical legal studies*, se han sostenido que en un sistema normativo son igualmente relevantes las condiciones en las que los operadores del sistema jurídico mantienen e integran dicho sistema pues usualmente existen elementos exógenos que van a repercutir en las reglas de operación y funcionamiento del mismo.<sup>29</sup> Dicho en una forma muy sencilla, las escuelas *iusrealistas* no descartan la descripción del modelo analítico, si no que integran dentro del estudio del derecho los distintos componentes que dotan de contenidos a la norma, así como a las personas que participan del sistema y los fenómenos que lo afectan.

Los elementos exógenos que afectan al Derecho son acontecimientos tales como los movimientos sociales, históricos y por supuesto el desarrollo de nuevas tecnologías.

Es importante recordar que los contenidos materiales de los sistemas normativos, constituyen en todo momento pretensiones emanadas de una voluntad convertida en norma para los cuales el Derecho se comporta como generador y portador en un momento y lugar histórico determinado, y ello implica que la formación profesional de sus operadores (abogados, servidores públicos y otros) esté condicionada a referenciar dichas pretensiones de forma cotidiana y doctrinal, siendo contingente la transformación o materialización de estas pretensiones ante los elementos ajenos que ingresan al sistema jurídico.

Cabría añadir que dichas pretensiones eventualmente adquieren la forma de principios, y dichos principios operan como una especie de eje rector o directriz hermenéutica en la aplicación de las normas, sin que necesariamente los mismos existan de forma expresa en un cuerpo normativo, pues sería absurdo encontrar la definición del principio contractual *pacta sunt servanda*, y sin embargo el mismo es inferible de la lectura de la legislación civil de cualquier país.

Por ello podemos afirmar que ciertos principios, a los que tradicionalmente se han llamado principios generales del derecho, operan no como fuente auxiliar sino como una fuente directa de la producción del sistema jurídico<sup>30</sup>, pues si se pretende realizar un estudio holístico de un fenómeno relevante para el Derecho como es la aparición de nuevas tecnologías, contar con un análisis metanormativo (a la fecha no existe jurisprudencia o tesis aislada en los Estados Unidos Mexicanos que aborde la interpretación de la denominada “Ley Fintech” o Ley para Regular las Instituciones de Tecnología Financiera en los Estados Unidos Mexicanos), podría presumir la inexistencia de problemas legales de calado tal que impliquen el rediseño de la interpretación jurisprudencial basado en la aparición de la tecnología *blockchain* o las criptomonedas.

En su concepción primigenia, el derecho existe como un disuasor conductual que valida una sanción implementada por un grupo representativo o que detenta el poder cuando se determina que una conducta hipotética transgrede los valores éticos elementales que representa.

Más aún, desde la escuela *iusrealista* habremos de decir que siempre es posible que existan contingencias en la aplicación efectiva de cualquier norma jurídica y que dicha contingencia también forma parte de la descripción del derecho bajo el modelo de los sistemas jurídicos, para los cuales categorías tradicionalmente consideradas fuera del objeto del estudio del derecho, como son los

28 Esta idea se encuentra más o menos desarrollada en ÁLVAREZ LEDESMA, Mario Ignacio, *Introducción al Derecho*, 2.a edición, México, 2010.

29 NARVÁEZ, José, *#Necroderecho*, sin edición, México, 2016.

30 Esta opinión es propia del autor y que sostienen otros escritores como José Narvárez, Óscar Correas y Otros, cfr.

antivalores o los sentimientos y prejuicios inherentes los operadores<sup>31</sup>, implican que el sistema jurídico puede concebirse como una concepción tendiente a la regulación y no afirmar que la condición *sine qua non* del derecho es la coercibilidad y la condición de eficacia del mismo, si no la aceptación e integración conductual de las normas y sus principios dentro de los operadores del sistema y sus receptores.

Verbigracia, en los sistemas jurídicos de coordinación existen Estados que reconocen subsistemas, como el caso de Bolivia, Colombia o México,<sup>32</sup> en materia de indígenas, el caso del reconocimiento de los Actores Beligerantes dentro del Derecho Internacional Público, que en definitiva gozan de una aplicación eficaz, que no legítima y conforman un subsistema de normas en los territorios que ocupan y que no necesariamente es válido en la concepción tradicional de la teoría del Derecho, entre otros.

Así las cosas, podemos intentar definir al Estado moderno como un sistema jurídico que representa un conjunto de pretensiones autorreferenciales tendientes a la regulación de conducta. Bajo esta definición, hemos sumariado implícitamente una identidad entre Estado y Derecho, teniendo como unidad básica la norma jurídica y como directriz operativa los principios generales del derecho.

El Estado, entendido como la personificación del sistema jurídico, cumple con ciertas funciones entre las que se encuentra garantizar la convivencia y cooperación social, el otorgar certeza y seguridad a sus integrantes y por supuesto ejercer una función de control de la sociedad<sup>33</sup>, siendo la forma más común de control la existencia de sanciones de cuando existe un quebranto a una norma o en general una irrupción que el sistema jurídico no puede tolerar, y eventualmente pueda obligarle a autocorregirse o colapsarlo.

### ***1. La función de las autoridades centralizadas***

El Estado como personificación del sistema jurídico debe administrar los procesos para cumplir sus objetivos de control y de autopreservación. Dentro de los llamados Estados Constitucionales, que adoptan la positivización de las aspiraciones populares en la forma de documentos denominados Constituciones, usualmente se distribuye la administración en una forma tripartita, que establece los contrapesos institucionales con la finalidad de atomizar el poder Estatal y que existan controles en el ejercicio del poder.<sup>34</sup> La más común de estas formas, particularmente en el continente americano, influenciado por la Constitución de los Estados Unidos de América describe tres actividades o funciones: la producción de normas, la administración del gobierno, y la impartición de justicia, que para efectos de este análisis funge como la revisión y autocorrección final propia del antereferido sistema.

Entonces, habría que enfocar la idea de una nueva tecnología como es el *Bitcoin*, dentro de los tres procesos anteriores, es decir, la creación o regulación de un marco jurídico para el desarrollo y utilización de las tecnologías *blockchain*, la aplicación de dicha tecnología dentro de los procesos administrativos del Estado, y la validación normativa y conductual de esta tecnología por una autoridad jurisdiccional competente.

### ***2. El gobierno digital al principio del Siglo XXI***

Derivado de la revolución digital de finales de los años 90, se debió repensar la forma en la que los Estados regulaban las nuevas tecnologías, pues dado el incremento vertiginoso de transacciones en

---

31 NARVÁEZ, *Op. Cit.*

32 La opinión es propia del autor, quien al momento de la redacción ha participado en el procedimiento de consulta, redacción y sistematización de la ley de Derechos de los Pueblos, Barrios Originarios y Comunidades Indígenas Residentes para la Ciudad de México.

33 ÁLVAREZ LEDESMA, *Op. Cit.*

34 ARTEAGA, Elisur, *Derecho Constitucional Mexicano*, 7.a edición, México, 2006.

Internet, internacionales, el aumento de la relevancia de activos inmateriales como tales las marcas, el *know how* y la internacionalización de patentes, reveló la debilidad de muchos Estados para poder modernizarse y adaptarse a este cambio.<sup>35</sup>

Las primeras generaciones que se enfrentaron a la digitalización han tenido dificultad para entender el valor intrínseco de los activos inmateriales. Como resultado de lo anterior, las autoridades que gobernaban durante la década de los noventa en México no tuvieron la claridad para desarrollar un marco regulatorio que pudiese anticipar la revolución digital, anquilosaron de manera significativa el nacimiento de una doctrina de Derecho Informático y de nuevas tecnologías nacional que facilitara el estudio para la regulación de estos fenómenos.

Por ello, la gran pregunta que los Estados de Latinoamérica deben de realizarse es si es siquiera valioso regular el *blockchain* o adoptarlo como herramienta de verificación y trazabilidad.

### 3. Sistema financiero

Dentro del sistema jurídico existe de forma paralela un sistema de coordinación que es el sistema financiero.<sup>36</sup> Es aquel que facilita el intercambio de fondos entre participantes del mercado financiero, operando en una escala global y nacional. Dicho sistema está compuesto de servicios complejos interrelacionados, mercados e instituciones intermediaria que proveen de una vinculación eficiente entre participantes.<sup>37</sup>

La base del sistema financiero es la idea del dinero, que es un activo circulante en una economía estatal y que goza de valor liberatorio de obligaciones por declaración de una autoridad competente.<sup>38</sup> El dinero apareja el concepto de crédito, como una creencia de pago atribuible a un sujeto<sup>39</sup>. El sistema financiero en el siglo XXI ha permeado la totalidad de aspectos de la sociedad, permitiendo establecer consensos de valor sobre los bienes y servicios estableciendo referencias de precio de acuerdo con las leyes de la oferta y la demanda o a través de la posibilidad de que los Estados regulen estos valores, operaciones y a las instituciones mismas que participan del sistema financiero.

Por ello diversos autores entre los que se cuentan los suscritos consideran que dicha interrelación basada en intereses estatales y particulares a menudo puede favorecer actores que detentan mayor poder adquisitivo o bien representan un sector relevante de la economía sin hacer miramiento alguno al posible daño que pueden generar ciertas acciones a los particulares.

### 4. Mecanismo de control financiero de la población

La idea de los instrumentos de control permeó a las filosofías posmodernas que después de la Segunda Guerra Mundial evidenciaron la facilidad con la que un Estado puede establecer un control policiaco a través del aparato comunicativo y económico.<sup>40</sup> Sin duda, sociedades de control han encontrado que a menudo los disuasores comunicativos y financieros son los más eficientes.<sup>41</sup>

Se ha demostrado que la política monetaria y la distribución de la riqueza pueden y deben ser elementos que los Estados toman para mantenerse y autocorregirse como sistemas. El problema fundamental de este fenómeno es un acto de cosificación sobre las personas, y pareciere que el colapso bursátil acontecido en Estados Unidos de América y el mundo en 2008 formó de manera prácticamente

35 WATSON, Peter, *A history of thought and invention, from Fire to Freud*, 3.a edición, Estados Unidos de América, 2006.

36 O'SULLIVAN, Arthur; SHEFFRIN, Steven M., *Economics: Principles in Action*, Estados Unidos de América, 2003.

37 *Ídem*.

38 O'SULLIVAN, *Op. Cit.*

39 *Ídem*.

40 *Exempli gratia*, Hanna Arnendt en *los Orígenes del Totalitarismo*.

41 *Ídem*.

dialéctica una contracorriente que, viendo peligrar su futuro financiero optó por crear una salida definitiva al control financiero a través de la definición de un activo autorregulado y sin valor de referencia asignado por la ley de oferta y demanda.

### **5. El llamado *blockchain* y el gobierno**

Ya hemos definido qué es *Bitcoin*, cuáles son sus principios, que aplicaciones ejercen una tecnología similar, y del mismo modo, como los Estados estructuran los sistemas financieros como entes garantes del control.

Si se miran lo anterior se puede plantear la hipótesis que a menudo se han cuestionado agentes gubernamentales y privados del sector financiero sobre la posibilidad de aplicar *blockchain* para mejorar el control, publicidad o trazabilidad de diversas transacciones y su consecuente regulación.

Es allí donde existe una trampa conceptual, pues si la red BTC cumple con las características que hemos abordado, bastará con aplicar un juicio lógico para determinar que el gobierno es, antagónico por ser centralizado, con fronteras, ejerce censura, no de forma absoluta abierto, y no necesariamente tiene una publicidad irrestricta, razón por la cual, en primera instancia resulta irrelevante el desarrollo de una regulación específica para el uso de activos virtuales con una tecnología *blockchain*, porque en el remoto caso de ser exitoso en regular el activo desnaturalizaría la esencia de la tecnología en comento.

Por otra parte, el Estado, no puede ni debe abrir los nodos de las operaciones que celebre de forma irrestricta. Ahora supongamos que los registros de la propiedad operasen bajo un esquema de *blockchain*. Esto removería la exclusividad de dichos registros como certificadores de publicidad, y necesariamente deberían existir nodos abiertos que verificaran las transacciones inmobiliarias sobre un territorio. Lo anterior es absurdo, porque precisamente la concentración de un registro es la que facilita el acceso a la información pública en la materia y permite a los Estados taxar dichas operaciones y llevar un registro que si bien es público, perfectamente ha sido resuelto sin necesidad de alimentar nodos de verificación a través de la creación de folios electrónicos o bien, se ha podido, bajo las transacciones monetarias de los sistemas interbancarios, verificar sin la necesidad de delegar esta función en la modalidad de nodos, ahorrando tiempo significativo, consumo de energía y centralizando la operación, cosa que como reiteramos desnaturaliza el propósito de contar con un activo virtual como es la criptomoneda BTC.

## **VI. CONCLUSIONES**

El *blockchain* es una tecnología que tiene sentido al desarrollar aplicativos basados en los principios de descentralización, resistencia a la censura, sin fronteras, con código abierto y público.

La naturaleza jurídica de *Bitcoin* es la de un bien, pero no es un activo circulante o divisa pues no goza de poder liberatorio o el respaldo de un banco central.

No es posible separar la tecnología *blockchain* de la red *Bitcoin*, en tanto que otras criptomonedas o activos virtuales no han podido cumplir de forma exitosa con los principios anteriores.

Los gobiernos centrales no pueden ni deben adoptar una tecnología *blockchain* pues su naturaleza centralizada obvia el requisito de que la red se construya por nodos abiertos.

No es posible que los Estados regulen más allá del control de las Sociedades que habitan en sus límites jurisdiccionales, pues ello implicaría una acción regulatoria imposible en un mundo globalizado.

Existen alternativas de trazabilidad igualmente confiables que pueden ajustarse a las necesidades de los Estados y los particulares en materia registral, que no implican un cálculo de poder de cómputo.

## FUENTES DE INFORMACIÓN

- ÁLVAREZ LEDESMA, Mario Ignacio, *Introducción al Derecho*, 2.a edición, México, 2010.
- ANTONOPOLOUS, Andreas, *Libre Not Libra: Facebook's Blockchain Project*, disponible en el sitio web: <https://www.youtube.com/watch?v=7S6506vkth4> (consultado el 11 de mayo de 2020).
- ARAYA, Daniel, *The Promise of Bitcoin: An Interview With Andreas M. Antonopoulos*, disponible en el sitio web: <https://futurism.com/promise-bitcoin-interview-andreas-m-antonopoulos> (consultado el 11 de mayo de 2020).
- ARCE Y CERVANTES, José, *De los bienes*, 7.a edición, México, 2008.
- ARTEAGA, Elisur, *Derecho Constitucional Mexicano*, 7.a edición, México, 2006
- BERNARD, Zoë, *Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator*, disponible en el sitio web: <https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12?r=MX&IR=T> (consultado el 10 de mayo de 2020).
- BUTERLINK, Vitalik, *Ethereum White Paper A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM*, disponible en el sitio web: [https://blockchainlab.com/pdf/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf) (consultado el 11 de mayo de 2020).
- GARNER, Bryan A., *Black's Law Dictionary*, 9.a edición, Estados Unidos de América, 2009.
- HERSZENHORN, David M., *Congress approves \$700 billion Wall Street bailout*, disponible en el sitio web: <https://www.nytimes.com/2008/10/03/business/worldbusiness/03iht-bailout.4.16679355.html> (consultado el 10 de mayo de 2020).
- HOBBS, Thomas, *Leviatán. O la materia, forma y poder de una república eclesiástica y civil*, 2.a edición, trad. de Manuel Sánchez Sarto, México, 2008.
- HOEPMAN, Jaap-Henk, *Distributed Double Spending Prevention*, disponible en el sitio web: <https://arxiv.org/pdf/0802.0832v1.pdf> (consultado el 10 de mayo de 2020).
- KELSEN, Hans, *La Teoría Pura del Derecho*, 16.a edición, trad. de Roberto J. Vernengo, México, 2015.
- KELSEN, Hans, *Teoría general del derecho y del Estado*, 3 ed., trad, de Eduardo García Máynez, México, 2014.
- KIRRMANN, Hubert, *Fault Tolerant Computing in Industrial Automation*, disponible en el sitio web: [https://web.archive.org/web/20140326192930/http://lamspeople.epfl.ch/kirrmann/Pubs/FaultTolerance/Fault\\_Tolerance\\_Tutorial\\_HK.pdf#page=94#page=94](https://web.archive.org/web/20140326192930/http://lamspeople.epfl.ch/kirrmann/Pubs/FaultTolerance/Fault_Tolerance_Tutorial_HK.pdf#page=94#page=94) (consultado el 10 de mayo de 2020).
- LUHMANN, Niklas, *Law as a Social System*, 3.a edición., Inglaterra, 2004.
- MALLESON, Kate and MOULES, Richard, *The Legal System*, 4.a edición, Estados Unidos de América, 2010.
- Merriam Webster dictionary, disponible en el sitio web: <https://www.merriam-webster.com/dictionary/systems> (consultado el 11 de mayo de 2020).
- MORALES LECHUGA, Ignacio Seminario sobre Principios Generales de la Contratación, impartido en la Escuela Libre de Derecho, 5 de noviembre de 2010.

- Nakamoto, Satoshi Bitcoin. A Peer-to-Peer Electronic Cash System, disponible en <https://Bitcoin.org/Bitcoin.pdf> (consultado el 10 de mayo de 2020).
- NAKAMOTO, Satoshi, *Bitcoin v0.1 released*, disponible en el sitio web: <https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html> (consultado el 10 de mayo de 2020).
- NAKAMOTO, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponible en el sitio web: <https://bitcoin.org/bitcoin.pdf> (consultado el 10 de mayo de 2020).
- NARVÁEZ, José, *#Necroderecho*, sin edición, México, 2016.
- O'NEAL, Stephen, *Bitcoin Halving, Explained*, disponible en el sitio web: <https://cointelegraph.com/explained/bitcoin-halving-explained> (consultado el 10 de mayo de 2020).
- O'SULLIVAN, Arthur; SHEFFRIN, Steven M., *Economics: Principles in Action*, Estados Unidos de América, 2003.
- PARSONS, Talcott, *The Structure of Social Action*. Free Press, Estados Unidos 2018.
- POPPER, Nathaniel, *A Hacking of More Than \$50 Million Dashes Hopes in the World of Virtual Currency*, disponible en el sitio web: <https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html> (consultado el 11 de mayo de 2020).
- PRITZKER, Y., *Inventing Bitcoin*, sin editorial, 2019.
- ROBERTS, Daniel, *Who Is Satoshi Nakamoto, Inventor of Bitcoin? It Doesn't Matter*, disponible en el sitio web: <https://fortune.com/2015/12/09/bitcoin-satoshi-identity/> (consultado el 10 de mayo de 2020).
- ROM, Tony, *Facebook's Zuckerberg takes broad lashing on Libra, 2020 election and civil rights at congressional hearing*, disponible en el sitio web: <https://www.washingtonpost.com/technology/2019/10/23/facebook-mark-zuckerberg-testifies-congress-election-libra/> (consultado el 11 de mayo de 2020)
- SOUTHURTS, John, *'Bitcoin Guru' Andreas Antonopoulos Appears Before Canadian Senate*, disponible en el sitio web: <https://www.coindesk.com/bitcoin-guru-andreas-antonopoulos-appears-canadian-senate> (consultado el 11 de mayo de 2020).
- TAMAYO Y SALMORÁN, Rolando, *Costumbre o eficacia. Condición necesaria y suficiente de existencia del derecho (Con especial referencia al acto constituyente)*, México, 2015.
- TAMAYO Y SALMORÁN, Rolando, *Introducción analítica al estudio del derecho*, 2.a edición, México, 2011.
- TAMAYO Y SALMORÁN, Rolando, *Juris Prudentia: More Geometrico. Dogmática, teoría y meta teoría jurídicas*, México, 2013.
- The Libra Association, *Libra White Paper*, disponible en el sitio web: <https://libra.org/en-US/white-paper/> (consultado el 11 de mayo de 2020).
- WALKER, Greg, *Difficulty. A mechanism for regulating the time it takes to mine a block*, disponible en el sitio web: <https://learnmeabitcoin.com/beginners/difficulty> (consultado el 11 de mayo de 2020).
- WALKER, Greg, *Difficulty. A mechanism for regulating the time it takes to mine a block*, disponible en el sitio web: <https://learnmeabitcoin.com/beginners/difficulty> (consultado el 11 de mayo de 2020).
- WATSON, Peter, *A history of thought and invention, from Fire to Freud*, 3.a edición, Estados Unidos de América, 2006.

- White and Case, *Cybersecurity: Legal implications and risk management*, disponible en el sitio web: <https://www.whitecase.com/publications/alert/recovering-ransom-high-court-confirms-bitcoin-status-property> (consultado el 11 de mayo de 2020).
- WONG, Ian Joon, *Fake news of a fatal car crash wiped out \$4 billion in ethereum's market value yesterday*, disponible en el sitio web: <https://qz.com/1014559/vitalik-buterin-dead-a-hoax-on-4chan-crashed-ethereums-price/> (consultado el 11 de mayo de 2020).
- ZILKJAER, Thomas, *14 Common Misunderstandings About Ripple And XRP*, disponible en el sitio web: <https://www.forbes.com/sites/thomassilkjaer/2019/03/07/14-common-misunderstandings-about-ripple-and-xrp/#31bdd8f571d0> (consultado el 11 de mayo de 2020).

## LEGISGRAFÍA

- Cámara de Diputados del Honorable Congreso de la Unión *Ley para Regular las Instituciones de Tecnología Financiera*, Ciudad de México, México.
- Cámara de Diputados del Honorable Congreso de la Unión, *Código Civil Federal*, Ciudad de México, México.
- Cámara de Diputados del Honorable Congreso de la Unión, *Código de Comercio*, Ciudad de México, México.
- Congreso de la Ciudad de México, *Código Civil para el Distrito Federal*, Ciudad de México, México.
- Congreso Constituyente, *Constitución Política de los Estados Unidos Mexicanos*, México, Querétaro de Arteaga.

## PRECEDENTES Y JURISPRUDENCIAS

- Higher Court of England and Whales, *AA VS Persons Unknown*.
- Higher Court of England and Whales, *Provincial Bank v Ainsworth*.

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).  
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.  
ISSN 2530-4496 – AÑO 1, N° 8, 2020, PÁGS. 35-52

**BREVE HISTORIA DE LOS SMART CONTRACTS**

BRIEF HISTORY OF SMART CONTRACTS

**Anahiby Becerril**

Doctora en Derecho y Globalización  
Universidad Nacional Autónoma de México



**RESUMEN:**

La historia de *Blockchain* y de los *Smart contracts* es una historia sobre el desarrollo de la tecnología. Las tecnologías que conforman estas nuevas herramientas nos han acompañado por un largo periodo de tiempo, no son nuevas, solo han sido reutilizadas en usos diferentes adaptándolas a las capacidades actuales. No obstante el marco jurídico que acompañan a herramientas como los mensajes de datos, el documento y firma electrónica, el Derecho aún no ha logrado vencer la barrera de la cultura del papel, de los grafos en ellos plasmados, así como de la confianza en dichos sistemas. Es por lo que en este artículo, más allá de hablar de futuras regulaciones a estas nuevas herramientas, pretendemos hacer un breve recorrido que nos recuerde que en el ámbito contractual aún hace falta desarrollar el aprovechamiento de estas herramientas, hacen falta mediciones del nivel de madurez que sistemas como la firma electrónica avanzada y su cifrado tienen dentro del marco jurídico, para poder aprovechar las nuevas herramientas que se están desarrollando.

**PALABRAS CLAVE:**

Blockchain, contrato, electrónico, inteligente, firma.

**ABSTRACT:**

*The history of Blockchain and Smart contracts is a story about the development of technology. The technologies that make up these new tools have accompanied us for a long period of time, they are not new, they have only been reused in different uses, adapting them to current capabilities. Despite the legal framework that accompanies tools such as data messages, electronic documents and signatures, the Law has not yet managed to overcome the barrier of the paper culture, of the graphs embodied in them, as well as of the trust in these systems. That is why in this article, beyond talking about future regulations for these new tools, we intend to make a brief overview that reminds us that in the contractual field it is still necessary to develop the use of these tools, it is necessary to measure the level of maturity that systems such as advanced electronic signature and encryption have within the legal framework, in order to take advantage of the new tools that are being developed.*

*Keywords: blockchain, contract, electronic, smart, signature.*

## INTRODUCCIÓN

Las consecuencias jurídicas más importantes que ha traído Internet y las Tecnologías de la Información y Comunicación (en adelante TIC), han sido la masificación, la globalización y desmaterialización de los fenómenos jurídicos. El poder plasmar actos jurídicos con un clic o a través de código de programación, no es algo reciente, lo que resulta novedoso es la innovación que acompaña a los habilitadores tecnológicos del derecho.

La innovación tecnológica es omnipresente en la actualidad, y desde hace décadas hemos sido testigos de su impacto en el mundo jurídico, para los efectos que nos ocupa, en el derecho de la contratación. La complejidad de la innovación tecnológica plantea un gran desafío a la ley, sin embargo la ley y la tecnología tienen una relación binaria misma que para poder comprenderse, debe estudiarse en ambos lados: de la tecnología a la ley y de la ley a la tecnología.

El contrato, como figura central del Derecho constituye un instrumento básico de intercambio, sirviendo a los fines de la distribución de los bienes económicos de la comunidad y a la satisfacción de las necesidades a través de la realización de los intercambios de bienes y servicios. La contratación electrónica, *online* y los *Smart contracts* son el resultado del vertiginoso avance de las TIC. Si bien los contratos informáticos se elaboran en el ámbito de la contratación de bienes y servicios informáticos, los otros atienden al avance de las transacciones en donde la manifestación de la voluntad, lo convenido entre las partes o la ley, se codifican en mensajes de datos.

Para que un contrato electrónico u *online*, así como, los *smart contracts* tengan valor jurídico, es imprescindible que el ordenamiento atribuya, a las declaraciones de voluntad expresadas en mensajes de datos transmitidas a través de redes informáticas o medios electrónicos, ópticos o de cualquier otra tecnología, efectos jurídicos equiparables a los de las declaraciones de voluntad tradicionales. Es en esta parte donde toman mayor importancia el conjunto de Leyes Modelo publicadas por la UNCITRAL (*United Nations Commission for the Unification of International Trade Law* o CNUDMI, para Comisión de las Naciones Unidas para el Derecho Mercantil Internacional), a saber: La Ley Modelo sobre Comercio Electrónico<sup>1</sup> (adoptada el 12 de junio de 1995<sup>2</sup>) y la Ley Modelo sobre Firmas Electrónicas (adoptada en el año 2001)<sup>3</sup>, ambas con sus respectivas Guías para su implementación en el Derecho interno de los Estados.

No pasa inadvertida la existencia de la Convención de las Naciones Unidas sobre la utilización de las Comunicaciones Electrónicas en los Contratos Internacionales(2005), sin embargo, gracias a su flexibilidad<sup>4</sup> y finalidad armonizadora, las Leyes Modelos son instrumentos que han sido adoptados por la mayoría de los países en su derecho interno, además de que la Convención en sí, lo que realiza es una adaptación de los principios que derivan de la Ley Modelo sobre Comercio Electrónico, para darle una mayor obligatoriedad, en búsqueda de la uniformidad. A partir de aquí es que el mundo de la contratación entró en un periodo de innovación.

1 Ley Modelo UNCITRAL/CNUDMI *sobre Comercio Electrónico*, disponible en: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453\\_s\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf) (Consultada el 29 de mayo de 2020)

2 El artículo 5 bis suplementario fue adoptado en 1998.

3 Ley Modelo UNCITRAL/CNUDMI *sobre firmas electrónicas*, disponible en: [http://www.jurisprudencia.gob.sv/visormlx/cduncitral/CD\\_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s\[1\].pdf](http://www.jurisprudencia.gob.sv/visormlx/cduncitral/CD_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s[1].pdf) (Consultada el 20 de mayo de 2020)

4 La “armonización” entendida como el proceso por el que pueden modificarse las leyes nacionales para aumentar la previsibilidad de las operaciones comerciales transfronterizas. Mientras que la “unificación” puede considerarse como la aprobación por Estados de normas jurídicas comunes aplicables a determinados aspectos de las operaciones comerciales internacionales. En esta tesitura una Ley Modelo ejemplifica el tipo de texto cuya finalidad es armonizar el derecho interno, a diferencia de una Convención la cual constituye un instrumento internacional aprobado por los Estados para unificar el derecho a nivel internacional.

## EL CAMINO HACIA LOS *SMART CONTRACTS*

Muchas de las tecnologías que ahora damos “por hecho” fueron revolucionarias en su época, desde el teléfono, al *smartphone* (pensemos que este último no tiene más de una década de su aparición); el radio, los CDs, hasta la música portátil; muchas de las herramientas tecnológicas que diariamente empleamos, han tenido predecesoras, los *smart contracts* no son diferentes, veamos.

Consideremos a EDI (*Electronic Data Interchange*) una suerte de “ancestros” de los *smart contracts*. EDI consiste en el intercambio de documentos e información de forma estandarizada y automatizada entre empresas, este transmite de forma directa desde una aplicación informática en una organización a una aplicación en otra. Sus orígenes se remontan a la época de la Guerra Fría. En 1948, durante un año, la Unión Soviética cerró el acceso entre Alemania y las partes de Berlín que estaban controladas por Estados Unidos, Inglaterra y Francia. Para hacer frente a tal crisis, en 1949, un sargento mayor del ejército de los Estados Unidos, llamado Edward A. Guilbert, y otros oficiales desarrollaron un sistema de manifiesto que podía transmitirse por télex, radioteletipo o teléfono.<sup>5</sup>

Las lecciones del Berlín se infiltraron en el sector privado. Guilbert -quien en ese momento trabajaba con DuPont-, inventó un sistema de intercambio electrónico de datos (*electronic data interchange*), en 1965, desarrollando un conjunto de estándares de mensajes electrónicos para enviar información de carga entre DuPont y uno de sus transportistas. Esta invención permitió a DuPont enviar documentos de envío transatlánticos como mensajes télex, que posteriormente se convirtieron en cinta de papel y se ingresaron en las computadoras de la compañía. En las décadas que siguieron a la invención de Guilbert, los sistemas EDI se desplegaron desde DuPont, encendiendo una tendencia de transformar los acuerdos en papel y las órdenes de confirmación en representaciones digitales.

Para el año 1968, los camioneros, las aerolíneas y las compañías de transporte marítimo estaban utilizando manifiestos electrónicos y formaron el Comité de Coordinación de Datos de Transporte (*Transportation Data Coordinating Committee*, DCC) para crear estándares entre industrias. En 1975, el TDCC publicó sus primeros estándares EDI.

Hoy en día, los sistemas EDI han ganado una adopción generalizada, particularmente de la gestión de cadenas de suministro complejas.

Para la Ley Modelo de UNCITRAL sobre Comercio Electrónico (en adelante Ley Modelo CE), EDI constituye la “transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida para tal efecto” (art. 2.b).<sup>6</sup>

EDI se encuentra principalmente basado en el estándar ISO 9735-10:2014, consistiendo en un sistema de intercambio de documentos electrónicos estandarizados, que permite, a través de redes de telecomunicaciones, entre partes contratantes definidas, con independencia de su ubicación, realizar transacciones electrónicas dotadas de interoperabilidad y con desmaterialización de los documentos. Con EDI, la información va directamente de una aplicación de computadora dentro de esta forma EDI efectúa, sin intervención humana, una serie de operaciones económicas, con rapidez y seguridad.

5 International Information Systems Management, disponible en: [https://www.sagepub.com/sites/default/files/upm-binaries/19325\\_entire\\_chapter\\_devoted\\_to\\_information\\_systems.pdf](https://www.sagepub.com/sites/default/files/upm-binaries/19325_entire_chapter_devoted_to_information_systems.pdf) (Consultada el 29 de mayo de 2020)

6 Ley Modelo UNCITRAL/CNUDMI sobre Comercio Electrónico, disponible en: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453\\_s\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf) (Consultada el 29 de mayo de 2020)

Dentro de las ventajas que presenta EDI se encuentran<sup>7</sup>:

- Mayor velocidad de procesamiento, menor tiempo de entrega y mayor eficiencia;
- Menos reingreso y transcripción de datos, menos probabilidad de error y mayor exactitud;
- Menor costo y mayor comodidad disminuyendo o evitando el transporte físico de documentos;
- Menor consumo de papel debido a la transmisión y el almacenamiento electrónicos.

Dentro de los sectores que emplean EDI se encuentran: la industria automotriz, al reducir el tiempo necesario para procesar los pedidos, este sistema les ha permitido ahorrar costos a través de la gestión justo a tiempo de las piezas de automóviles. Del mismo modo, la industria del transporte lo ha adoptado, para intercambio de documentos de ruta y aduanas.

Este constituye una actividad en red propia del *ecommerce* (comercio electrónico) a través de las cuales las empresas integran y comparten diversos tipos de documentos, desde órdenes de compra, facturas, solicitudes de cotizaciones, hasta solicitudes de préstamo y más. En su mayoría, las empresas son socios comerciales que emplean EDI para intercambiar bienes y servicios como parte de sus cadenas de suministros y redes de *business to business* (B2B).

Los sistemas EDI tienen algunas limitaciones. Considerando que estos contratos electrónicos simplemente reafirman los términos y condiciones existentes en un formato electrónico, hacen poco por cambiar la forma en que las partes celebran y cumplen sus obligaciones comerciales. Atendiendo a su estructura y automatización, consideramos a EDI una suerte de “ancestro” de los *smart contracts*.

En los años 90’s el científico informático Nick Szabo vio estas limitaciones y concibió una nueva forma de ejecutar contratos electrónicos. En un documento titulado «*Formalizing and Securing Relationships on Public Networks*»<sup>8</sup> (Formalizar y asegurar las relaciones en las redes públicas), Szabo describió cómo la dependencia de protocolos criptográficos más robustos permitiría escribir software de computadora que se asemejara a «cláusulas contractuales» y a las partes vinculadas, de una manera que reduciría las oportunidades para cualquiera parte para rescindir sus obligaciones de desempeño, lo que daría pie a la creación de los *smart contracts*.

## EL MARCO JURÍDICO CONTRACTUAL PARA LOS “0” Y “1”<sup>9</sup>

Lo decisivo para efectos de la manifestación de la voluntad por medios electrónicos, no lo es el contenido del documento o soporte a través del cual se realice, sino el medio electrónico a través del cual surge y se concreta. Para que los actos jurídicos puedan plasmarse en contratos electrónicos, *blockchain* y *smart contracts* resulta indispensable que la Ley otorgue reconocimiento y validez jurídica a los mensajes de datos.

La desmaterialización de las comunicaciones se basa precisamente en la seguridad que implica la forma escrita y la firma, sólo que se realiza de forma virtual. Los mensajes de datos son el elemento fundamental del documento electrónico, firma electrónica y de todo el desarrollo del uso de las tecnologías, ya que estos son los que contienen la información (texto, video, audio, etc.) que constan en los mismos.

7 Ley Modelo UNCITRAL/CNUDMI *sobre firmas electrónicas*, disponible en: [http://www.jurisprudencia.gob.sv/visormlx/cduncitral/CD\\_content/electronic%20commerce/ML%20elecsig/ml-elecsigs\[1\].pdf](http://www.jurisprudencia.gob.sv/visormlx/cduncitral/CD_content/electronic%20commerce/ML%20elecsig/ml-elecsigs[1].pdf) (Consultada el 20 de mayo de 2020)

8 SZABO, Nick, «*Formalizing and Securing Relationships on Public Networks*», disponible en: <https://firstmonday.org/article/view/548/469> (Consultada el 29 de mayo de 2020)

9 Código binario de programación

Los mensajes de datos incluyen información electrónicamente tratada que contiene declaraciones de voluntad, así como objetos materiales e inmateriales susceptibles de contratación. Estos son intangibles, lo que representa uno de los más importantes bienes o valores de la Sociedad de la Información y el Conocimiento.

La Ley Modelo CE refiere que por mensaje de datos se entenderá *la información generada, enviada o archivada o comunicada por medios electrónicos, ópticos o similares, como pudiera ser; entre otros, el intercambio electrónico de datos (EDI, siglas en inglés para Electronic Data Interchange), el correo electrónico, el telegrama, el télex o el telefax* (artículo 2. a))<sup>10</sup>. Misma definición encontramos en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre las Firmas Electrónicas<sup>11</sup> (artículo 2. a).

En esta tesitura, en las referidas Leyes Modelo, la CNUDMI ha establecido cuáles son los requisitos jurídicos que debe contener un mensaje de datos, a saber:

Cuando la Ley requiera que la información conste por escrito, este requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta, requisito que será aplicable tanto en el caso que la ley marqué como obligación la firma del documento, así como, si ésta prevé las consecuencias en caso de que el mismo no conste por escrito;

Cuando la Ley prevea la firma de una persona, este requisito quedará satisfecho en los siguientes casos: a) si se utiliza algún método para identificar y asegurar que la persona aprueba la información contenida en el mensaje de datos; b) que el método en cuestión sea fiable para los fines por los cuales se generó y comunicó el mensaje de datos;

Cuando la ley requiera que la información sea presentada y conservada en su forma original, este requisito quedará satisfecho en los siguientes casos: a) que exista alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva; b) en caso de que se requiera presentar la información, que esta se pueda mostrar a la persona interesada.

Estos requisitos se consolidan a través de los principios establecidos para la contratación electrónica, que derivan de la Ley Modelo CE, a saber:

Principio de equivalencia funcional;

Principio de inalteración del derecho preexistente de obligaciones y contratos privados;

Principio de neutralidad tecnológica;

Principios de buena fe (contractual); y,

Principio de libertad contractual.

Estos principios se encuentran presentes en el Derecho interno de los Estados, pero al ser aplicables al Derecho Internacional forman parte de todo el orden jurídico. Recordemos que las Leyes Modelo, al conformar un método indirecto de uniformidad, son sólo un marco de referencia para las legislaturas de los Estados, que delinear los principios y disposiciones que deberán ser adoptadas por estos, para su adopción en el Derecho interno. En este sentido, la Ley Modelo sobre Comercio Electrónico de CNUDMI, al ser una guía para que los Estados, influyó dentro del Derecho interno, fomentando la

10 Ley Modelo UNCITRAL/CNUDMI *sobre Comercio Electrónico*, disponible en: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453\\_s\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf) (Consultada el 29 de mayo de 2020)

11 Ley Modelo UNCITRAL/CNUDMI *sobre Firmas Electrónicas*, disponible en: [http://www.jurisprudencia.gob.sv/vi-sormlx/cduncitral/CD\\_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s\[1\].pdf](http://www.jurisprudencia.gob.sv/vi-sormlx/cduncitral/CD_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s[1].pdf) (Consultada el 20 de mayo de 2020)

adopción de estos principios generales basados en el Derecho Informático que sirven como pauta para valorar los actos jurídicos que de llevan a cabo por medio de mensajes de datos<sup>12</sup>.

### ***Principios generales de los contratos que constan en mensajes de datos***

#### *Principio de equivalencia funcional.*

Los artículos 5 y 5 bis de la Ley Modelo CE<sup>13</sup> refieren:

*Artículo 5.- Reconocimiento jurídico de los mensajes de datos.*

*No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.*

*Artículo 5 bis.- Incorporación por remisión*

*(En la forma aprobada por la Comisión en su 31.º período de sesiones, en junio de 1998)*

*No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión.*

La equivalencia funcional, implica aplicar a los mensajes de datos una pauta de no discriminación respecto de las declaraciones de voluntad realizadas por una de las partes contratantes. De esta forma los efectos jurídicos apetecidos por el emisor de la declaración deben producirse con independencia del soporte escrito o electrónico en el que conste tal declaración.

La misma Ley Modelo CE refiere en su artículo 11.1, que no se negará validez ni fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos<sup>14</sup>. De esta forma el principio de equivalencia funcional claramente establece que no deberá restarse validez ni eficacia jurídica a la manifestación de la voluntad o al acto jurídico por el hecho de haberse celebrado por mensaje de datos.

El principio de equivalencia funcional de los actos jurídicos celebrados a través de mensajes de datos, respecto de aquellos actos jurídicos suscritos en forma manuscrita, e incluso oral, constituye el principal fundamento de las transacciones que se realicen vía mensajes de datos.

Si bien no pasa desapercibido que dentro de la Ley Modelo sobre Comercio Electrónico no se hace referencia expresa al término equivalencia funcional, en la exposición de motivos de afirma particularmente que se favorecerá la celebración de contratos por vía electrónica, a asegurarse *la equivalencia* entre los documentos en soporte papel y los documentos electrónicos a efectos de cumplimiento del requisito de forma escrita que figura en diversas leyes.

Del referido principio se deduce que la función jurídica que ataña la instrumentación escrita y autógrafa respecto de todo acto jurídico, o su expresión oral, se cumple de igual forma mediante la instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, extensión, alcance y finalidad del acto que se realice, lo que implica básicamente una pauta de no discriminación de los mensajes de datos independientemente del medio a través del cual se generen. Es por lo que algunos autores se refieren a este como *principio de no discriminación*, toda vez que con este se pretende formular un entorno jurídico neutro en donde se otorgue la misma importancia y validez jurídica a la in-

12 CASTRILLÓN Y LUNA, V.M. & BECERRIL, A., “Contratación Electrónica Civil Internacional. Globalización, Internet y Derecho”, Porrúa, México, 2014, p. 143.

13 Ley Modelo UNCITRAL/CNUDMI *sobre Comercio Electrónico*, disponible en: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453\\_s\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf) (Consultada el 29 de mayo de 2020)

14 *Idib.*

formación que conste en soporte papel a la que conste en soporte electrónico, óptico o de cualquier otra tecnología.

*Principio de inalteración del derecho preexistente de obligaciones y contratos privados.*

Este principio reconoce que los elementos esenciales de un vínculo contractual y por lo tanto las normas que lo regulan, no se modifican cuando el contrato es perfeccionado por medios electrónicos. A este respecto la Ley Modelo CE refiere:

*Artículo 6.- Escrito*

*Cuando la ley requiera que la información conste por escrito, este requisito quedará satisfecho con un mensaje de datos si la información que éste contiene es accesible para su ulterior consulta.*

*El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no conste por escrito.<sup>15</sup>*

Como se desprende del numeral citado, este principio se basa en la afirmación de que las relaciones contractuales plasmadas en soporte electrónico forman parte del ámbito de aplicación de la teoría general de las obligaciones y contratos. Lo anterior implica, además de utilizar las normas preexistentes del Derecho contractual, en cuanto al fondo, se tendrán que aplicar las normas específicas referentes a los mensajes de datos, para la forma.

*Principio de neutralidad tecnológica.*

El principio de neutralidad tecnológica se utilizó por vez primera como principio de regulación en el año 1999, en un documento oficial de la Comisión Europea sobre la revisión del marco normativo de las comunicaciones electrónicas. Este principio se adoptó como uno de los cinco principales que regían el marco regulador de las comunicaciones electrónicas en la Unión Europea. Este explica que la neutralidad tecnológica supone que la legislación debe definir los objetivos a conseguir sin imponer ni discriminar el uso de cualquier otro tipo de tecnología para conseguir los objetivos fijados.

Este principio pretende conseguir un trato igualitario a los mensajes de datos, fomentando el acceso y la creación de transacciones a través de los medios electrónicos, sin que se encuentren limitantes tecnológicas para su implementación.

Desde una perspectiva de no discriminación la neutralidad tecnológica busca asegurar un tratamiento igualitario y regulador entre las comunicaciones electrónicas, evitando así un marco jurídico en función de la tecnología usada para la manifestación de la voluntad.

La Guía para la Incorporación al Derecho Interno de la Ley Modelo sobre Comercio Electrónico enfatiza que los principios y sus disposiciones son igualmente aplicables a las técnicas de comunicación menos avanzadas, que la misma se basa principalmente a EDI y al correo electrónico, por lo que la ley no discrimina la base tecnológica sobre la cual se emita el mensaje de datos. La Ley plantea una serie de supuestos en relación con la creación de los mensajes de datos, con finalidad de responder a la necesidad de los usuarios del comercio electrónico de poder contar con un régimen coherente aplicable a las diversas técnicas de comunicación que puedan emplearse, refiriendo: Es preciso señalar, en principio, no se excluye ninguna técnica de comunicación en el ámbito de la Ley Modelo, que debe acoger en su régimen toda eventual innovación técnica en este campo.

---

15 Ley Modelo UNCITRAL/CNUDMI sobre Comercio Electrónico, disponible en: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453\\_s\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf) (Consultada el 29 de mayo de 2020)

*Principio de buena fe.*

La buena fe constituye un principio básico en aras de interpretar y ejecutar contratos de compraventa internacional y constituye uno de los fundamentos del régimen jurídico aplicable al intercambio internacional y nacional de bienes y servicios, siendo a este efecto irrelevante que se haya llevado a cabo por medios electrónicos, verbales o electrónicos.

Resulta común encontrar en la doctrina la alusión de la buena fe como un conjunto de valores, así es en general la consideración, mediante su utilización se dan valores como la honestidad, honorabilidad, fidelidad, lealtad y al respeto a la confianza que una determinada relación hace surgir entre partes.

En la contratación electrónica, este principio adquiere especial relevancia por cuanto a las características del intercambio realizado por medio de soportes tecnológicos, fundado en la confianza de los intervinientes. Sin importar si se trata de derecho nacional o uniforme, la buena fe constituye uno de los fundamentos del régimen jurídico aplicable al intercambio nacional e internacional de bienes, el que tal intercambio de haya convenido en forma escrita, verbal o electrónica no es relevante en cuanto a la observancia de la buena fe.

*Principio de libertad contractual.*

La voluntad contractual se manifiesta en la voluntad autónomamente expresada, determinando el establecimiento de las estipulaciones que las partes se otorgan de manera libre, pudiendo, en ciertos casos, hacer exclusión parcial o total de la norma jurídica, y son obligatorias para ellas desde el punto de vista jurídico.

En este sentido, el principio reconoce la libertad de los contratantes de decidir no sólo el medio a través del cual se celebrarán los actos jurídicos, sino el derecho en él constituido. Esto es, con independencia que las partes manifiesten su voluntad de obligarse por mensajes de datos, quedarán vinculadas.

***La firma electrónica avanzada***

Para el efecto de la fiabilidad y conservación de los mensajes de datos es requisito que la información en estos contenida pueda ser archivada para su ulterior consulta, ya sea en el mismo medio en que se constituyeron o en otro diferente, además debe conservarse todo dato que permita determinar el origen y destino del mensaje, incluyendo la fecha y la hora en que haya sido enviado o recibido.

Jurídicamente la firma es un mecanismo de imputación a un sujeto de declaraciones de voluntad, se fundamenta en la base personalista de la autografía, es decir, en la correlación comúnmente admitida, entre personalidad individual y escritura manuscrita. Una de las herramientas que se considera suficiente para identificar a una persona en las relaciones realizadas mediante mensajes de datos, equivalente funcional de la firma autógrafa se denomina firma electrónica.

Con la finalidad de desarrollar principios fundamentales respecto al cumplimiento de la función de la firma en las operaciones de comercio electrónico y para que ésta fuera tratada bajo el equivalente funcional de las firmas autógrafas, en el año 2001, se crea la Ley Modelo de UNCITRAL sobre Firmas Electrónicas (en adelante LMFE).

La cual define a la firma electrónica como: ... *los datos en forma electrónica, que se encuentran consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en éste* (art. 2, a)).<sup>16</sup>

---

16 Ley Modelo UNCITRAL/CNUDMI *sobre firmas electrónicas*, disponible en: [http://www.jurisprudencia.gob.sv/vi-sormlx/cduncitral/CD\\_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s\[1\].pdf](http://www.jurisprudencia.gob.sv/vi-sormlx/cduncitral/CD_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s[1].pdf) (Consultada el 20 de mayo de 2020)

Destaca que la finalidad de la firma electrónica no se limita a contener las mismas características de identificación de la autógrafa, previstas en el principio de equivalencia funcional. Además de ser un medio para atribuir el origen personal de un mensaje de datos, cumple además una función adicional: cifra el mensaje de datos firmado a fin de que sólo las personas autorizadas o su destinatario conozcan el contenido. Funciones que sobrepasan las de la firma manuscrita. De esta forma firmar los documentos electrónicos que consignan contratos electrónicos con firma electrónica avanzada, constituye un acto de voluntad claro e inequívoco de la expresión del consentimiento.

La Ley Modelo CE, en un principio, estableció que la forma de identificar o ligar al emisor del mensaje de datos, con éste es a través de un método fiable que pueda identificarlo. En su artículo 7 señala:

*Artículo 7. — Firma*

*1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:*

*a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y*

*b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.<sup>17</sup>*

La LMFE, vino a reforzar la seguridad jurídica de las comunicaciones, transacciones y acuerdos, proporcionando la presunción de que una firma electrónica es equivalente a una firma manuscrita<sup>18</sup>. La LMFE define a la firma electrónica:

*Artículo 2. Definiciones*

*Para los fines de la presente Ley:*

*a) Por “firma electrónica” se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos;<sup>19</sup>*

Lo anterior demuestra que la identidad de las partes, y por consiguiente la manifestación de su voluntad, puede determinarse por la firma electrónica o su especie más adelantada, avanzada (o reconocida). El uso de la firma electrónica avanzada (o reconocida) dentro de la contratación electrónica, permite determinar la identidad y la identificación de un signatario dentro de un documento, garantizando la integridad del mensaje de datos, al detectar cualquier alteración, desde el momento en que el documento realiza en su forma última, gracias a su sistema de creación. La influencia de la LMFE se ha visto reflejada y ha sido adoptada en diversas normas, tanto nacionales como internacionales.

El artículo 7 de la LMFE, citado *supralineas*, establece tres requisitos básicos que deben cumplir los mensajes de datos: autenticación, integridad o inalterabilidad y confidencialidad o identidad. Así, la firma electrónica además de ser un medio para atribuir el origen personal de un mensaje de datos establece la conformidad de la persona firmante con su contenido y cumple además una función adicio-

17 Ley Modelo UNCITRAL/CNUDMI *sobre Comercio Electrónico*, disponible en: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453\\_s\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf) (Consultada el 29 de mayo de 2020)

18 VILALTA NICUESA, Aura Esther, *Mediación y Arbitraje Electrónicos*, Ed. Aranzadi, Pamplona, 2013, p. 57.

19 Ley Modelo UNCITRAL/CNUDMI *sobre firmas electrónicas*, disponible en: [http://www.jurisprudencia.gob.sv/vi-sormlx/cduncitral/CD\\_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s\[1\].pdf](http://www.jurisprudencia.gob.sv/vi-sormlx/cduncitral/CD_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s[1].pdf) (Consultada el 20 de mayo de 2020)

nal; cifra el mensaje de datos firmado a fin de que sólo las personas autorizadas o su destinatario conozcan el contenido. Funciones que sobrepasan las de la firma manuscrita. Por otra parte, la LMFE establece en su artículo 3,<sup>20</sup> el principio de igualdad de tratamiento de las tecnologías para la firma.

### *El cifrado*

La criptografía consiste en el estudio de sistemas «matemáticos» para resolver dos tipos de problemas de seguridad: privacidad y autenticación. Un sistema de privacidad impide la extracción de información por parte de personas no autorizadas de los mensajes transmitidos a través de un canal público, asegurando así al remitente de un mensaje que solo el destinatario lo está leyendo. Un sistema de autenticación evita la inyección no autorizada de mensajes en un canal público, asegurando al receptor de un mensaje la legitimidad de su remitente.

La Guía de la LMFE, señala que la criptografía es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original. Explica que las firmas numéricas utilizan lo que se denomina “criptografía de clave pública”, que con frecuencia se basa en el empleo de funciones algorítmicas para generar dos “claves” diferentes, pero matemáticamente relacionadas entre sí (por ejemplo, grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primos). Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible, y la otra, para verificar una firma numérica o devolver el mensaje a su forma original. El equipo y los programas informáticos que utilizan dos de esas claves se suelen denominaren conjunto “criptosistemas” o, más concretamente, “criptosistemas asimétricos «cuando se basan en el empleo de algoritmos asimétricos (párrafo 36).<sup>21</sup>

La firma electrónica avanzada se crea cuando aplicamos una función de compendio (*hash*) y el resultado lo ciframos, usando una clave privada del remitente (R), y la clave pública del destinatario (D) que sólo puede ser verificada por el destinatario (D), usando la clave pública asociada del remitente y la propia clave privada. La asignación de valores *hash* que presente el mensaje una vez cifrado, constituye un tipo de huella digital de la elaboración del documento y la firma.

El cifrado consiste, por tanto, en cifrar los programas por un sistema de codificación sofisticado que emplea una o varias claves, conjunto de caracteres que transforman un método general o un algoritmo específico en informaciones codificadas, a efecto de que si alguien distinto al autor conoce el algoritmo no le sea de provecho, porque deberá conocer también la clave, la cual podrá ser cambiada y representa un nuevo obstáculo para aquel que quiera tener acceso al sistema.

### *El Hash*

El código *hash* se utiliza para cifrar los mensajes de datos y asegurar la integridad del texto en ellos consignados. Las firmas electrónicas avanzadas están compuestas por valores *hash* cifrados. Las funciones de resumen *hash* consisten en sistemas, los cuales, partiendo de todos los datos del documento, calculan un compendio codificado o condensación algorítmica del contrato (*digest*) que se procesará electrónicamente en la firma digital. Posteriormente, el destinatario, recuperará con la clave pública del remitente el resumen *hash* recibido de la firma del documento y lo comprobará con el *hash*, que

20 Artículo 3. Igualdad de tratamiento de las tecnologías para la firma. Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1 del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable; Cfr. Ley Modelo UNCITRAL/CNUDMI sobre firmas electrónicas, disponible en: [http://www.jurisprudencia.gob.sv/visormlx/cduncitral/CD\\_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s\[1\].pdf](http://www.jurisprudencia.gob.sv/visormlx/cduncitral/CD_content/electronic%20commerce/ML%20elecsig/ml-elecsig-s[1].pdf) (Consultada el 20 de mayo de 2020)

21 La Guía de la Ley Modelo UNCITRAL/CNUDMI sobre Firmas Electrónicas, disponible en: <http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf> (Consultada el 19 de mayo de 2020)

resulte, del documento recibido y compararía si coincide con el sello original y si observa que ha variado, es que ha perdido la integridad y/o autoría del documento, en cambio si coincide, no cabría duda de la identidad del documento.

*Una función de hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo). Varían en los conjuntos de partida y de llegada y en cómo afectan a la salida similitudes o patrones de la entrada. Una propiedad fundamental del hashing es que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son.<sup>22</sup>*

Las funciones hash se denominan también funciones unidireccionales porque es sencillo aplicar una función hash a un mensaje, pero es matemáticamente inviable obtener el mensaje a partir de un código hash.

La longitud de un código hash se mide en bits<sup>23</sup> (*binary digit o dígito binario*), lo que significa que un código hash de 64 bits puede representar  $2^{64}$  valores hash diferentes (18.446.744.073.709.551.616). Por ejemplo, a un ritmo de comprobación de 10 millones de mensajes por segundo, se tardaría unos 58.494 años para encontrar una coincidencia.

Utilizando un código hash, se añade el tiempo y la hora, se emite la firma y se envía el documento compuesto al cliente. Al estampar la firma, el cliente se asegura de que el TSS en realidad procese su solicitud, así como la correcta recepción del código hash y que el tiempo correcto se ha incluido. Este sistema se ocupa del problema presente y futuro de incompetencia del TSS, eliminando por completo la necesidad del TSS de almacenar registros.

## LOS 12 AÑOS DE BLOCKCHAIN.

A las 6:10:00 PM (UTC) del 31 de octubre de 2008, apareció un mensaje en una lista de correo de criptología (véase imagen 1). El mensaje, escrito por Satoshi Nakamoto, hacía la siguiente afirmación: «He estado trabajando en un nuevo sistema de efectivo electrónico que es completamente de igual a igual, sin un tercero confiable». Incluyó un enlace a un libro blanco de nueve páginas con el título “*Bitcoin: A Peer-to-Peer Electronic Cash System*” (Bitcoin: un sistema de efectivo electrónico de igual a igual)<sup>24</sup>.

22 MICROSOFT, “Ensuring Data Integrity with Hash codes”, disponible en: [http://msdn.microsoft.com/es-es/library/f9ax34y5\(VS.95\).aspx](http://msdn.microsoft.com/es-es/library/f9ax34y5(VS.95).aspx) (Consultada el 09 de mayo de 2020)

23 *Bit es el acrónimo Binary digit (‘dígito binario’). El bit es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información. Con él, podemos representar dos valores cuales quiera, como verdadero o falso, abierto o cerrado, blanco o negro, norte o sur, masculino o femenino, rojo o azul, etc. Basta con asignar uno de esos valores al estado de «apagado» (0), y el otro al estado de «encendido» (1). Con un bit podemos representar solamente dos valores, que suelen representarse como 0, 1. Para representar o codificar más información en un dispositivo digital, necesitamos una mayor cantidad de bits. Si usamos dos bits, tendremos cuatro combinaciones posibles:*

*0 0 - Los dos están «apagados»*

*0 1 - El primero (de derecha a izquierda) está «encendido» y el segundo «apagado»*

*1 0 - El primero (de derecha a izquierda) está «apagado» y el segundo «encendido»*

*1 1 - Los dos están «encendidos»*

*Cfr: WIKIPEDIA, “Bit”, disponible en: <http://es.wikipedia.org/wiki/Bit> (Consultada el 14 de mayo de 2020)*

24 NAKAMOTO, Satoshi, “Bitcoin: A Peer-to-Peer electronic Cash System”, disponible en: <https://bitcoin.org/bitcoin.pdf> (Consultada el 29 de mayo de 2020)



Imagen 1. Mensaje de Satoshi Nakamoto

Fuente: Satoshi Nakamoto Institute<sup>25</sup>

En el documento, Nakamoto esbozó de forma clara y ordenada su idea de un nuevo tipo de dinero digital llamado Bitcoin, el cual permitiría a las personas enviarse dinero directamente entre sí a través de Internet, sin necesidad de intermediarios. Los bancos no tendrían control sobre el sistema, ni tampoco los gobiernos. Sería dirigido, en cambio, por todos. Bitcoin sería una especie de dinero puro, completamente democrático, con costos de transacción mínimos, sin intermediarios y completamente digital.

Esta notable nueva tecnología irrumpió en el escenario en la última década y rápidamente capturó la imaginación del público, así como gran parte de su dinero.

La tecnología subyacente a Bitcoin es Blockchain. Se le denomina Blockchain o cadena (*chain*) de bloques (*block*) al resultado de aplicar la tecnología digital criptográfica que permite crear bases de datos almacenadas y compartidas en una comunidad o red no jerárquica o *inter pares* (*peer-to-peer*), construida sobre grupos, bloques (*blocks*) o eslabones de datos ligados o vinculados entre sí por *hashes*. La tecnología DLT (*Distributed Ledger Technology*) o registros distribuidos produce el efecto de identificar a estos de manera inequívoca, inalterable y transparente.

Un *ledger* (libro mayor) es un libro de registro permanente. El registro debe ser correcto y sin alteraciones. Un Blockchain es un libro de contabilidad que se reúne en Internet de manera descentralizada por un número indefinido de contribuyentes. Blockchain es una cadena de archivos que contiene lo que necesita ser grabado permanentemente. Una cadena de bloques básica conecta archivos para formar una cadena simple de cadena. Una cadena de bloques más sofisticada conecta archivos para formar una estructura similar a una red.

El *ledger* distribuido, descentralizado, compartido y replicado, puede ser público o privado, autorizado o sin permiso, o conducir a la economía criptográfica tokenizada o sin token. Los datos en el *ledger* se encuentran protegidos con criptografía, son inmutables y auditables y proporcionan una verdad sin censura. De esta forma cualquier puede revisar la base de datos, pero no modificarla.

Bitcoin y otras criptomonedas representan solo la primera «*app*» para la tecnología blockchain. Hay otras posibilidades infinitas para esa tecnología, desde el comercio de valores y productos básicos, hasta la cadena de suministro, los derechos de propiedad intelectual, la gestión de la identidad y la se-

<sup>25</sup> SATOSHI NAKAMOTO INSTITUTE, disponible en: <https://satoshi.nakamotoinstitute.org/emails/cryptography/threads/1/> (Consultada el 29 de mayo de 2020)

guridad, los bienes inmuebles y los servicios gubernamentales, solo por nombrar algunos, podrían transformar la forma de hacer negocios en el mundo, como en su oportunidad Internet lo hizo hace más de 20 años. Por ejemplo, Blockchain aplicado a los *smart contracts*, permitiría no solo ser autoejecutables y de cumplimiento automático, sin la necesidad de intermediarios, sino además cada transacción sería automáticamente registrada en la base de datos distribuida. De esta forma los *smart contracts* basados en *blockchain* puede referirse a «contratos inteligentes descentralizados», dada la ausencia de una base de datos/registro central.

Podemos medir la evolución de los primeros 12 años de blockchain de la siguiente forma:

La primera innovación importante de *blockchain* fue *Bitcoin*, un experimento de moneda digital.

La segunda innovación se llamó *blockchain*, era esencialmente la comprensión de que la tecnología subyacente operadora de *bitcoin* podía separarse de la moneda y usarse para todo tipo de otra cooperación interorganizacional.

La tercera innovación se llamó el contrato inteligente (*smart contract*) incorporado en un sistema *blockchain* de segunda generación llamado *Ethereum*, el cual construyó pequeños programas de computadora directamente en *blockchain* permitiendo a la representación de los instrumentos financieros, como préstamos o bonos, en lugar de solo los tokens similares a efectivo de bitcoin;

La cuarta innovación se llama «*proof-of-stake*» (prueba de participación). Los blockchain de la generación actual están aseguradas por una «*proof-of-work*» (prueba de trabajo) en la que el grupo (*miners*) con la mayor potencia informática toma las decisiones. Los mineros operan grandes centros de datos para proporcionar esta seguridad, a cambio del pago de criptomonedas. Los nuevos sistemas eliminan los centros de datos, reemplazándolos con instrumentos financieros complejos, por un grado de seguridad similar o incluso mayor.

En 12 años de blockchain se ha tratado de solucionar todo con su uso, se ha buscado explotar las ventajas, confianza y seguridad que esta tecnología provee en el ámbito jurídico, económico, financiero, entre muchos otros. También han existido intentos en aras de proveer una regulación o principios que permitan obtener sus beneficios y disminuir los riesgos. El último intento es el presentado por el Consejo Global Blockchain del Foro Económico Mundial, el cual en mayo del año 2020 publicó los «Principios de Presidio: valores fundamentales para un futuro descentralizado»<sup>26</sup>. Estos dieciséis principios tienen como objetivo proteger a los usuarios y preservar los valores de la tecnología para que todos puedan beneficiarse. Reconocen que las aplicaciones creadas sobre sistemas basados en blockchain deben preservar los siguientes derechos de los participantes: *transparency* y *accessibility* (el derecho de información acerca del sistema); *interoperability* y *agency* (el derecho de los participantes de poseer y gestionar sus datos); *privacy* y *security* (el derecho a la protección de datos personales); *accountability* y *governance* (el derecho de los partícipio antes a entender los recursos disponibles).

## **SMART CONTRACTS**

¿Cómo percibe y se “ve” un documento legal? Sin soporte papel, sin grafos, solo “0” y “1”. Estos protocolos informáticos autónomos y de ejecución automática facilitan, ejecutan y hacen cumplir los acuerdos comerciales entre dos o más partes. Al igual que sucede con otros términos tecnológicos, no existe una definición única. El término tampoco resulta tan novedoso, recordemos que hace más de

26 WORLD ECONOMIC FORUM, “Presidio Principles: Foundational Values for a Decentralized Future”, disponible en: [https://www.weforum.org/communities/presidio-principles?utm\\_source=press-release&utm\\_medium=website&utm\\_campaign=presidio-principles](https://www.weforum.org/communities/presidio-principles?utm_source=press-release&utm_medium=website&utm_campaign=presidio-principles). (Consultada el 29 de mayo de 2020)

20 años, Nick Szabo los definió como: “*a computerized protocol that executes the terms of a contract*”<sup>27</sup> (un protocolo computarizado que ejecuta los términos de un contrato), señalando que en términos generales los *smart contracts* se encuentran diseñados para satisfacer condiciones contractuales comunes (como condiciones de pago, gravámenes, confidencialidad e incluso cumplimiento).

Dentro de un *smart contract* no se encuentra implícito el uso de inteligencia artificial (IA), la palabra «inteligente» (*smart*), como se entiende hoy en día, puede referirse al concepto de IA. Sin embargo, como se observó anteriormente, la definición original de Szabo explícitamente establece: «no se implica el uso de inteligencia artificial». Se trata de un mecanismo que realiza las funciones definidas a medida que se cumplen ciertas condiciones previas (cláusulas); un programa hace cumplir el contrato integrado en el código (*code*), se trata pues de palabras escritas en lenguaje de computadora (mensajes de datos) que son automáticamente ejecutados por una máquina; en algunos casos se suma a la definición el requisito de que dichos contratos se ejecuten en Blockchain o tecnologías de *ledger* similares.

Un contrato inteligente no es un contrato escrito en papel del tipo tradicional, ni es simplemente un contrato en línea. Se describe como «inteligente» porque puede hacer más que estos dos paradigmas, de la misma manera que un «teléfono inteligente» puede hacer más que solo hacer llamadas. Toma la forma de un código de computadora en una tecnología de libro mayor distribuido (que puede ser un *blockchain*) y se ejecuta al recibir entradas de datos electrónicos. Efectúa una acción en un DLT de manera comparable a una fórmula en la celda de una hoja de cálculo de Excel: Se ajusta o transfiere pagos u otros activos, monitorea los niveles de existencias o realiza otras acciones automáticamente porque eso es lo que está programado para hacer.

Estamos en presencia de un acuerdo entre dos partes para ejecutar compromisos previamente convenidos o pactados (cláusulas), sustituyendo el documento físico o papel, por un código de computadora predeterminado con la voluntad de las partes.

## CONSIDERACIONES FINALES

Al igual que sucedió con la contratación online que se realiza a través de Internet, en dónde aún surgen cuestionamientos en torno a su validez y eficacia jurídica, la aplicación de los *smart contracts* y la certeza jurídica que la manifestación de la voluntad que se realice por estos medios será sujeta a debate en los años por venir. O tal vez no necesariamente sea así, tal vez tomemos las lecciones aprendidas de los contratos online y las aprovechemos para facilitar y potenciar su empleo.

Tomemos por ejemplo la reforma llevada a cabo en el Estado de Arizona, Estados Unidos, en donde en el año 2015, se aprobó un proyecto de ley que contiene una definición legal de *smart contract*, a saber: “*an event-driven program that runs on a distributed, decentralized, shares and replicated ledger and that can take custody over and instruct transfer of assets on that ledger*”<sup>28</sup>. Y en marzo del año 2017 se enmendó la *Arizona Electronic Transactions Act* (Az. Rev. Stat. § 44-7061<sup>29</sup>) la cual específicamente considera que: (i) una «firma asegurada a través de la tecnología blockchain» es una firma electrónica, (ii) un «registro o contrato asegurada a través de la tecnología blockchain» como una forma o registro electrónico, y (iii) que un «contrato inteligente» es legalmente válido y exigible, re-

27 SZABO, Nick, “Smart contracts”, 1994, disponible en:

<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> (Consultada el 29 de mayo de 2020)

28 “Un programa basado en eventos que se ejecuta en un libro mayor distribuido, descentralizado, compartido y replicado y que puede tomar la custodia e instruir la transferencia de activos en ese libro mayor”

29 (i) a «signature secured through blockchain technology» to be an electronic signature, (ii) a «record or contract secured through blockchain technology» to be an electronic form or record, and (iii) a «smart contract» to be legally valid and enforceable; Cfr., Arizona Electronic Transactions Act, disponible en: <https://blockchainlawguide.com/resources/Arizona-44-7061—Blockchain-Signatures-and-Smart-Contracts.pdf> (Consultada el 29 de mayo de 2020)

firiendo que no se puede negar el efecto legal, la validez o la aplicabilidad de un contrato relacionado con una transacción únicamente porque ese contrato contiene un término de *smart contract*. Esto refleja la adopción del principio de equivalencia funcional, reconocido en la contratación electrónica, aplicable para los *smart contracts*.

Los *smart contracts* necesitan de un objeto, el acuerdo previo de las partes y la manifestación de la voluntad, la cual quedará plasmada dentro de un código que puede auto-ejecutarlas de forma automática. Esta voluntad y convenio se traduce en mensajes de datos, los cuales reflejan la libertad contractual de las partes, quienes pueden elegir la forma y medio para que esta manifestación quede plasmada (libertad contractual). Siempre que la Ley permita la equivalencia funcional de dicha manifestación a través de mensajes de datos.

La realidad es que aún no existe un marco legal internacional específicamente diseñado para tecnologías *blockchain* y contratos inteligentes. Al ser *Blockchain* una tecnología, parece mucho más razonable esperar y regular los posibles usos de esta, en lugar de la tecnología en sí misma, prestando atención para no sofocar la innovación. Con relación a los *smart contracts*, su situación legal aún es totalmente «poco clara». El hecho de que no exista una regulación específica sobre estos temas claramente no significa que las leyes actuales y los principios generales de derecho pueden no ser aplicables a ellos, o que no están regulados en absoluto: los *smart contracts* son de hecho piezas de software, piezas autoejecutables. En ausencia de regulaciones específicas, las leyes existentes deben regular estas tecnologías.

Las diferentes jurisdicciones tienen diferentes requisitos para los contratos válidos, pero en general, la libertad de contrato permite a las partes elegir si desean comprometerse mediante un contrato, cuándo y con quién. Las partes no solo son libres de elegir y acordar el contenido de su contrato, también son libres de elegir su forma (excepto cuando la ley requiera una forma especial). Mientras el acuerdo y la intención de las partes de comprometerse (o no, según sea el caso en las etapas preliminares) sean claros, las partes tienen la libertad de adaptar sus asuntos y diseñar sus contratos de la manera que quieran, de acuerdo con sus propias necesidades e intereses. Si lo desean, pueden optar por desviarse del paradigma tradicional en el que los contenidos de los contratos se expresan solo como texto.

No obstante el empleo diario de la tecnología en cada aspecto de nuestra vida, el mundo jurídico aún es renuente de dejar atrás la cultura del papel y los grafos en ella plasmada y pasar al de los bits. El problema es que sí a más de 20 años de la publicación y adopción de diversos países de los principios de la contratación vía mensajes de datos y uso de firma electrónica (derivados de la Ley Modelo CE), su implementación y reconocimiento en el mundo jurídico no ha logrado avanzar, estaremos “estancados” para emplear los *smart contracts* o cualquier otra tecnología través de la cual se manifieste la voluntad contractual.

En tal situación, los medios electrónicos como característica esencial de la globalización y la sociedad de la información y el conocimiento, continúan – y de seguro continuarán- planteando a los juristas nuevos retos, ante los problemas que parten de su convergencia, como de la aplicación de normas jurídicas a casos concretos derivados de su uso, porque en cierta forma dichos expertos están más habituados a *operar con materiales dados o establecidos (de lege data), que para avanzar en la prospectiva de la lege ferenda*.<sup>30</sup>

---

30 PÉREZ LUÑO, Antonio E., *Ensayos de Informática Jurídica*, Ed. Fontamara, México, 2009, p. 11

## BIBLIOGRAFÍA

- Arizona Electronic Transactions Act, disponible en: <https://blockchainlawguide.com/resources/Arizona-44-7061---Blockchain-Signatures-and-Smart-Contracts.pdf> (Consultado el 29 de mayo de 2020)
- CASTRILLÓN Y LUNA, V.M. & BECERRIL, A, “Contratación Electrónica Civil Internacional. Globalización, Internet y Derecho”, Porrúa, México, 2014.
- International Information Systems Management, disponible en:
- [https://www.sagepub.com/sites/default/files/upm-binaries/19325\\_entire\\_chapter\\_devoted\\_to\\_information\\_systems.pdf](https://www.sagepub.com/sites/default/files/upm-binaries/19325_entire_chapter_devoted_to_information_systems.pdf) (Consultado el 29 de mayo de 2020)
- Ley Modelo de la CNUDMI sobre Comercio Electrónico (adoptada el 12 de junio de 1995), disponible en: [https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453\\_s\\_ebook.pdf](https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/05-89453_s_ebook.pdf)
- Ley Modelo de la CNUDMI sobre Firmas Electrónicas (adoptada en el año 2001), disponible en: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/es/ml-elecsig-s.pdf>
- Microsoft, “Ensuring Data Integrity with Hash codes”, disponible en: [http://msdn.microsoft.com/es-es/library/f9ax34y5\(VS.95\).aspx](http://msdn.microsoft.com/es-es/library/f9ax34y5(VS.95).aspx) (Consultado el 09 de mayo de 2020)
- NAKAMOTO, Satoshi, “Bitcoin: A Peer-to-Peer electronic Cash System”, disponible en: <https://bitcoin.org/bitcoin.pdf> (Consultado el 29 de mayo de 2020)
- PÉREZ LUÑO, Antonio E., *Ensayos de Informática Jurídica*, Ed. Fontamara, México, 2009.
- SATOSHI NAKAMOTO INSTITUTE, disponible en: <https://satoshi.nakamotoinstitute.org/emails/cryptography/threads/1/> (Consultado el 29 de mayo de 2020)
- SZABO, Nick, “Smart contracts”, 1994, disponible en: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> (Consultado el 29 de mayo de 2020)
- VILALTA NICUESA, Aura Esther, *Mediación y Arbitraje Electrónicos*, Ed. Aranzadi, Pamplona, 2013.
- WORLD ECONOMIC FORUM, “Presidio Principles: Foundational Values for a Decentralized Future”, disponible en: [https://www.weforum.org/communities/presidio-principles?utm\\_source=press-release&utm\\_medium=website&utm\\_campaign=presidio-principles](https://www.weforum.org/communities/presidio-principles?utm_source=press-release&utm_medium=website&utm_campaign=presidio-principles) (Consultado el 29 de mayo de 2020)

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).  
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.  
ISSN 2530-4496 – AÑO 1, N° 8, 2020, PÁGS. 15-30

**ENTENDIENDO BLOCKCHAIN, SU APLICACIÓN Y SUS IMPLICACIONES  
LEGALES Y TÉCNICAS**

UNDERSTANDING BLOCKCHAIN APPLICATIONS AS WELL AS ITS LEGAL AND  
TECHNICAL IMPLICATIONS

**David Amado Monroy<sup>1</sup>**

Blackpol Venture and Law, S.L.co

1. Es socio de Telecomunicaciones, Privacidad y Comercio Electrónico en Blackpol Venture and Law, S.L. tanto en México como en España. David comenzó su práctica profesional en el área mercantil y corporativa, a lo largo de su trayectoria se ha especializado en nuevas áreas del Derecho que han tomado un papel primordial en todo el mundo, como son telecomunicaciones, privacidad, ciberseguridad, e-commerce e inteligencia artificial. A lo largo de su trayectoria, ha tenido la oportunidad de trabajar en proyectos relevantes para empresas como Ebay, PayPal, MasterCarrd, Ford, American Tower, British Telecom, Amazon, Facebook, Uber, Bla Bla Car, entre otras. David es licenciado en Derecho por la Universidad Panamericana con mención honorífica; Maestría *cum laude* en Derecho de las Nuevas Tecnologías por la Universidad Complutense de Madrid; Certificación en Regulación de la Inteligencia Artificial y Compliance por Harvard Law School; Especialidad en Compliance por la Universidad de Pennsylvania; Certificación en LegalTech and Startups por el IE Business School; Certificación en Ciberseguridad por la Cámara de Comercio Internacional en conjunto con la embajada de Israel.

**Datos de contacto:**

Correo: [damado@blackpol.es](mailto:damado@blackpol.es)

LinkedIn: [www.linkedin.com/in/david-amado/](http://www.linkedin.com/in/david-amado/)

Página web: [www.blackpol.net](http://www.blackpol.net)



## RESUMEN

En el presente, se aborda desde una cuestión tanto teórica como práctica el funcionamiento de Blockchain, permitiendo al lector comprender cuál es su funcionalidad, sus elementos integradores, su aplicación en el mundo actual y los retos que trae a futuro el uso de esta tecnología. Asimismo, se explica que Blockchain será la base para una tecnología más desarrollada que venga después, pero que por seguro buscará cubrir de una mejor manera los objetivos claves que busca alcanzar Blockchain.

Por otro lado, se analiza la labor de los abogados en torno al uso de la tecnología, el cómo debemos cambiar nuestra visión para acoplarnos a un mundo totalmente revolucionado y en constante cambio tras la innovación tecnológica, lo que hace que el derecho ya no se practique o deba practicarse de la misma manera a como se hacía hace 50 años, donde la tecnología no tenía ni remotamente los alcances que hoy en día. El abogado actual debe de comprender que las necesidades de los clientes y los clientes en sí mismos, han cambiado radicalmente, cuestión que queda demostrada teniendo enfrente al sector tecnológico como la potencia económica mundial, conformada principalmente por el quinteto GAFAM (Google, Apple, Facebook, Amazon y Microsoft)

## ABSTRACT

*This article deals with the operation of Blockchain on a theoretical and practical approach allowing the reader to understand functionality, integrating elements, today's uses, and future challenges of this technology. It is further explained that Blockchain will be the foundation for newer technologies that will seek to better cover the key objectives that Blockchain seeks to achieve.*

*At the same time, we analyze the use of this technology by current professionals. Explaining our vision in a world that is constantly changing due to technological innovations. As a result, law in the future, will change and will no longer be practiced the way it is practiced today. Technology will become a key component. Today's professionals need to understand that both clients and their needs have changed and this is demonstrated by having the technology sector as one of the world's economic powers composed mainly by the GAFAM (Google, Apple, Facebook, Amazon and Microsoft).*

## PALABRAS CLAVES/KEY WORDS:

#Blockchain #SmartContracts #Tokens #LegalTech #NewLaw

## INTRODUCCIÓN

El exponencial desarrollo de la tecnología, han hecho que la sociedad se esté viendo continuamente transformada en todos sus ámbitos. Las investigaciones en materia de computación cuántica, el desarrollo de la inteligencia artificial o el Internet de las Cosas (IoT), no son más que algunos ejemplos relevantes que nos ayudan a afianzar la concepción de que estamos ante la cuarta etapa de la revolución industrial o incluso que ya estamos entrando en la quinta etapa de ésta.

La tecnología está constantemente retando al abogado tradicional, tanto en la manera en la que se lleva a cabo la profesión, así como en la interpretación que se le tiene que dar a la legislación cuando entra en juego algún elemento tecnológico que no está previsto en el ordenamiento.

El presente artículo intenta explicar qué es Blockchain, sus diferentes tipos, sus usos y algunos retos que ya se presentan tanto en el ámbito financiero como en el ámbito de derecho mercantil o corporativo.

## ¿QUÉ ES BLOCKCHAIN?

De entre todas las tecnologías que han surgido en los últimos años, hay una que ha tenido un auge importante y que también que trae consigo muchas dudas e inquietudes por no conocer realmente de qué se trata. Me refiero en esta ocasión al «Blockchain» (o denominada en español “cadena de bloques”). Quienes han oído hablar del término lo suelen asociar a las famosas criptomonedas, pero lo que puede ofrecer Blockchain es mucho más y cada vez tendremos que estar más familiarizados con esta tecnología, pues los procesos comerciales, jurídicos, de producción y muchos más comenzarán cada vez a implementar esta tecnología o por lo menos, el futuro se basará en tecnologías similares que permitan dar seguridad y confianza, desarrolladas y mejoradas tomando como base inicial Blockchain.

Respecto al origen de Blockchain, siempre han existido incertidumbre y contradicciones, puesto que el desarrollo informático pasó por varias facetas e incluso algunos avances han sido bajo el anonimato. Sin embargo, intentaré recapitular la historia de Blockchain tomando en consideración las teorías más aceptadas por los expertos.

Aquellos familiarizados con el término normalmente lo asocian al año 2008 con un creador anónimo llamado Satoshi Nakamoto,

<sup>1</sup> ligado a un movimiento tan novedoso como es, o era, el Criptoanarquismo,<sup>2</sup> donde tuvo aparición la criptomoneda *Bitcoin*. Sin embargo, Blockchain dista de ser una tecnología reciente, ya que su origen teórico se remonta a años atrás, en la década de los 90’s cuando empezó a desarrollarse de forma embrionaria. En el año 1991, W. Scott Stornetta, físico estadounidense y su colaborador, Stuart Haber, trabajaron en un estudio cuyo fin era describir un sistema de jerarquía digital. El objetivo principal de la investigación fue buscar la creación de mecanismos que pudieran crear sellos de tiempo digitales y ordenar los archivos registrados de forma única y segura.<sup>3</sup>

Esos mecanismos fueron las cadenas de bloques, encontrándose protegidas criptográficamente sin que nadie pudiera manipular las marcas de tiempo de los documentos. De modo que la implementación y uso de esos mecanismos permitieron que desde aquellos años se sentaran las bases de esta tecnología que conocemos hoy en día como Blockchain.

Luego en 1998, Nick Szabo describió un sistema descentralizado de pagos basado en el uso de técnicas criptográficas para facilitar la generación de unidades de valor virtual de forma estructurada (sistema hoy conocido como «*proof-of-work*»<sup>4</sup>).

1 Reseñado por primera vez en el libro blanco llamado “*Bitcoin: A Peer-to-Peer Electronic Cash System*” (2008).

2 VÁZQUEZ GARCÍA, R., “Ponga un algoritmo en su vida. Blockchain, Bitcoin, Fintech y otros barbarismos al uso”, *La Notaría*, núm. 1/2, 2017, págs. 36-41.

3 Academy Bit2me, disponible en sitio web: <https://academy.bit2me.com/quien-es-w-scott-stornetta/> ( Fecha de consulta 20 de mayo de 2020).

4 PORXAS, N., y CONEJERO, M., “Tecnología *Blockchain*: funcionamiento, aplicaciones y retos jurídicos relacionados”, *Actualidad jurídica Uriá & Menéndez*, núm. 48, 2018, págs. 24-36.

Debido a la aparición y estudio de las criptomonedas, se empieza a estudiar dicha tecnología por su peculiar funcionamiento y atributos, pues los usuarios de éstas querían saber cuál era la seguridad de apostar o invertir en ellas y cómo se podía asegurar lo que sus creadores afirmaban sobre la seguridad, inalterabilidad y descentralización de las transacciones.

Poco tiempo después, se vislumbró una tecnología revolucionaria en el paradigma cotidiano y posible de producir innovaciones en otros ámbitos, no quedando reservado exclusivamente su uso en el mercado financiero y trayendo ventajas como la eliminación de los gastos de intermediación y la imposibilidad de alterar el registro. Incluso algunos se beneficiaron de la descentralización implementando la tecnología para llevar a cabo negocios ilícitos a través de ella como es el lavado de dinero o blanqueo de capitales.<sup>5</sup>

Blockchain proporciona una base de datos distribuida inmutable y públicamente, conformando un sistema abierto que potencia la confianza a través de la transparencia y la solidez de la técnica de su construcción. No obstante, esta tecnología provoca escepticismo, planteando varias incógnitas como: ¿en qué se basa? ¿qué elementos lo integran? ¿cuál es su grado de fiabilidad? ¿para qué puede emplearse? ¿qué ventajas trae su uso?

Todas las preguntas en torno a Blockchain se han ido respondiendo con el paso del tiempo, lo que en un primer momento parecía no ser fiable, ha terminado siendo una tecnología disruptiva. De hecho, según numerosos juristas especializados en derecho de las tecnologías, su uso puede contribuir al desarrollo de la sociedad, y una mejora en la vida cotidiana, alcanzando el éxito en sectores como el jurídico, el bancario, el entretenimiento y otros más, algunos conocidos y otros por conocer.

## ¿CÓMO FUNCIONA LA CADENA DE BLOQUES?

Es necesario advertir que hay varios tipos de Blockchain, que posteriormente abordaremos, siendo la Blockchain pública la más utilizada. Muñoz Pérez señala que en la Blockchain pública los usuarios participan en la red de forma directa, sin intermediarios de ninguna clase, conectados gracias a Internet y algoritmos matemáticos.<sup>6</sup> Por tanto, en la tecnología Blockchain el único intermediario es la tecnología, sin que intermedie gobierno ni autoridades controladoras. Es decir, al ser una tecnología pública, de licencia libre, no perteneciente a ninguna compañía o gobierno, no cuenta con el respaldo de ninguna organización Internacional, Estado u organización. Son los propios usuarios, quienes mantienen el funcionamiento, y la tecnología es la que sirve como base de confianza. Que se trate de una base de datos descentralizada se traduce a que hay una eliminación de los entes, dando lugar a que los que distribuyen, emiten, regulan y validan la transacción o el intercambio de información, son los mismos usuarios que acceden a esa base de datos compartida, pero con la intervención de los nodos, que más adelante explicaremos de qué se tratan.

La descentralización o distribución, permite que los usuarios se encuentren unidos los unos a los otros mediante el uso de técnicas criptográficas, cuya manipulación resulta imposible o casi imposible si se contemplaran las manipulaciones *off-chain* o fuera de la red (mundo físico).

Cuando hablamos de Blockchain, es frecuente confundir el concepto con el de Distributed Ledger Technology (DLT por sus siglas en inglés). Generalmente se tiende a pensar que ambas son lo mismo, pero la relación entre éstas podría describirse para efectos prácticos, como una relación género-especie, donde Blockchain es un tipo de DLT. Una DLT es una simple base de datos que es gestionada por los participantes que la crean y se encuentra descentralizada. Esto se traduce en una ventaja respecto a

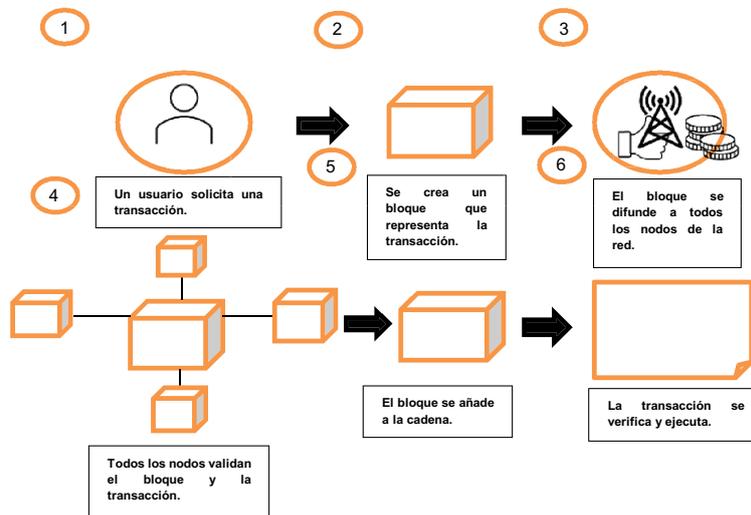
5 Bolsamanía, “Blockchain: la tecnología que cambiará las finanzas mundiales”, disponible en el sitio web: [https://www.bolsamania.com/noticias\\_amp/economia/Blockchain-la-tecnologia-que-cambiara-las-finanzas-mundiales—2370508.html](https://www.bolsamania.com/noticias_amp/economia/Blockchain-la-tecnologia-que-cambiara-las-finanzas-mundiales—2370508.html) (Fecha de consulta 13 de mayo de 2020).

6 MUÑOZ PEREZ, A.F, “Criptomonedas, el dinero mágico. Aspectos jurídicos”, *Revista de derecho del mercado de valores*, núm.,21,2017, págs.1-3.

anteriores sistemas de registro de datos, pues una DLT aumenta la transparencia de la información que es registrada, dificultando cualquier tipo de manipulación o fraude y, por tanto, siendo más complicada de *hackear*. Blockchain es un tipo de DLT con características particulares, especialmente porque como su nombre lo indica, su funcionamiento se basa en bloques que forman una cadena. Cada bloque va a tener su propio ADN o huella, es decir, la transparencia está asegurada mediante una firma criptográfica. Esto significa que en cada bloque se anota una determinada información o transacción, que estará encriptada, que quedará registrada y no podrá verse alterada o modificada si no se tiene permiso.

Esta tecnología, como tipología de una DLT, “permite a los usuarios grabar y almacenar permanentemente, simultáneamente y públicamente los datos introducidos en un programa que comparte un colectivo de personas en distintas máquinas telemáticas o servidores informáticos llamados nodos”.<sup>7</sup> La introducción de datos se realiza empleando claves criptográficas. Los registros distribuidos permiten a varios usuarios operar en un mismo espacio en Internet, quedando grabados en la base, aquellas anotaciones o transacciones que realizan, pudiendo recuperarse posteriormente, pero sin sufrir alteraciones. Blockchain posee cuatro características principales: i) almacenamiento de datos descentralizado; ii) cifrado; iii) inmutabilidad; y iii) un algoritmo de consenso.

El almacenamiento de datos en un libro mayor descentralizado supone que se registre en aquél, la información o transacción que realizan los usuarios. Esa información no se queda permanente, sino que se dispersa entre los distintos participantes de Blockchain. La información que contiene cada bloque estará cifrada. La verificación de la transacción o información se realiza por grupos de trabajo o consenso de los denominados nodos, cuyos algoritmos trabajan para que la información sea coherente e inmutable en la red y evitan que los usuarios agreguen información sin autorización de la red. A continuación, incluyo un esquema para ilustrar gráficamente cómo funciona la operación y la cadena de bloques que integran Blockchain:



Para entender completamente las características de Blockchain, es necesario conocer cuáles son los elementos que la conforman:<sup>8</sup>

**I. Libro mayor o libro de contabilidad digital (Ledger).** Aquí es donde quedan registradas las transacciones o información efectuadas por la red, construyendo bloques que se enlazan uno detrás de otro. El buen funcionamiento dependerá del bloque anterior.

7 IBAÑEZ JIMENEZ, J.W., “Blockchain: primeras cuestiones en el ordenamiento español”, Dykinson, 1.ª edición, Madrid, 2018, pág.15,

8 PYMNTS, “Blockchain tracker: back to basics”, disponible en el sitio web: <https://www.pymnts.com/blockchain/2017/blockchain-tracker-back-to-basics/> (Fecha de consulta 13 de mayo de 2020).

**II. Nodos.** Ordenadores conectados a la red que utilizan un software que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques.<sup>9</sup> Son computadoras que se configuran como los máximos garantes de la seguridad de la red, su función principal es el almacenamiento de una copia del libro mayor, velar por la integridad de las normas de la red y verificación de las transacciones e información transmitida.

**III. Criptografía.** Es la que permite crear pruebas matemáticas que proveen de seguridad, mediante la creación de claves numéricas que solo conocerán aquellos autorizados para acceder a la información.

En otras palabras y resumiendo lo explicado previamente, *Blockchain* mediante un protocolo informático de código abierto, permite la gestión de bases de datos de forma descentralizada, sin tener que contar con una autoridad o entidad poseedora de la información que actúe como garante o intermediaria.<sup>10</sup> Es como si se tratase de un Registro Público que acumula los distintos movimientos e intercambios en una red y los transcribe para que sean seguros y difíciles de falsificar.

## V. ¿CUÁLES SON LOS PRINCIPALES TIPOS DE BLOCKCHAIN?

Podemos diferenciar tres tipos de *Blockchain*: públicas, privadas e híbridas o también llamadas de consorcio.<sup>11</sup>

**I. Pública:** es aquella donde todo el mundo puede participar. Todas las transacciones realizadas son de dominio público, sin que se requiera un permiso especial ni admisión equivalente de los usuarios para poder operar en la *Blockchain* y es manejada por el consenso entre los usuarios de la misma. En las Blockchains públicas hay un libro público visible públicamente y están completamente descentralizadas, es decir, no hay ningún registro único donde se englobe toda la operación que se registra, la información está en movimiento entre todos los operadores que conforman la red. Los ejemplos más conocidos de Blockchains públicas son Bitcoin y Ethereum.

**II. Privada:** a diferencia de la Blockchain pública, ésta no es abierta al público y los usuarios pueden establecer condiciones que tendrán que cumplir los potenciales nuevos usuarios si quieren adherirse a ésta, además de disponer de una invitación, pues están ideadas para transacciones en un marco cerrado. Las más relevantes son Hyperledger,<sup>12</sup> R3<sup>13</sup> o Ripple. Las Blockchains privadas están menos descentralizadas y suelen utilizarse en grupos más pequeños de usuarios; asimismo, encontramos un uso práctico de ésta en administraciones de datos o auditorías internas de una sola empresa, en la que su lectura pública puede no ser necesaria ni recomendable en muchas ocasiones.

**III. Híbridas o Consorcio:** son aquellas parcialmente privadas y públicas, mezclan las dos anteriores conjugando características de las mismas, aunque también poseen diferencias entre sí. En esta, los nodos participantes son usuarios e inspeccionan el proceso de aprobación, pero las transacciones son de carácter público, es decir visibles para todo el mundo, sean o no participantes de la Blockchain. Por ejemplo, 15 organizaciones, cada una de las cuales maneja un nodo y 10 de ellas deben validar para que el bloque sea legítimo. Su principal ventaja es que son más rápidas y poseen

9 ÉCIJA BERNAL, A., “El dinero virtual”, *El ciberespacio, un mundo sin ley*, Wolters Kluwer, 2017, págs. 116-117.

10 PORXAS, N., y CONEJERO, M., “Tecnología Blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados”, *Actualidad jurídica Uría & Menéndez*, núm. 48, 2018, págs. 24-36.

11 Abanca innova, “ Los tipos de blockchain: pública, privada o consorcio”, disponible en el sitio web: <http://abancainnova.com/es/opinion/los-tipos-de-Blockchain-publica-privada-o-consorcio-explicados/> (Fecha de consulta: 20 de mayo de 2020).

12 Disponible en el sitio web: <https://www.hyperledger.org/>, perteneciente a la fundación Linux (Fecha de consulta 13 de mayo de 2020).

13 Disponible en el sitio web: <https://www.r3.com/> (Fecha de consulta 13 de mayo de 2020).

mayor privacidad en las transacciones. Algunas de las más conocidas son BigchainDB o Evernym.

## ¿CUÁLES SON LOS USOS QUE SE LE PUEDEN DAR A BLOCKCHAIN?

Las monedas virtuales como el *Bitcoin*, *Ethereum* o *Dash* suponen los ejemplos por antonomasia de la realidad práctica de la tecnología *Blockchain*, pero dentro del listado de usos y aplicación, encontramos también los siguientes:<sup>14</sup>

- I. **Como medio de transacción y sistema de pago.** Donde mayor repercusión ha tenido Blockchain ha sido en el sector financiero, con la aparición de Bitcoin. Los elementos inherentes a Bitcoin y las criptomonedas en general, hacen que sea una novedad no solamente financiera, sino una interrogante y preocupación constante para la política monetaria. Debido a las características que conforman la tecnología Blockchain, como el anonimato, seguridad o celeridad a la hora de efectuar transacciones, el aumento de usuarios de criptoactivos es exponencial. Hoy en día existe una gran variedad de oferta de criptomonedas, hasta llegar al grado de que Facebook ha anunciado el lanzamiento de su propia criptomoneda llamada “Libra”, cuestión que abordaré más adelante.
- II. **Como medio de registro de documentos.** Esta función no atiende exclusivamente a activos digitales, sino de cualquier cosa virtual, dando acceso a varias partes en cualquier lugar del mundo. Esta utilidad se ve materializada gracias a procesos y herramientas de verificación y autenticación. Esta aplicación se podría materializar tanto en el ámbito privado como en el público. Un libro privado en Blockchain puede ayudar a crear un registro resistente a la falsificación. Esto permite abrir nuevas fronteras a la hora de automatizar procesos de negocio.
- III. **Como medio de seguimiento de la cadena de suministros.** Uno de los retos es la verificación de la procedencia de las cosas. Gracias a las características que revisten la tecnología *Blockchain* y su estructuración en cadena de bloques, se puede sellar casi cualquier objeto con una huella digital denominada *hash*, permitiendo que se encuentre identificado y sea auténtico en todo momento, impidiendo que el proceso sea alterado o modificado sin que las partes se enteren, pues si se altera o cambia algún elemento, el *hash* también se modificaría y las partes tendrían conocimiento de ello.
- IV. **Smart Contracts o contratos inteligentes.** Estos contratos basan su funcionamiento en la tecnología *Blockchain*, contribuyendo a ejecutar acuerdos establecidos previamente por las partes (los usuarios e individuos que celebran el contrato), y que, una vez cumplidas las condiciones estipuladas en el contrato, automáticamente se ejecuten sin necesidad de intervención de un tercero o de las mismas partes.
- V. **Comercio.** La innovación que ofrece la tecnología *Blockchain* permite reforzar la autonomía de la voluntad de las partes, es decir, de control en el tráfico jurídico por parte de los empresarios y los consumidores. En el caso de transacciones transfronterizas entre empresas internacionales, supone un ahorro de costes tales como comisiones bancarias o documentos crediticios.
- VI. **Protección de los derechos de la propiedad intelectual y de autor.** La utilización de la *Blockchain* en libros electrónicos, música o fotos es un mecanismo efectivo para prevenir la piratería e impulsar las ventas mediante la garantía de autenticidad de las obras.
- VII. **Como sistema de votación.** Ya se está planteando en diversos países el implementar esta tecno-

14 WADHWA, T., BOBKOFF, D., “Blockchain could soon power stock markets, music sales, and even prevent child labor”, disponible en el sitio web: <https://www.businessinsider.nl/what-is-Blockchain-2016-10/?international=true&r=US>); CLANCEY, “Could Blockchain Really Replace The Need For Clearinghouses?”, disponible en el sitio web: <https://www.risktech-forum.com/opinion/could-Blockchain-really-replace-the-need-for-clearinghouses> (Fecha de consulta 14 de mayo de 2020).

logía para en un futuro votar telemáticamente. Blockchain garantizaría que la persona no vote más de una vez, su anonimato, y la inmutabilidad de lo votado. Otra de sus ventajas sería la reducción de costes que conlleva una elección, así como una mayor rapidez de votación y gestión de los votos.

**VIII Como almacenamiento en una nube.** La tecnología permite almacenar datos en una red basada en *peer to peer*, de igual a igual, quedando los datos guardados simultáneamente por cada uno de los miembros de la red. Cada miembro cuenta con un espacio donde almacenar información y es compartido con los demás miembros, siendo la misma información en cada dispositivo. Hay varias copias idénticas en un mismo tiempo, pero en espacios diferentes, lo que garantiza que se trata de un método más seguro, pues al haber más copias idénticas de esa información, es menos probable que sea robada o destruida.

**IX. Como gestión de identidades.** Dentro de poco, prescindiremos de un usuario y contraseña para acceder a webs como medio de identificación (ej. cuenta de Facebook), sustituyéndolo por ID propia creada por nosotros gracias a la tecnología *Blockchain* para acceder a webs y firmar documentos digitales. La identidad de la persona se verificará por los demás miembros que formen la red.

**X. Como un registro de salud.** también puede utilizarse como un mecanismo seguro para la creación de registros médicos electrónicos de pacientes, pudiendo ser accesible desde cualquier parte y en cualquier momento. No obstante, esta Blockchain sería privada, para garantizar el derecho a la intimidad de los pacientes y el secreto profesional del médico. Al ser privada, los participantes de la red necesitarían una clave cifrada.

**XI. Como Registro de la Propiedad.** Son varios los países como Suecia o Georgia los que están probando crear un registro de la propiedad electrónico, consiguiendo almacenar los contratos de compraventa, la titularidad, cargas, transacciones realizadas, entre otros datos, de modo que se evite la existencia de cualquier tipo de manipulación en los documentos o fraude. Esto permitiría que los participantes de la red pudieran conocer toda información relativa a su propiedad en tiempo real.

Como podemos apreciar, son innumerables las opciones de uso que se le pueden dar a Blockchain. Esto significa eficientar y tener mayor seguridad en las tareas que realizamos en nuestro día a día. Blockchain ofrece no solamente ventajas meramente tecnológicas, sino que genera un clima de confianza, transparencia y de seguridad, siendo un medio idóneo para establecer algún tipo de acuerdo en el que se lleve a cabo la contraprestación una vez se hayan cumplido ciertas cláusulas suspensivas o resolutorias establecidas en él. Asimismo, promueve la productividad, asegurando ser eficiente en contraposición a instituciones con trabas burocráticas y poco útiles.

Lo anterior nos lleva en el ámbito del Derecho, a hablar de los famosos Smart Contracts y su implementación.

## VI. SMART CONTRACTS

Últimamente está siendo utilizada cada vez más la acepción de Smart Contracts o contratos inteligentes, pero este término no es del todo preciso, pues esta figura no se refiere a un contrato como tal, sino más bien es un software que permite ejecutar automáticamente lo pactado en los contratos. Díaz Díaz<sup>15</sup> explica que se trata de “un programa informático que ejecuta la voluntad reflejada en acuerdos entre

15 DÍAZ DÍAZ, E., Legaltoday, “Una aplicación jurídica del Blockchain: los smart contracts”, disponible en el sitio web: <http://www.legaltoday.com/firmas/legaltech/una-aplicacion-juridica-del-Blockchain-los-smart-contracts> (Fecha de consulta 25 de mayo de 2020).

dos o más partes, de modo que sus efectos son el resultado de que se cumplan una serie de condiciones específicas”. En definitiva, podemos decir que es un programa informático de órdenes condicionadas que garantizan el cumplimiento de un acuerdo de forma automática y segura, mediante la ejecución de una cláusula correspondiente programada con anterioridad.

Tradicionalmente, los contratos han necesitado de la intervención de diferentes operadores jurídicos tales como abogados, notarios o jueces para la creación de los contratos, la verificación de su contenido, su cumplimiento y la ejecución de los mismos. No obstante, con el surgimiento de los smart contracts, la intervención de aquellos se ve reducida. Los smart contracts se configuran basados en el principio de la autonomía de la voluntad de las partes. Éstos son los protagonistas, los que deciden cómo y cuándo se ejecuta lo que contiene el programa, el smart contract, es decir, establecen los parámetros para la ejecución.

Esto se plasma de la siguiente manera: los acuerdos a los que llegan se materializan en un programa informático, pero antes, es necesario que ese acuerdo se codifique para que pueda ser leído por el programa, y en su caso, ejecutado de cumplirse las condiciones estipuladas previamente por las partes o al término del mismo.

Los smart contracts van a permitir que los contratos se ejecuten de forma automática, sin necesidad de intermediarios en un negocio jurídico, pero aún el humano no desaparece totalmente del panorama, pues es necesaria la labor de un abogado para redactar el contrato que posteriormente se traducirá en algoritmos y en caso de alguna desavenencia, siempre quedará la labor de los jueces y árbitros.

Los smart contracts no son un tipo de contrato, sino que son una forma de articular un proceso contractual, facilitando el desarrollo y cumplimiento de lo estipulado por las partes y las consecuencias que deriven de su cumplimiento o incumplimiento. Lo relevante de esta figura y donde realmente tiene una especial relevancia es en contratos donde la prestación puede ejecutarse de manera automática y/o autónoma, pues existen diversos contratos que mientras no avance la tecnología, no puede establecerse automáticamente un cumplimiento o ejecución.

El smart contract permite ejecutar un acuerdo entre las partes, pero para que se ejecute es necesario que se encuentre en un lenguaje de códigos, esos códigos están supeditados a unos protocolos o instrucciones, que trabajan de forma condicionada, “IF/THEN”, “Si A... entonces B...” por tanto, se desplegarán los efectos del contrato, cuando el dispositivo lea ese código y verifique que se cumplen las condiciones para dar lugar a su ejecución. Por lo tanto, el contrato en forma de programa se ejecuta por sí solo si se cumplen las condiciones correspondientes. Este hecho conlleva a que nadie tenga que vigilar el proceso, eliminando costes de tiempo y dinero en el proceso y simplificando la tarea, resultando mucho más eficiente.<sup>16</sup>

Un tema relevante a destacar, es que la interpretación y argumentación jurídica, como una de las principales figuras que empleamos los abogados en nuestra labor de juriconsultos, desaparece con este tipo de ejecución automática, pues el funcionamiento es simple y su lectura no da lugar a interpretaciones. De modo que, si se cumplen las condiciones establecidas, el contrato ejecuta automáticamente la consecuencia a esa acción. Esto genera grandes ventajas y puede resultar eficiente, pero también deja un vacío que puede llegar a ser sumamente peligroso en el ámbito jurídico.

Para la eficacia de los smart contracts es necesario un marco de confianza y seguridad. Se busca una tecnología que permita la inmutabilidad del código, que registre y verifique el cumplimiento de las prestaciones o transacciones y facilite la ejecución de las mismas. Blockchain es la solución tecnológica que da respuesta a esas necesidades, pues los smart contracts van de la mano con la dicha tecnología, pues utilizan su infraestructura para que las condiciones establecidas por las partes sean almacenadas en una base de datos dentro de una red, apoyándose en el marco de confianza y seguridad

---

16 *Ibidem*.

de Blockchain y brindándole la inmutabilidad requerida en un convenio, asegurando que los códigos no sean alterados.

En algunos casos, los smart contracts necesitan obtener información del exterior con el fin de concretar las prestaciones o su cumplimiento. En este contexto, se acude a un intermediario, un tercero para que informe si se debe o no seguir con la ejecución de las prestaciones. Esta figura es generalmente denominada “oráculo”, que es el encargado de verificar información de la que depende que el contrato se auto-ejecute y en función de la información recibida por éste, se realiza o no la ejecución automática de las operaciones programadas.<sup>17</sup> Es importante siempre prever que por seguridad, los oráculos que se elijan estén descentralizados o den seguridad a la operación. Un proveedor de oráculos que está siendo bastante seguro y que su popularidad va subiendo es “Chainlink”.

Los smart contracts se caracterizan por ser: públicos, seguros, inmutables y fiables gracias a la tecnología Blockchain. Por lo anterior, se han desarrollado diversos usos de estos smart contracts, siendo las DAOs de las figuras más innovadoras tanto a nivel tecnológico, como económico y jurídico.

## VII. ORGANIZACIONES AUTÓNOMAS DESCENTRALIZADAS (DAOs)

Las Organizaciones Autónomas Descentralizadas o DAOs como se conocen por sus siglas en inglés (Decentralized Autonomous Organizations). Son comunidades en línea incorporadas a Blockchain utilizando un código de contrato inteligente que regula su gobierno, sus estatutos y la propiedad de sus activos.

Una DAO es “una entidad nativa de Internet sin administración central que está regulada por un conjunto de reglas automáticamente exigibles en una cadena de bloques pública, y cuyo objetivo es adquirir vida propia e incentivar a las personas a lograr una misión común compartida”.<sup>18</sup> En una DAO los miembros de esa comunidad toman las decisiones electrónicamente mediante un voto o código. Su funcionamiento está basado en un sistema de reglas codificadas que establecen las normas que hay que seguir.<sup>19</sup>

Se concibe DAO como “una organización virtual definida por smart contracts” siguiendo los principios de descentralización de una tecnología Blockchain.<sup>20</sup> Con su aparición se da paso a la posibilidad de construir organizaciones descentralizadas, lo que implica que las decisiones no se toman de forma vertical, sino horizontalmente y mediante el consenso de todos los miembros de la red. Esto acaba con las formas de organización a las que estamos acostumbrados.

Por tanto, en una DAO, su estructura y cohesión no depende de contratos de trabajo sino en el cumplimiento de lo establecido en los smart contracts que también son almacenados en la Blockchain.<sup>21</sup> La primera DAO fue la denominada “THE DAO”, nacida en la Blockchain Ethereum, en 2016. Su creación fue financiada mediante la venta de tokens a cambio de la moneda de Ethereum. El lenguaje de programación del smart contract fue Solidity, que según los programadores era sólido e inquebran-

17 ÁLVAREZ DE LA VEGA, L., El País, “ Smart contracts, oráculos y jueces”, disponible en el sitio web: [https://cincodias.elpais.com/cincodias/2019/05/17/legal/1558091069\\_957664.html](https://cincodias.elpais.com/cincodias/2019/05/17/legal/1558091069_957664.html) (Fecha de consulta 26 de mayo de 2020).

18 Decentralized Autonomous Organizations, disponible en el sitio web: <https://aragon.org/dao> (Fecha de consulta 25 de mayo de 2020).

19 NOGALES, B., Bitcoin, “ ¿ Qué es una DAO?”, disponible en el sitio web: <https://bitcoin.es/criptomonedas/que-es-un-dao-organizacion-autonoma-descentralizada/> (Fecha de consulta 25 de mayo de 2020).

20 AGRAWAL, R., “DAO: Democratizing ownership of organization through smart contract on Blockchain”, disponible en el sitio web: <https://medium.com/@xragrawal/dao-democratizing-ownership-of-organization-through-smart-contract-on-Blockchain-19d080332591> ( Fecha de consulta 26 de mayo de 2020).

21 Vector ITC, “DAO, una nueva forma de organización basada en la descentralización”, disponible en el sitio web: <https://www.vectoritcgroup.com/tech-magazine/innovation-trends/dao-una-nueva-forma-de-organizacion-basada-en-la-descentralizacion/> (Fecha de consulta 26 de mayo de 2020).

table. Sin embargo, ocurrió un problema que llevó a descubrir que había un fallo en el código fuente de Solidity, permitiendo que un tercero se aprovechara de ese fallo y obtuviera beneficios económicos.

Las DAOs está compuesta por tres elementos:

- I. Token Holders:** son aquellos que invierten, en principio, dinero a cambio de una criptomoneda (Ether), la cual posteriormente se invierte en un proyecto a cambio de recibir tokens, los cuales son libremente transmisibles y asignan la propiedad y el derecho de voto.
- II. Contractors:** son los que envían una propuesta a una entidad DAO. Por ejemplo, un guionista envía su borrador a una DAO para que evalúen si lo desarrollan en una película. Estas propuestas se hacen vía smart contracts con la finalidad de utilizar fondos o desarrollar productos o servicios.
- III. Curators:** son la entidad designada por la DAO que actúa como intermediario entre el mundo virtual de la sociedad y el real. Su principal labor es revisar las propuestas que se envían a la DAO y enviarlas a una “whitelist” si cumple con los requisitos. Esta *whitelist* es una lista en Ethereum de proyectos que pueden recibir Ether si la mayoría de los token holders han votado en sentido positivo.

Su funcionamiento está condicionado por varios mecanismos:

- I. Smart Contracts.** Para permitir condicionar acciones y hacer que estas se ejecuten de forma autónoma.
- II. Protocolo de consenso.** Con la finalidad de que las decisiones que se tomen en la organización hayan sido por consenso de las partes que conforman la red, sin que ningún factor externo o tercero intervenga directamente.
- III. Tokens.** Un token es un medio de cambio equiparable a una acción en una organización tradicional, confiriéndole representación, voto y permitiéndole obtener de la DAO beneficios.
- IV. Blockchain.** El mecanismo que hace inalterable la información una vez codificada y condicionada en un smart contract. Blockchain registra todo lo relativo a la DAO, garantizándose así que la información se encuentra protegida y transparente.

La DAO es buena para coordinar proyectos en común entre varias personas. Permite que varias personas se reúnan y trabajen en proyectos comunes de una manera muy simple. Asimismo, permite identificar la identidad de los demás miembros, sus finanzas y las decisiones tomadas.

Por un lado, sus puntos débiles entre otros son que los códigos empleados, difícilmente pueden modificarse y esto hace que si un código está mal programado, no se pueda modificar hasta que se obtenga el consenso de la mayoría de los miembros de la red, además al tratarse de una novedad que influye en varios sectores, se requiere que cumpla ciertas reglas legales y esto de momento, es una tarea pendiente, por su carácter novedoso aún queda camino para que se desarrolle una normativa que las regule.

Existen muchas incertidumbres respecto de las DAOs, por ejemplo, la responsabilidad de la empresa y de sus token holders, el régimen tan diferente de los tokens con respecto al capital de una sociedad, la ausencia de un órgano de administración, entre otros muchos temas e instituciones que tantos años los juristas teníamos claros y que ahora es momento de abordar, trayendo consigo no solo la incertidumbre, sino incluso la necesidad de modificar aquellas estructuras mercantiles que conocíamos e incluir estos nuevos conceptos que serán el mañana de una economía digital.

## VIII. RED ARAGON

Aragon es una StartUp que nació en España con la misión de descentralizar empresas en el mundo.

Se creó con la finalidad de probar al mundo la capacidad de autogestión de este tipo de empresas, siendo una plataforma que ofrece un conjunto de aplicaciones y servicios que permiten nuevas formas de comunidades globales como es una DAO.

El objetivo de Aragon es ayudar a crear fácilmente una DAO, proporcionando aquellos elementos necesarios para la administración de una empresa tales como un sistema financiero, sistema de representación y voto, estatutos, gestión de nóminas, etc., sin necesidad de intermediarios ni en la creación, ni en el mantenimiento de la misma.

Sin embargo, esta plataforma va más allá, cambiando no solo las instituciones mercantiles, sino también el papel de los abogados y árbitros, pues proporciona también un servicio de resolución de conflictos, ya que cuenta con un tribunal formado por un jurado de personas encargadas de resolver disputas que planteen los smart contracts y que no puedan resolverse, decidiendo, en su caso, las penalizaciones a imponer. A este tribunal se le conoce por Tribunal de Aragón, el cual se encarga de resolver disputas que surjan en el marco de un smart contract, debido a que van más allá de la automatización.

Para formar parte de este jurado, es necesario poseer el token nativo del tribunal, el cual es llamado Aragon Network Juror (por sus siglas en inglés, conocido como ANJ). Ese token tiene que ser activado para que sean seleccionados y obtengan sus honorarios por resolver las disputas. Los que deseen ser miembros del jurado se inscriben para que puedan ser elegidos mediante la activación de tokens de jurado de la red de Aragon (ANJ) en el smart contract del tribunal de Aragón. Cuántos más tokens se activen mayor es la posibilidad de ser elegido. Cada vez que se recluta un jurado para una disputa, una parte de sus tokens activados se bloquean hasta que finalice la disputa. Los miembros del jurado tienen una serie de deberes y responsabilidades como revisar los argumentos que viertan las partes en la disputa y emitir un voto.

Las disputas son creadas por los suscriptores del tribunal de Aragón, para formar parte de este deben primero abonar una tarifa de suscripción mensual. Creada la disputa, se permite presentar en un plazo de siete días una evidencia que posteriormente será revisada por los jurados del tribunal. Esa evidencia se puede enviar en formato de texto o enlaces HTTP e IPFS. Tras ese periodo, tiene lugar el reclutamiento de aquellos que van a formar el jurado. Las posibilidades de ser reclutado como jurado dependen de la cantidad activa de ANJ (a mayor cantidad mayor posibilidad de ser elegido). Posteriormente, se abrirá un periodo de votación, en este el jurado deberá revisar las evidencias presentadas y tratar de anticipar cual será la decisión que más voten los jurados. Para lograr un consenso, son incentivados mediante recompensa o penalizados en consecuencia. Es muy importante emitir el voto porque de lo contrario, a aquel que no lo hace, se le penalizará disminuyendo el valor de su token y redistribuyéndolo a los jurados ganadores tras la decisión final.

Hay tres tipos de votos: permitir, bloquear o negarse a votar. La clave para ganar es votar de la manera que se cree o espera que vote una pluralidad de miembros del jurado. Para que se mantenga el voto secreto, se le adjudica un código aleatorio que se recomienda guardar en un sitio seguro. Finalizado el periodo de votación, los miembros del jurado tendrán dos días para revelar lo que han votado. Una vez revelados los votos, los miembros podrán ver si votaron con la pluralidad o no, pero antes de que se dicte el fallo, se abre un periodo de apelación.

El resultado decisivo más votado es el que gana, sin necesidad de mayorías, basándose en la pluralidad de votos. Los jurados pueden negarse a votar una decisión si creen que los argumentos no son coherentes o no están completos. La decisión final se envía al smart contract que desencadenó la disputa.<sup>22</sup>

---

22 Aragon Court, disponible en el sitio web: <https://help.aragon.org/article/41-aragon-court> ( Fecha de consulta 26 de mayo de 2020).

Otra plataforma que permite resolver disputas subjetivas en smart contracts con Blockchain es Kleros. Kleros pone a disposición de las empresas un tribunal formado por un jurado de personas. Para ser jurado es necesario tener el token de Kleros, PNK, que funciona bajo las mismas reglas del ANJ (cuantos más se tenga más alta es la probabilidad de que sea elegido como jurado). Votando coherentemente, con la mayoría, se gana ETH y PNK. Votando incoherentemente, aquello que vota la minoría, se pierde PNK.<sup>23</sup>

## IX. BLOCKCHAIN EN EL MUNDO

La adopción de Blockchain por parte de los distintos Estados ha sido una cuestión que no está homogeneizada, pues algunos están trabajando arduamente para implementarla en sus Administraciones Públicas y en su política monetaria, mientras otros se rehúsan simplemente a adoptar una política monetaria basada en criptoactivos. Por lo anterior, resulta sumamente interesante analizar la situación actual de los países respecto de esta tecnología.

**I. Europa:** derivado del mercado económico común, Europa es uno de los mayores puntos financieros del mundo y la intención de las instituciones es posicionar a Europa a la vanguardia de esta tecnología. La Comisión Europea está trabajando para investigar los modos en los que se puede aplicar esta tecnología. Un ejemplo de ello es que en abril del año 2008 se puso en marcha la *European Blockchain Partnership* que tiene como objetivo extender una red de nodos de Blockchain a lo largo del continente. En el año 2016 la Comisión propuso incluir a los proveedores de carteras de custodia de moneda virtual y las plataformas de intercambio dentro de la Cuarta Directiva contra el lavado de dinero.

En abril de 2019 la Comisión, en su afán de asegurar la colaboración público-privada en el ámbito de Blockchain, estableció la *International Association for Trusted Blockchain Applications*, la cual reúne a proveedores y usuarios de *Distributed Ledger Technology* (DLT) con representantes de organizaciones gubernamentales y organismos de normalización de todo el mundo.<sup>24</sup> Por otro lado, ciertos sectores están fomentando la inversión en la *Blockchain*, desde el sector manufacturero, hasta la banca.<sup>25</sup>

**II. China y Asia Oriental:** La región de Asia es uno de los mercados más competitivos del mundo para los proyectos tecnológicos, ya que desempeñan un papel fundamental en el impulso del crecimiento económico de las mayores economías de la región, como es el caso de China y Singapur. Asia Oriental posee un papel destacado en lo que a patentes de Blockchain se refiere, siguiéndole a Estados Unidos en segunda posición.<sup>26</sup>

China, tratando de seguir liderando, está probando el desarrollo de una nueva moneda virtual llamada DCEP (por sus siglas en *Digital Coin Electronic Pay*). Con esta moneda digital, China busca vincular 1:1 su actual fiat el RMB (RenMinBi), su otra moneda embrionaria. El objetivo del gigante asiático es convertirse en una referencia económica cada vez más poderosa.<sup>27</sup>

**III. Estados Unidos:** con un marco normativo más afianzado, tras décadas de desarrollo tecnológico a sus espaldas, Estados Unidos actualmente se mantiene en cabeza en lo que a implementación

23 Kleros, “3 things to know about becoming a kleros juror”, disponible en el sitio web: <https://blog.kleros.io/become-a-juror-Blockchain-dispute-resolution-on-ethereum/> ( Fecha de consulta 26 de mayo de 2020).

24 BIRCH, J., “El estado de la tecnología Blockchain: los expertos opinan sobre la adopción en todo el mundo”, disponible en el sitio web: <https://es.cointelegraph.com/news/the-state-of-blockchain-experts-weigh-in-on-adoption-around-the-world> (Fecha de consulta: 25 de mayo de 2020).

25 *Ibidem*.

26 *Ibidem*.

27 Observatorio Blockchain, “DCEP, la criptomoneda con la que China quiere conquistar el mundo”, disponible en el sitio web: <https://observatorioBlockchain.com/dcep-la-cripto-de-privacidad-manejable-con-la-que-china-quiere-conquistar-el-mundo/>, (Fecha de consulta: 25 de mayo de 2020).

de esta tecnología se refiere. Se estima que Estados Unidos lleva invertidos cerca de 1.100 millones de dólares, superando los 661 millones invertidos por Europa Occidental y los 304 millones de China.<sup>28</sup>

Facebook, lanzó en 2019 su proyecto de moneda virtual denominada “*Libra*”. Varios socios se implicaron en el desarrollo y lanzamiento de esta nueva moneda, como son Uber, Spotify, Vodafone, Visa y PayPal, quienes buscan un objetivo en común, reinventar los pagos en la era de Internet. La idea de *Libra* es que ésta haga uso de su propia red de Blockchain. A diferencia de otras monedas virtuales como *Bitcoin*, *Ethereum* o *Ripple*, la intención de Facebook con *Libra* es que pueda intercambiarse por divisas reales a una tasa de cambio estable. En paralelo, Facebook además ha creado *Calibra*, la cual es una filial para ofrecer servicios financieros, y que tiene como intención integrar esta criptomoneda en WhatsApp y Facebook Messenger.<sup>29</sup>

Sin embargo, como todo proyecto que está aún en fase de desarrollo, se ha visto envuelto en una serie de cambios y reestructuraciones. Las compañías que en un inicio la respaldaban han abandonado el proyecto y Facebook se ha visto en la necesidad de replantear su plan con la criptomoneda, asimilándose más a una red de pago que una *stablecoin* (las criptomonedas afianzadas y respaldadas) como fue concebida en un principio, con el fin de vincularse a las monedas locales donde opere, y asemejándose más a una plataforma de pago tipo *PayPal*.<sup>30</sup>

**IV. Latinoamérica:** América Latina no es ajena a esta nueva realidad tecnológica y se encuentra en una fase de rápido crecimiento en su implementación. En esta parte del mundo destaca el proyecto presentado por el Banco Interamericano de Desarrollo, en el que se impulsa el uso de la tecnología Blockchain en la región, así como el *Big Data*, conjuntamente con proyectos en Colombia y Paraguay a través de LACChain, alianza a la cual se han ido sumando otros países.<sup>31</sup> De igual manera es reseñable que el mayor banco de inversión de la región, el Banco BTG Pactual SA, con sede en Brasil, ha revelado sus planes de lanzar un token de valor, que podría adquirirse con *Gemini Dollars* o *Ethereum*.

Para finalizar, debemos hacer mención del papel que juegan actualmente los bancos centrales. Hoy en día ya emiten reservas de dinero digital pero sólo a un grupo selecto de instituciones financieras, teniendo como objetivo estimular la competencia en la industria de los pagos.<sup>32</sup>

## X. CONCLUSIONES: EL PAPEL DEL ABOGADO EN EL SIGLO XXI

Aunque son evidentes las aportaciones que la tecnología Blockchain trae a los diversos sectores económicos, no podemos perder de vista que, como toda tecnología, está en constante desarrollo y, Blockchain principalmente, tiene aún mucho camino por recorrer, pues tendrá que solucionar los problemas particulares de cada industria e innovarse para cubrir los retos que sus usuarios cada vez pondrán sobre la mesa o incluso una tecnología competitiva.

28 LIMA, A., “Inversión centrada en Blockchain llega a USD 23.700 millones desde 2013”, disponible en el sitio web: <https://www.morocotacoin.com/2019/08/inversion-centrada-en-Blockchain-llega-a-usd-23-700-millones-desde-2013/>, (Fecha de consulta: 25 de mayo de 2020).

29 El País, “Facebook lanza Libra, su propia criptomoneda para usar en WhatsApp y Messenger”, disponible en el sitio web: [https://cincodias.elpais.com/cincodias/2019/06/18/mercados/1560850171\\_435534.html](https://cincodias.elpais.com/cincodias/2019/06/18/mercados/1560850171_435534.html), (Fecha de consulta: 25 de mayo de 2020).

30 RUS, C., “Libra, la criptomoneda respaldada por Facebook, se reestructura por completo y será más similar a PayPal que a Bitcoin”, disponible en el sitio web: <https://www.xataka.com/empresas-y-economia/libra-criptomoneda-respaldada-facebook-se-reestructura-completo-sera-similar-a-paypal-que-a-bitcoin>, (Fecha de consulta 26 de mayo de 2020).

31 BASTARDO, J., Cointelegraph “El BID presenta varios proyectos de implementación de Blockchains en Latinoamérica”, disponible en el sitio web: <https://es.cointelegraph.com/news/idb-presents-several-projects-to-implement-Blockchains-in-latin-america>, (Fecha de consulta 26 de mayo de 2020).

32 NIEPELT, D., VOX Columns “Digital money and central bank digital currency: An executive summary for policymakers” disponible en el sitio web: <https://voxeu.org/article/digital-money-and-central-bank-digital-currency-executive-summary>, (Fecha de consulta: 26 de mayo de 2020).

Ejemplos de lo anterior y que son áreas de mejora para la tecnología Blockchain son: el gran consumo de electricidad que se requiere; el elevado precio que conlleva la implementación inicial (pues a largo plazo está diseñada para ahorrar recursos); y sin que sea de menor importancia, el marco normativo tan incierto que la rodea.

La tecnología ha cambiado nuestra realidad, pues toda nuestra vida, hoy en día, gira en torno a ella y esto conlleva un enorme reto para el Derecho, pues, aunque éste siempre estará un paso atrás de la realidad, no se debe perder de vista que debemos acelerar nuestros procesos legislativos y debemos de estar conscientes de la responsabilidad que hemos adquirido como juristas.

Todo nuestro entorno está cambiando y el Derecho se está quedando rezagado a pesar de los grandes esfuerzos que hacen los Estados por regular aquellos escenarios que hace 20 años sólo eran ciencia ficción. La innovación tecnológica está poniendo en jaque la labor de los legisladores y juristas. Hoy más que nunca, como abogados tenemos un papel fundamental, debemos hacer frente a realidades que vivimos con legislación obsoleta y por lo tanto el derecho positivo ha dejado, en gran medida, de dar respuestas, dejando a la labor interpretativa un papel preponderante.

Con motivo de los avances que se están dando en el sector jurídico, efectos de la transformación y avance tecnológico, es necesario que el abogado tanto comprenda los términos, conceptos y procesos tecnológicos, como que también se apoya en la tecnología para prestar sus servicios. Ejemplo de lo anterior es que las Administraciones Públicas y de Justicia, están comenzando a digitalizarse, implementando mecanismos tecnológicos que permitan el llevar a través medios remotos diversas partes del procedimiento.

Nuestra vida va encaminada a realizar procesos cada vez más eficientes, rápidos, a distancia y de manera transparente y seguros. Esto no sería capaz de lograrse si no fuese con la tecnología. Asimismo, la provisión de bienes y servicios está cambiando radicalmente y los servicios del sector legal también lo están comenzando a percibir. Los clientes cada vez exigen procesos más eficientes, lo cual implica que el servicio se preste en menor tiempo y a un menor costo. Por ello, los abogados tradicionales están comenzando a ser suplidos por abogados que empleen lo denominado *New Law* o *Legal Tech*, que la prestación de servicios con apoyo de la tecnología, lo que permite alcanzar los objetivos que requieren los clientes y reduciendo recursos tanto económicos como humanos.

De lo anterior deriva la importancia de conocer el uso que en el sector legal tiene Blockchain, pues esta tecnología será empleada el día de mañana por muchas firmas de abogados para el resguardo de información, documentación y registros, para la firma de contratos, la autenticación y por supuesto, para implementar los famosos smart contracts. Asimismo, otras áreas del derecho como es el ámbito penal ya están evaluando el impacto de utilizar Blockchain para salvaguardar la cadena de custodia de las pruebas y periciales.

La labor de los abogados no está en peligro, no es real hablar de que el abogado va a ser suplido por algoritmos o por robots como algunos aseguran. La labor del abogado tiene un elemento de valor que no puede ser sustituido por la tecnología. Ese valor que le da la inteligencia, el razonamiento y el saber cómo aplicar e interpretar los conceptos jurídicos a la realidad que vivimos, es lo que hace que el abogado con la tecnología evolucione y, por ende, la forma en prestar los servicios cambie. Se comenzarán a requerir de abogados especializados y que sepan de tecnología, pero también habrá cabida para los abogados tradicionales; sin embargo, cada vez más se apelará a la eficiencia, pues en el mercado la competencia será por el que se apoye de la tecnología para prestar un servicio más eficiente, es decir, en menor tiempo y a menos costo, pero manteniendo o mejorando la calidad.

Es evidente también que las grandes firmas como las concebíamos tienen que comenzar a cambiar. Hoy en día la tecnología y los principales clientes que son del sector de las TIC's requieren que una firma de abogados no sea como ortodoxamente eran, es decir, el despacho formal que está lleno de abogados especializados. Lo que se requerirá de las mejores firmas es que en el mismo ambiente con-

vivan abogados, ingenieros, informáticos y programadores, pues eso es lo que le dará el valor añadido que buscan los gigantes tecnológicos.

Como abogados, debemos de cambiar nuestra práctica y nuestra mentalidad, para poder abordar de manera real y actualizada, los requerimientos y necesidades de los clientes. Debemos de innovar y comenzar a plantearnos el uso de la tecnología en nuestra labor diaria, pues esto nos permitirá, así como lo exigimos de la Administración Pública y de Justicia, brindar servicios en eficientes, transparentes y mejorando la calidad, generando de nuevo confianza en los abogados. El papel del abogado hoy en día es fundamental, pero debe saber perfectamente su lugar y saberse alinear a la realidad cambiante y tecnológica que vivimos, pues en caso contrario, los abogados que no vean este cambio quedarán obsoletos y estarán destinados al fracaso por no saberse anteponer al cambio tecnológico exponencial que estamos viviendo.



REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).  
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.  
ISSN 2530-4496 – AÑO 1, N° 8, 2020, PÁGS. 71-82

**EL USO DE BLOCKCHAIN PARA LA VALORACIÓN DOCUMENTAL  
CON MIRAS A LA CONFORMACIÓN DE LA MEMORIA HISTÓRICA EN MÉXICO**

THE USE OF BLOCKCHAIN FOR DOCUMENTARY ASSESSMENT  
WITH A VIEW TO THE CONFORMATION OF HISTORICAL MEMORY IN MEXICO

**Claudia Alin Escoto Velázquez<sup>1</sup>**

Instituto Nacional de Transparencia y Acceso a la Información y  
Protección de Datos Personales (INAI)

1 Maestra en Derecho por la UNAM, con estudios de Especialidad en el Reglamento General de Protección de Datos de la Unión Europea, actualmente labora como Directora de Gestión Documental en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ([www.inai.org.mx](http://www.inai.org.mx))



## RESUMEN

El presente artículo propone el uso de Blockchain en el proceso de valoración documental para facilitar la emisión de dictámenes para la baja o transferencia secundaria de registros públicos establecida en la Ley General de Archivos de México. Atribución que en el caso de los sujetos obligados recae en el Archivo General de la Nación y para el caso de las entidades federativas, en los Archivos Generales Locales. Esto permitiría que cada dictamen generado sería único, irrepetible e infalsificable, otorgaría certeza a las instituciones involucradas y haría transparente el proceso a la ciudadanía a fin de conocer los registros que serán eliminados o conservados en razón de los criterios (requisitos) previamente establecidos, lo cual daría credibilidad en las instituciones públicas en cuanto a la salvaguarda de los registros que les permitan una adecuada rendición de cuentas del ejercicio de las atribuciones que tienen conferidas, pero sobre todo en la conformación de la memoria histórica de México.

## PALABRAS CLAVE:

Blockchain, archivos, registros, valoración documental, dictamen de baja, transferencia secundaria.

## ABSTRACT

This article proposes the use of Blockchain for document assessment that ensures the issuance of opinions for the removal or secondary transfer of public records established by the Mexican General Archives Law. It argues that this would facilitate the role of the National Archive and those of the Local General Archives. Additionally, it would guarantee that each opinion generated would be unique, unrepeatable, and unfalsifiable, which in turn would grant certainty to the institutions involved, and open the process to public scrutiny, allowing general audiences to know the criteria under public records will be either eliminated or preserved. This in turn would strengthen the credibility of public institutions in terms of safeguarding the records that allow them to be adequately accounted for the exercise of the powers conferred on them, but above all, in shaping the historical memory of Mexico.

## KEYWORDS

Blockchain, files, records, documentary valuation, withdrawal opinion, secondary transfer.

## INTRODUCCIÓN

Los archivos gubernamentales son fuentes de información, toda vez que resultan fundamentales para garantizar derechos y libertades de las personas, para la continuidad de actividades y operaciones de las instituciones públicas, para la rendición de cuentas, generación de datos abiertos, entre otros, así como para conformar la memoria de las instituciones, la memoria nacional y el patrimonio cultural de la humanidad.

También tienen gran relevancia para la protección y promoción de los derechos humanos, es por ello que la Organización de las Naciones Unidas desde el año 1997 resaltaba la necesidad de preservar los archivos relacionados con violaciones a derechos humanos, para lo cual se deben contemplar medidas orientadas a impedir la sustracción, destrucción y desviación de los mismos, la creación de un inventario de los archivos disponibles, así como la reglamentación para su acceso y consulta a fin de garantizar el derecho a saber, a la verdad y a la memoria.<sup>1</sup>

Por su parte, el derecho a saber también encuentra vinculación con el derecho de acceso a la información, que encuentra su precedente en el artículo 11 de la Declaración de los derechos del hombre y del ciudadano de 1789, el cual establecía que todo ciudadano puede, hablar, escribir e imprimir libremente, salvo la responsabilidad que el abuso de esta libertad produzca en los casos determinados por la ley; y que sirvió de base para que en el año 1948, la Declaración Universal de los Derechos Humanos, en su artículo 19 señala que todo individuo tiene derecho a la libertad de opinión y de expresión, lo cual incluye el derecho a investigar y recibir informaciones y opiniones.

Para el año 1966, lo anterior se retoma en el Pacto Internacional de Derechos Civiles y Políticos, que en su artículo 19.2 establece que toda persona tiene derecho a la libertad de expresión, el cual comprende la libertad de buscar, recibir y difundir informaciones. Y en la Convención Americana sobre Derechos Humanos (Pacto de San José), que en el año 1969 estableció en su artículo 13.1 que toda persona tiene derecho a la libertad de pensamiento y expresión, lo cual comprendía la libertad de buscar, recibir y difundir informaciones y emitir opiniones de toda índole, por cualquier medio.

En el caso de México, la Constitución desde el año 1917 establecía el derecho a la libertad de expresión en su artículo 6º, el cual fue reformado en el año 1977 para adicionar que el derecho de acceso a la información sería garantizado por el Estado. En 2007 se reforma nuevamente dicho artículo para sentar la vinculación del derecho de acceso a la información con los archivos.

En 2011, la UNESCO adopta la Declaración Universal de los Archivos, creada por el Consejo Internacional de Archivos, la cual destaca que:

*[...] Los documentos son fuentes fiables de información que garantizan la seguridad y la transparencia de las actuaciones administrativas, juegan un papel esencial en el desarrollo de la sociedad contribuyendo a la constitución y salvaguarda de la memoria individual y colectiva. El libre acceso a los archivos enriquece nuestro conocimiento de la sociedad y promueve la democracia, protege los derechos de los ciudadanos y mejora la calidad de vida.<sup>2</sup>*

En razón de lo anterior, en el año 2014 se lleva a cabo otra reforma al artículo 6º. Constitucional en materia de transparencia, en la que se vinculan los archivos con la transparencia, el acceso a la información y la protección de datos personales, para lo cual se instruye al Congreso de la Unión la emisión de tres leyes generales en la materia, por lo que en fecha 15 de junio de 2018 se publica la Ley General

1 Cfr. COMISIÓN DE DERECHOS HUMANOS Subcomisión de Prevención de Discriminaciones y Protección a las Minorías; Informe final revisado acerca de la cuestión de la impunidad de los autores de violaciones de los derechos humanos (derechos civiles y políticos) preparado por el S. L. Joinet de conformidad con la resolución de 1996/119 de la Subcomisión. Disponible en el sitio web: <https://undocs.org/es/E/CN.4/Sub.2/1997/20/Rev.1> (Fecha de consulta, 8 de julio de 2020)

2 ICA-UNESCO, Declaración Universal sobre los Archivos, 2011. Disponible en el sitio web: [https://www.ica.org/sites/default/files/UDA\\_June2012\\_web\\_SP.pdf](https://www.ica.org/sites/default/files/UDA_June2012_web_SP.pdf) (Fecha de consulta, 10 de julio 2020).

de Archivos (LGA), que tiene por objeto establecer los principios y bases generales para la organización y conservación, administración y preservación homogénea de los archivos en el país, cuyo cumplimiento en materia de valoración documental puede verse favorecido con el uso de Blockchain a fin de garantizar la conformación de la memoria nacional.

## LA VALORACIÓN DOCUMENTAL

En principio considero pertinente explicar de manera general el significado de valoración documental, un breve acercamiento a su base teórica, así como su regulación en México. Es así que desde el punto de vista archivístico, la valoración documental se define como: *el proceso de determinar el valor de los documentos de archivo con el propósito de establecer su periodo de retención y disposición (destrucción o transferencia), así como los términos y condiciones de su transferencia desde el productor hacia el preservador (archivos).*<sup>3</sup>

La Norma ISO/TR 2146 IN<sup>4</sup> define la valoración documental como: *el proceso recurrente de evaluar las actividades de una organización para determinar qué documentos deben ser creados y capturados, y determinar cómo y cuánto tiempo deben mantenerse los documentos.* Por su parte, la LGA, la define como *la actividad que consiste en el análisis e identificación de los valores documentales; es decir, el estudio de la condición de los documentos que les confiere características específicas en los archivos de trámite o concentración, o evidenciales, testimoniales e informativos para los documentos históricos, con la finalidad de establecer criterios, vigencias documentales y, en su caso, plazos de conservación, así como para la disposición documental.*<sup>5</sup>

No obstante, cabe referir que el proceso de valoración documental, ha evolucionado desde el punto de vista teórico y metodológico a lo largo del tiempo, teniendo como punto de partida el nacimiento de la archivística como ciencia cuando se publicó el manual de los holandeses Muller, Feith y Fruin en el año de 1898, el cual refiere que la archivística evoluciona en tres fases: la “custodial” (hasta el S. XVIII) en la que se consideraba una disciplina auxiliar de la historia, la “técnica y custodial” (hasta la década de los 80 del S.XX), que adiciona un enfoque patrimonialista y la “científica y poscustodial” (actual), que concibe los archivos como sistemas de información.<sup>6</sup>

En las dos últimas etapas se formularon diversas definiciones de la valoración documental, en razón de que dicho proceso determina la información que será salvaguardada para la conformación de la memoria colectiva y social, por lo que se identifican dos tendencias de valoración a partir del siglo XX: una orientada a la conservación (alemana) y otra a la eliminación (inglesa).

Es así que, el inglés Hilary Jenkinson señalaba que la valoración para decidir qué documentos se eliminaban o mantenían, era responsabilidad exclusiva de los productores de la misma (*Manual of Archive Administration, 1922*), al atribuirle la característica de evidencia de actos y transacciones a los mismos, por lo que consideraba que la intervención de los archiveros podría menoscabar dicho carácter, reconociéndose sólo como custodios.<sup>7</sup>

3 Juan Voutssas M., Alicia Barnad Amozorrutia, Coordinadores; México, UNAM – Instituto de Investigaciones Bibliotecológicas y de la Información, Glosario de preservación archivístico digital versión 4.0; 2014. Disponible en el sitio web: [http://iibi.unam.mx/archivistica/glosario\\_preservacion\\_archivistica\\_digital\\_v4.0.pdf](http://iibi.unam.mx/archivistica/glosario_preservacion_archivistica_digital_v4.0.pdf) (Fecha de consulta, 10 de julio 2020).

4 PNE-ISO/TR 21946 IN. Información y documentación. Identificación y valoración para gestionar los documentos.

5 Ley General de Archivos, Artículo 4, fracción LIX; Diario Oficial de la Federación en fecha 15 de junio de 2018. Disponible en el sitio web: [http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA\\_150618.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA_150618.pdf) (Fecha de consulta, 1 de junio de 2020).

6 Montilla Peña, Leomar José y Mayra M. Mena Mujica. Estado de desarrollo de la archivística clásica hasta los años 30 del siglo XX: Tres manuales archivísticos de trascendencia universal. No 52 (2013), DOI 10.5195/biblios.2013.122. Disponible en el sitio web: <http://biblios.pitt.edu/> (Fecha de consulta, 10 de junio de 2020).

7 Schellenber, T.R. *Archivos modernos. Principios y técnicas* Traducción y adiciones por el Dr. Manuel Carrera Stampa, Ar-

Posterior a la segunda guerra mundial, con la explosión documental, se identifica la necesidad darle un giro a la valoración documental, por lo que Philip Brooks y Theodore Schellenber, desarrollan una propuesta orientada a otorgar valores a los documentos. Es así que Brooks propone tres criterios de valor: i) para la institución, ii) para la historia de la entidad administrativa productora, y iii) para la historia en general (*The Selection of record for preservation*) y Schellenber, define dos conjuntos de valores para los documentos, acordes al contenido y uso: valores primarios y valores secundarios (*Modern Archives: Principles and Techniques*), en la que los archiveros tenían participación.<sup>8</sup>

Schellenber plantea que los valores documentales constituyen categorías relacionadas con las funciones y usos de la información en las organizaciones, así como evidencias históricas y de investigación, que en conjunto con la *teoría de las tres edades de los documentos*, formulada por el archivista belga Charles Wiffells, que asocia los valores primarios a las primeras etapas (activa y semiactiva) y los valores secundarios a la fase histórica, permitieron conformar nuevas corrientes para la valoración documental.

Tal es el caso de Booms, quien plantea que la valoración debe atender una visión en conjunto, sistemática y planificada, lo cual influye en la postulación de la denominada *macrovaloración*, promovida por Richard Brown, según la cual es necesario analizar las interacciones entre la estructura (productores de documentos) y funciones, en el marco de su relación con la sociedad.<sup>9</sup>

Ramírez Deleón señala al respecto que desde un punto de vista teórico, la valoración surgió como respuesta a los problemas de acumulación y expansión de documentos, cuyo propósito central fue establecer criterios, métodos e instrumentos que coadyuvan a la mejor administración de los documentos resultantes de los procesos de gestión de las organizaciones, así como a la construcción de su patrimonio histórico documental. Por lo que desde el punto de vista teórico, requiere un conocimiento profundo de la entidad productora de los documentos, su marco jurídico, reglamentación interna, políticas y programas, manuales, entre otros, en los que sustenta sus actividades.

En adición a lo anterior, refiere que el concepto de valoración como función archivística se traduce en la ejecución de un proceso con tres tipos de acciones:

- “1) acciones destinadas al diseño y construcción de los criterios, regulaciones e instrumentos de la valoración (actividad intelectual);
- 2) acciones destinadas a la generación de políticas, reglas e instrucciones para normar el proceso de valoración (actividad normativa);
- 3) acciones destinadas al uso y aplicación de las políticas y regulaciones asociadas a la valoración en los archivos, que se materializan en instrumentos previamente diseñados, tales como el catálogo de disposición documental, los inventarios de transferencia, las cédulas de disposición, el calendario de caducidades, etcétera, que deberán mantenerse permanentemente actualizados (actividad instrumental)”.<sup>10</sup>

El desarrollo de la sociedad de la información y el uso de las TICs, trae nuevos retos a la valoración documental en cuanto a que los documentos, además de ser evidencia, deben ser auténticos, lo que ha llevado a que los archivistas tienen un papel más activo para involucrarse en el diseño y creación de sistemas automatizados de gestión documental también garanticen la disponibilidad de los mismos a largo plazo.

En el caso de México, la valoración documental se realizaba inicialmente sólo por los titulares de las unidades administrativas productoras y los responsables de los archivos de trámite a través de las

chivo Nacional, La Habana, 1958. Pág. 199.

8 Ibid. Pág. 197-202.

9 Ramírez Deleón, José Antonio. *Metodología para la valoración y disposición documental: aspectos teóricos y metodológicos*. Cuadernos de la serie Gestión de Documentos y Administración de Archivos. IFAI-AGN. México, 2011. P. 23-25

10 Ramírez Deleón, José Antonio. *Metodología para la valoración y disposición documental: aspectos teóricos e instrumentales*, IFAI-AGN, México, 2011. Pág. 32 y 33

fichas de valoración documental, en coordinación con el Responsable del Área Coordinadora de Archivos y del entonces Comité de Enlace (hoy Comité de Transparencia).

Con miras a reforzar el proceso de valoración documental, a partir del interés público en la documentación a ser valorada, los costos de su conservación tanto en soportes físicos como digitales, así como la relevancia de la misma para la rendición de cuentas, entre otros, en el año 2016 el Consejo Nacional del Sistema Nacional de Transparencia emitió los *Lineamientos para la organización y conservación de los archivos*, en los que se adiciona la obligación de establecer un Grupo Interdisciplinario, integrado por los titulares del área coordinadora de archivos, de la unidad de transparencia, área de planeación estratégica, jurídica, mejora continua, órganos internos de control o sus equivalentes, las áreas responsables de la información y el responsable del Archivo Histórico, lo cual se retoma en la LGA publicada en el año 2018.

Dicho grupo interdisciplinario coadyuvará en el análisis de los procesos y procedimientos institucionales que dan origen a la documentación de los sujetos obligados, a fin de colaborar con las áreas o unidades administrativas productoras para establecer los valores documentales, vigencias, plazos de conservación y disposición documental durante el proceso de elaboración de las fichas técnicas de valoración, de las series documentales que integrarán el Catálogo de Disposición Documental, el cual será validado por el Archivo General de la Nación para aquellos sujetos obligados de la Administración Pública Federal y por los archivos generales locales para el caso de las entidades federativas.

Es así, que la valoración que inicialmente realizarán los titulares de las unidades administrativas productoras de la información y los responsables de los archivos de trámite, en coadyuvancia con el Grupo Interdisciplinario de Valoración Documental, a través de las fichas de valoración documental que conformarán el Catálogo de Disposición Documental del sujeto obligado, serán una herramienta fundamental para que se cumplan los plazos de conservación de los documentos en el archivo de trámite y concentración, dónde su acceso a la ciudadanía deberá atender lo establecido en la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)<sup>11</sup>, la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPO)<sup>12</sup> y demás normatividad aplicable; así como que de conformidad con lo establecido en el artículo 36 de la LGA, una vez que se encuentren en un archivo histórico, serán una fuente de acceso público.

Otro punto de vital importancia, será la emisión del dictamen de baja documental o de transferencia secundaria que para el caso de los sujetos obligados del Poder Ejecutivo Federal, recaerá en el Archivo General de la Nación y en los Archivos Generales Locales para las entidades federativas. No obstante, en el resto de los sujetos obligados, dicha responsabilidad recaerá en las instancias que el propio sujeto obligado determine, por ejemplo en el caso del Instituto Nacional Electoral se cuenta con el Comité Técnico para la Administración de Documentos (COTECIAD), es quien emite dicho dictamen<sup>13</sup> y en el caso del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, corresponde a su Comité de Valoración Documental.<sup>14</sup>

11 Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación en fecha 4 de mayo de 2015. Disponible en el sitio web: [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5391143&fecha=04/05/2015](https://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015) (Fecha de consulta, 10 de junio de 2020).

12 Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, publicada en el Diario Oficial de la Federación en fecha 26 de enero de 2017. Disponible para su consulta en: [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5469949&fecha=26/01/2017](https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017) (Fecha de consulta, 10 de junio de 2020).

13 El artículo 44 numeral 5 del Reglamento del Instituto Nacional Electoral en Materia de Transparencia y Acceso a la Información Pública, establece que el COTECIAD será el encargado de vigilar la instrumentación, en las diversas áreas del Instituto, de la aplicación de los programas, lineamientos, manuales y políticas que apruebe el Comité en materia de archivos, así como determinar el destino final de los documentos que por su particularidad así lo requieran. Disponible en el sitio web: <https://www.ine.mx/compendio-normativo/> (Fecha de consulta, 30 de junio de 2020).

14 El artículo 4 fracción IV del Reglamento de operación del Comité de Valoración Documental del INAI, establece que dicho Comité tiene entre sus atribuciones la de emitir un dictamen de baja documental o de transferencia secundaria de los documentos de archivo con valor histórico generados por el Instituto. Disponible en el sitio web:

En razón de lo anterior y considerando que el Archivo General de la Nación no tienen entre sus atribuciones emitir los dictámenes de baja documental ni transferencia secundaria para aquellos sujetos obligados que no forman parte del Poder Ejecutivo Federal, lo cual se replica en los Archivos Generales Locales para las entidades federativas, *Blockchain* podría ser una herramienta útil para generar confianza en la ciudadanía en cuanto a la documentación que será conservada por tener un valor histórico, como aquella que será eliminada de manera permanente, tal como se explicará más adelante.

## LA TECNOLOGÍA BLOCKCHAIN

Cuando escuchamos el término *Blockchain* en inmediato pensamos en *Bitcoin*, que tiene su origen en el documento publicado en el año 2008 por Satoshi Nakamoto<sup>15</sup>, a través del cual plantea una propuesta de creación de una red para transacciones electrónicas de usuario a usuario sin necesidad de que una institución financiera sea intermediaria para garantizar la autenticidad de las mismas. Pero los antecedentes de *Blockchain* se remontan a los años noventa con Stuart Haber y W. Scott Stornetta<sup>16</sup>, a través de su publicación “*How To Time-Stamp a Digital Document*”, en el que proponían un sellado de tiempo para garantizar la integridad de documentos de texto, audio, imagen o video en formato digital.

No obstante, toda vez que *Bitcoin* se encontraba orientada para transacciones monetarias, para el año 2014, la plataforma *Ethereum*, implementa una *Blockchain* con los fundamentos de *Bitcoin* planteados por Nakamoto, pero que adiciona los “contratos inteligentes” (*Smart contract*), los cuales permiten alojar condiciones pre-programadas en las que no interviene la valoración humana.

Si bien es cierto el uso de *Blockchain* ha tenido mayor relevancia para el uso y funcionamiento de criptomonedas por la popularidad de *Bitcoin*, también lo es que se están explorando nuevas aplicaciones para dicha tecnología, en razón de que ha cambiado la forma en que se crea y procesa información a través de la misma, tales como las cadenas de suministro de bienes, registro de tierras o garantizar la integridad de los registros gubernamentales y servicios.<sup>17</sup>

El Banco Interamericano de Desarrollo ha señalado que otra de las aplicaciones de *Blockchain* es el registro de documentos de forma descentralizada, al ser un *registro de información distribuido tipo P2P (Peer-to-Peer) en donde los diferentes participantes no tienen por qué confiar los unos en los otros, puesto que hay un protocolo de consenso que garantiza la seguridad y la veracidad de las transacciones; sumado a la inmutabilidad de la cadena que imposibilita editar o borrar información, así como la identificación de cada uno de los bloques a través de un código alfanumérico denominado hash y la firma electrónica de validación.*<sup>18</sup>

La arquitectura de *Blockchain* se encuentra basada en bloques, que contienen datos (información) y un *hash*, el cual garantiza la autenticidad de la información del mismo, por lo que no puede ser replicado y de ser el caso, emitirá una advertencia al resto de los bloques. A través de cada uno de estos bloques, se puede llevar a cabo una transacción (información) que contiene un remitente, receptor y

---

<http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-04-12-2019.06.pdf> (Fecha de consulta, 30 de junio de 2020).

15 NAKAMOTO, SATOSHI, “Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario”. Disponible en el sitio web: [https://bitcoin.org/files/bitcoin-paper/bitcoin\\_es\\_latam.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf) (Fecha de consulta 25 de mayo de 2020)

16 HABER, S., STORNETTA, W.S. “How to time-stamp a digital document”. *J. Cryptology* 3, 99–111 (1991). Disponible en el sitio web: <https://doi.org/10.1007/BF00196791> (Fecha de consulta 25 de mayo de 2020).

17 Government Office for Science, *Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser*, London, 2016.

18 Allende López, Marcos. *Blockchain. Cómo desarrollar confianza en entornos complejos para generar valor de impacto social*. Banco Interamericano de Desarrollo, 2018. Diponible en el sitio web: <https://publications.iadb.org/es/blockchain-como-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social> (Fecha d consulta, 10 de julio de 2020).

valor, que se actualizará en todos los nodos que forman parte de la cadena de bloques. Finalmente, debe existir un consenso, a través del cual se establecerán las reglas que atenderán los nodos participantes de la red.

Existen tres tipos de arquitectura de *Blockchain*: pública, privada y federada, ésta última surge a partir de la necesidad de contar con registros descentralizados que generen confianza entre diferentes entidades, para lo cual existe un administrador de la red, que brinda acceso a cada uno de los nodos que participan a través de una interfaz *web*, permite establecer las reglas de consenso y garantiza una eficiencia alta.

Uno de los ejemplos del uso de blockchain que podría tomarse como referente para la propuesta del presente artículo es la Organización Autónoma Descentralizada (DAO por sus siglas en inglés), que pretende resolver el problema de gobernanza a través de una plataforma disponible y reglas comerciales éticas. Lo cual se realiza a través de automatización de contratos inteligentes que mejoren la gobernanza otorgando los mismos derechos y oportunidades a cada una de las partes interesadas, eliminando la mala gestión y la burocracia.<sup>19</sup>

## EL USO DE BLOCKCHAIN PARA LA VALORACIÓN DOCUMENTAL EN MÉXICO

En el entendido de que *Blockchain* es una herramienta que facilita la transparencia a través de redes privadas y federadas, que permiten el acceso vía *web* para los usuarios que formen parte de la cadena de bloques, así como la descentralización de la información a través de nodos a los que se les pueden asignar roles en base a las reglas previamente establecidas y garantiza la inmutabilidad de la información que cada uno de los bloques contenga, se considera una alternativa para la valoración documental que permita la elaboración de los dictámenes de baja documental y transferencia secundaria que no serán emitidos por el Archivo General de la Nación ni por los Archivos Generales Locales, lo cual otorgaría certeza a la ciudadanía, sobre todo en razón de la documentación que pretenda eliminarse.

Lo anterior, también abonará a las actividades encomendadas al Archivo General de la Nación, que si bien no tiene atribuciones para emitir los dictámenes antes mencionados, es la entidad especializada en materia de archivos a nivel nacional, que tienen por objeto salvaguardar la memoria nacional de corto, mediano y largo plazo, así como contribuir a la transparencia y la rendición de cuentas del Estado mexicano. Para lo cual, podría generarse una red a través de *Blockchain* que administrara el propio AGN, a fin de que pudiera habilitar los nodos de cada uno de los sujetos obligados no forman parte de Poder Ejecutivo Federal.

Adicionalmente, se podrían establecer las reglas para que las instancias correspondientes de dichos sujetos obligados puedan emitir dichos dictámenes de manera homogénea a través de lo que se pretende regular en los Lineamientos para que el Archivo General de la Nación emita el dictamen de baja documental o de transferencia secundaria para los sujetos obligados del Poder Ejecutivo Federal, que permitiría efficientar y transparentar el procedimiento de dictaminación de bajas documentales, al quedar registrados en la cadena de bloques para rendir exigir responsabilidades sobre las decisiones que al respecto se tomen tanto quienes tienen la facultad de llevar a cabo la valoración documental como quienes toman la decisión final.

La cadena de bloques podría dar cuenta de las transacciones (información) que se genere durante el proceso, vinculado al sistema automatizado para la gestión documental y administración de los archivos, que los sujetos obligados deberán implementar en cumplimiento al artículo 44 de la LGA, para lo cual se podría utilizar la metodología sugerida por el Banco Interamericano de Desarrollo en su do-

---

19 Rodríguez, Nelson. Uso de Blockchain: lista de 20+ casos de uso de la tecnología Blockchain. Julio 23 de 2019. Disponible en el sitio web: <https://101blockchains.com/es/uso-de-blockchain/> (Fecha de consulta, 10 de julio de 2020).

cumento denominado *Blockchain*. *Cómo desarrollar confianza en entornos complejos para generar valora de impacto social*, para lo cual sería necesario definir los participantes: unidades administrativas productoras de la información, integrantes del Grupo Interdisciplinario, instancia del sujeto obligados que tenga la atribución de emitir los dictámenes de baja documental y transferencia secundaria, Archivo General de la Nación y Archivos Generales Locales, y de ser el caso, alguna comunidad académica, investigadores o asociaciones civiles interesadas.

Por otra parte, si bien al día de hoy está pendiente la emisión del marco normativo secundario por parte del Consejo Nacional de Archivos, que aporte mayor claridad a la función de la dictaminación de baja documental o transferencia secundaria, así como a la valoración que llevarán a cabo los sujetos obligados, existen normas técnicas que podrían servir de apoyo avanzar en las reglas de operación entre los participantes de la cadena de bloques, es el caso de la norma ISO 21946<sup>20</sup>, que entre otros, explica cómo identificar los requisitos de los registros, las relaciones entre estos requisitos, las funciones y procesos de trabajo de las instituciones, así como la evaluación de riesgos para la toma de decisiones relacionadas con los registros y cómo documentar los resultados de la valoración.

Es por ello, que se propone el uso de *Blockchain* tanto para la emisión de los dictámenes de baja documental o transferencia secundaria de documentación a los archivos históricos en el que todos los involucrados pudieran formar parte a fin de otorgar confianza y seguridad tanto para las instituciones como para la sociedad en general de aquella información, con independencia de su soporte que sea valorada para eliminación o para conservación permanente y sirvan de evidencia en caso de auditoría, así como para dar certeza a la sociedad en cuanto a la salvaguarda de la información que formará parte de la memoria nacional y del mundo.

Lo cual encuentra sustento en la cadena de bloques que forma parte de *Blockchain*, la cual puede contener cualquier tipo información, tales como el formato de los dictámenes antes referidos, que además una vez validado puede encriptarse a través de un código único e irrepetible (*hash*), para enlazarse con el bloque previo y posterior. Dicha cadena de bloques podría ser pública no sólo entre los actores sino también para la sociedad en un ejercicio de transparencia que no dé lugar a la eliminación de información a discreción, ya que si en alguno de los bloques se pretendiera eliminar o modificar información, el “*hash*” resultante sería distinto y al original que ya fue replicado por otros nodos por lo que cualquier alteración podría identificarse.

## CONCLUSIONES

El uso de esta tecnología podría otorgar seguridad a la función de dictaminar por parte del Archivo General de la Nación y los Archivos Generales Locales, garantiza la integridad y disponibilidad de dichos dictámenes, podría involucrar a organizaciones de la sociedad civil, especialistas en los diversos sectores (comunicaciones, salud, economía, etc.), e investigadores, entre otros. Lo cual, en un momento como el que nos estamos viviendo actualmente puede ser de vital importancia a fin de salvaguardar los registros que se están generando en torno a la pandemia y que sin duda, podrían formar parte de alguna violación grave de derechos humanos, relacionados con el incremento de la violencia contra las mujeres, niñas y niños<sup>21</sup>, el derecho a la salud para las personas privadas de su libertad o en situación de desplazamiento forzado, migrantes y refugiados, las comunidades indígenas y afro americana; para la transparencia y rendición de cuentas que será necesaria en razón de los recursos que están siendo utilizados para hacer frente a la pandemia, entre otros.

20 ISO/TR 21946:2018. *Information and documentation. Appraisal for managing records*.

21 ONU Mujeres, El impacto del COVID19 en la violencia contra las mujeres y las niñas y la necesidad de actuar, Disponible en el sitio web: <https://mexico.unwomen.org/es/noticias-y-eventos/articulos/2020/05/comunicado-mcig> (Fecha de consulta 10 julio 2020).

**REFERENCIAS BIBLIOGRAFICAS:**

- Allende López, Marcos. *Blockchain. Cómo desarrollar confianza en entornos complejos para generar valor de impacto social*. Banco Interamericano de Desarrollo, 2018. Disponible en el sitio web: <https://publications.iadb.org/es/blockchain-como-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social> (Fecha de consulta, 10 de julio de 2020).
- HABER, S., STORNETTA, W.S. “How to time-stamp a digital document”. *J. Cryptology* 3, 99–111 (1991). Disponible en el sitio web: <https://doi.org/10.1007/BF00196791> (Fecha de consulta 25 de mayo de 2020).
- Montilla Peña, Leomar José y Mayra M. Mena Mujica. Estado de desarrollo de la archivística clásica hasta los años 30 del siglo XX: Tres manuales archivísticos de trascendencia universal. No 52 (2013), DOI 10.5195/biblios.2013.122. Disponible en el sitio web: <http://biblios.pitt.edu/> (Fecha de consulta, 10 de junio de 2020).
- NAKAMOTO, SATOSHI, “Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario”. Disponible en el sitio web: [https://bitcoin.org/files/bitcoin-paper/bitcoin\\_es\\_latam.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf) (Fecha de consulta 25 de mayo de 2020)
- Ramírez Deleón, José Antonio. *Metodología para la valoración y disposición documental: aspectos teóricos y metodológicos*. Cuadernos de la serie Gestión de Documentos y Administración de Archivos. IFAI-AGN. México, 2011.
- Rodríguez, Nelson. Uso de Blockchain: lista de 20+ casos de uso de la tecnología Blockchain. Julio 23 de 2019. Disponible en el sitio web: <https://101blockchains.com/es/uso-de-blockchain/> (Fecha de consulta, 10 de julio de 2020).
- Schellenber, T.R. *Archivos modernos. Principios y técnicas* Traducción y adiciones por el Dr. Manuel Carrera Stampa, Archivo Nacional, La Habana, 1958.
- COMISIÓN DE DERECHOS HUMANOS Subcomisión de Prevención de Discriminaciones y Protección a las Minorías; Informe final revisado acerca de la cuestión de la impunidad de los autores de violaciones de los derechos humanos (derechos civiles y políticos) preparado por el S. L. Joinet de conformidad con la resolución de 1996/119 de la Subcomisión. Disponible en el sitio web: <https://undocs.org/es/E/CN.4/Sub.2/1997/20/Rev.1> (Fecha de consulta, 8 de julio de 2020)
- Government Office for Science, *Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser*, London, 2016.
- ICA-UNESCO, Declaración Universal sobre los Archivos, 2011. Disponible en el sitio web: [https://www.ica.org/sites/default/files/UDA\\_June2012\\_web\\_SP.pdf](https://www.ica.org/sites/default/files/UDA_June2012_web_SP.pdf) (Fecha de consulta, 10 de julio 2020).
- Juan Voutssas M., Alicia Barnad Amozorrutia, Coordinadores; México, UNAM – Instituto de Investigaciones Bibliotecológicas y de la Información, Glosario de preservación archivística digital versión 4.0; 2014. Disponible en el sitio web: [http://iibi.unam.mx/archivistica/glosario\\_preservacion\\_archivistica\\_digital\\_v4.0.pdf](http://iibi.unam.mx/archivistica/glosario_preservacion_archivistica_digital_v4.0.pdf) (Fecha de consulta, 10 de julio 2020).
- Ley General de Archivos, Artículo 4, fracción LIX; Diario Oficial de la Federación en fecha 15 de junio de 2018. Disponible en el sitio web: [http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA\\_150618.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA_150618.pdf) (Fecha de consulta, 1 de junio de 2020).

- Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación en fecha 4 de mayo de 2015. Disponible en el sitio web: [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5391143&fecha=04/05/2015](https://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015) (Fecha de consulta, 10 de junio de 2020).
- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, publicada en el Diario Oficial de la Federación en fecha 26 de enero de 2017. Disponible para su consulta en: [https://www.dof.gob.mx/nota\\_detalle.php?codigo=5469949&fecha=26/01/2017](https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017) (Fecha de consulta, 10 de junio de 2020).
- ONU Mujeres, El impacto del COVID19 en la violencia contra las mujeres y las niñas y la necesidad de actuar, Disponible en el sitio web: <https://mexico.unwomen.org/es/noticias-y-eventos/articulos/2020/05/comunicado-mcig> (Fecha de consulta 10 julio 2020).
- PNE-ISO/TR 21946 IN. Información y documentación. Identificación y valoración para gestionar los documentos.

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).  
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.  
ISSN 2530-4496 – AÑO 1, N° 8, 2020, PÁGS. 83-90

**BLOCKCHAIN: TEORÍA Y PRÁCTICA. APLICACIONES LEGALES Y TÉCNICAS.  
LOS CASOS DE COLOMBIA Y REPUBLICA DOMINICANA**

BLOCKCHAIN: THEORY AND PRACTICE. LEGAL AND TECHNICAL APPLICATIONS.  
THE CASES OF COLOMBIA AND THE DOMINICAN REPUBLIC

**Manfry Rafael Sierra Alemán**  
**Félix Juan Rivera Aquino**  
**Alexis German Antonucci L.C.**

PRIMEROS EN FIADI<sup>1</sup>.

1 Manfry Rafael es Graduado en Derecho por la Universidad del Magdalena, Santa Marta, Colombia.  
Félix Juan es Graduado de Derecho por la Universidad O&M y Máster en Administración de Justicia Constitucional.  
Santo Domingo, República Dominicana.  
Alexis German hizo la Coordinación y es el Director de Primeros en FIADI.



## INTRODUCCION

En la teoría esta tecnología hace referencia a una estructura en donde determinada información se agrupa en bloques los que contienen y añaden meta información contenida en otros bloques de la misma, siempre siendo anteriores en una línea temporal. Esto permite que se pueda utilizar para crear bases de datos en donde cada modificación y cambio sea registrado de forma irrefutable por los demás segmentos de la cadena. Basta decir que la cadena de bloques no necesita de una institución central para que certifique o valide lo que hace

En la práctica con la ayuda de la criptografía asimétrica da lugar a que se puedan dar registros contables y permitir la seguridad del dinero digital. Esto se debe a que los propios miembros hacen a la confianza y seguridad de la tecnología.

Si internet trajo consigo intercambio de información de forma ágil, esta tecnología implicará una forma de intercambiar valor entre negocios, instituciones y particulares.

## CASO COLOMBIA

Últimamente el termino Blockchain anda en boga, muchos hablan de ella, debido a su uso y desarrollo que cada día se generaliza y expande de poco a poco. En términos simples, la tecnología (trabaja en cadena de bloques) consiste en una base de datos descentralizada que almacena un registro – contabilidad digital- de activos y transacciones a través de una red peer-to-peer (entre pares). Es decir, es un registro público en el cual se consigna quién posee qué y quién tramita qué<sup>1</sup>.

Las bondades de estas tecnologías se pueden usar en muchos campos y cada día esa lista se vuelve, desde las criptomonedas hasta los contratos inteligentes, pasando por el campo de los seguros, aplicaciones militares, propiedades intelectuales, notariados, contratos inteligentes, etc, entonces hay que entender que va mucho más allá de la criptodivisas. sin embargo, se hará énfasis teniendo hoy por hoy una mayor visibilidad el ámbito de las divisas, donde se les denomina (criptodivisas o criptomonedas), siendo tanto Bitcoin su punta de lanza o Ethereum, al bum de las criptodivisas se le conoce la primera ola de la tecnología blockchain.

De la misma forma que en otras latitudes del mundo de poco a poco el uso de las criptodivisas sigue tomando fuerza por parte de la sociedad en general, en Colombia no es diferente, aunque ese avance hoy por hoy contrasta con su marco legal. Muchos actores vienen haciendo su aparición. La creación de Blockchain Colombia es un reflejo de esto, esta asociación, fruto de la unión de empresas como buda Colombia, bitcoin Colombia, cajero.co, IntiColombia, panda group, y rsk y es que se han propuesto promover el uso y la aplicación de esta tecnología encaminada a soluciones descentralizadas, combatir la corrupción y otras aplicaciones en el sector público “Es muy importante que Colombia se incluya rápido (en la tecnología Blockchain) para aprovechar las oportunidades (...).

Se necesitan «tecnologías que obliguen a los bancos a una mejor auto regulación”, La fundación (IntiColombia) quiere ser un actor que articule todo el sistema y que encuentre las soluciones para adoptar esta tecnología, dijo a periodistas el codirector de IntiColombia, Mauricio Tovar, donde hizo mención que el sistema financiero del país es abusivo, con tasas altas y costos que no debería cobrarse. (Agencia EFE, 2018). Siguiendo la misma línea Tovar manifestó en dicho evento que el sistema financiero del país es abusivo con los colombianos. Algo que no es lejano de la realidad, un ejemplo de esto es que la Superintendencia Financiera (superfinanciera) emitió en una circular externa en el 2016 donde evidenció 54 prácticas y 54 cláusulas abusivas productos de la revisión de contratos que firmaron los clientes y del desarrollo de las relaciones entre los consumidores financieros y las entidades vigiladas. (www.superfinanciera.gov.co, 2016)

---

1 (Torres Varela, 2020 pág. 40).

Siguiendo la misma línea otras empresas colombianas siguen aportando a que esta tecnología siga masificándose, con el anuncio hecho por Facebook de querer poner en marcha su criptomoneda “libra”, Llama la atención que solo dos compañías latinoamericanas sean socias de este colectivo: Mercado Libre, a través de su ‘fintech’ Mercado Pago y PayU, de origen colombiano.<sup>2</sup>

Es cierto que es una tecnología en crecimiento y desarrollo de allí su uso tímido por parte de diferentes actores y de la sociedad ya sea en el ámbito privado o público debido al reconocimiento generalizado de la gran mayoría de la sociedad y por falta de un marco normativo que respalde y brinde tranquilidad.

Sin embargo se está dando pasos significativos en pro de aplicar y usar Blockchain, en el 2019 se realizó el primer piloto, donde 1500 estudiantes del colegio el Rodeo en la ciudad de Bogotá para la elección de personeros de esas instituciones.

El marco regulatorio es escaso a superar, Colombia sigue en busca de un marco regulatorio que vaya acorde a los beneficios y oportunidades que trae la tecnología Blockchain. Como antecedentes se encuentra que en el 2014 la Superintendencia Financiera, por medio de la circular 29<sup>3</sup>, en el 2016 el Banco de la Republica de Colombia en un el concepto N° 20348<sup>4</sup>. En el año 2018 se radicó ante el congreso de la Republica de Colombia el proyecto de ley 028, con el objetivo de regular las criptomonedas sus transacciones, vigilancia, inspección y control de dichas operaciones en el territorio nacional. actualmente el proyecto se encuentra estancado y no ha sido aprobado).

Por ejemplo, en el uso de contratos inteligentes tampoco existe actualmente una regulación específica como tal, debido al principio de Neutralidad Tecnológica establecido en la ley 1341 del 2009 se encuentra permitido, se entiende que estas no tienen un estatus de contrato como tal, sino de herramienta tecnológica.

## CASO REPÚBLICA DOMINICANA

La cadena de bloques, mejor conocido como *blockchain*, es la tecnología detrás de las criptomonedas como lo son *bitcoin* o *ethereum*. A través de esta tecnología todas las transacciones financieras son registradas y compartidas públicamente haciendo dichas transacciones seguras sin la necesidad de un tercero que valide la operación, es decir, se establece un conjunto de reglas que aseguran la integridad de la transacción a través de la intervención de distintos sujetos, sin que ninguno de ellos pueda calificar como una tercera parte de confianza<sup>5</sup>.

El potencial de esto va mucho más allá de las monedas, como ya hemos dicho, su tecnología permite asegurar la integridad de la información pudiendo ser aplicada, por ejemplo, en la construcción de un proyecto de identidad digital que pueda contrastar o unificar nuestra identidad *offline* con la *online* recopilando nombre, domicilio, edad, etc.

En la práctica, en la República Dominicana, la tecnología de *blockchain* a pesar de sus bondades, no ha contado por parte del sector público o privado con el impulso necesario para poder desarrollar dicha tecnología mas allá de las criptomonedas.

Sin embargo, recientemente se realizó un *hackathon*<sup>6</sup> patrocinado por Blockchain Academy Dominicana en donde reunieron talentos del sector tecnológico, para competir en retos reales y desarrollar sobre la base de *blockchain*, tecnología escalable y con un gran potencial comercial en todos los sectores de la sociedad.

2 La empresa colombiana que hace parte de la criptomoneda de Facebook, 2019

3 No se encuentran reguladas por la ley colombiana ni sujetas a control.

4 El único medio de pago de curso legal en el país es el peso colombiano.

5 RICO CARRILLO, M., “Blockchain, Bitcoin y Monedas Virtuales: el cambio de Paradigma en los Sistemas de Pago Electrónico”, Memorias del XXII Congreso Iberoamericano de Derecho e Informática, 2008, pág. 430

6 Una *hackathon* o *hackatón*, es un término usado en las comunidades hacker para referirse a un encuentro de programadores cuyo objetivo es el desarrollo colaborativo de software, aunque en ocasiones puede haber también un componente de hardware. Estos eventos pueden durar entre dos días y una semana.

Por su parte, las criptomonedas han empezado a ofrecer una opción diferente de la moneda fiduciaria en algunos aspectos como hoy la conocemos. Empresas locales como BitRD o BitcoinRD ofrecen servicios de compra y venta de criptomonedas con una red de cajeros a nivel nacional donde se puede realizar dichas operaciones con rapidez y seguridad.

## SITUACIÓN LEGAL

La República Dominicana no cuenta con una regulación especializada dentro de su marco jurídico sobre *blockchain* o criptomonedas donde se establezcan las reglas adecuadas o las pautas necesarias para el uso de estos activos virtuales. Sin embargo, el uso de las criptomonedas o de *blockchain* no está prohibido en el país, lo que indica que son activos no regulados; de tal suerte que, quedan excluidas de todas las garantías estatales por no ser reconocida como moneda de curso legal.

El Banco Central dominicano en fecha 22 de junio de 2017 emitió una resolución donde advertía a las entidades de intermediación financiera (EIF), a los agentes de remesas y cambio, a las entidades del mercado de valores, a las entidades del mercado de seguros, a los sectores económicos y al público en general que el uso de activos virtuales tales como *Bitcoin*, *Litecoin* y *Ethereum* conlleva un riesgo por no contar con el respaldo del Banco Central y por lo tanto no gozan de la protección legal que otorga el marco jurídico de la República Dominicana<sup>7</sup> a consecuencia de ello no reciben las garantías ni seguridad que ofrece la intermediación cambiaria ni la libre convertibilidad, consagradas en los artículos 28 y 29 de la Ley Monetaria y Financiera<sup>8</sup>.

En ese mismo sentido, el comunicado emitido por el Banco Central dominicano deja bien claro que las criptomonedas no son consideradas como una moneda de curso legal, por lo que no gozan del respaldo ni las garantías ofrecidas por el Estado.

Por otra parte, Dominicanos en Wall Street (Dominicans on Wall Street o DOWS), es una organización sin fines de lucro que busca promover el desarrollo de los mercados capitales y la bolsa de valores en la República Dominicana, organizó un panel titulado “*Blockchain* y Criptomonedas 101: Su impacto en los mercados de Estados Unidos y la República Dominicana”, en donde explicó que es *blockchain* y que su uso va mucho más allá de *bitcoin*.

Según se ha visto, en el debate constructivo en dicho panel, la Subgerente de Sistemas e Innovación Tecnológica del Banco Central de la República Dominicana declaró que los bancos centrales no pueden permitir la existencia de dos sistemas económicos paralelos<sup>9</sup>, en el sentido de que se tenga la necesidad de tener un sistema económico centralizado no para el control, sino para el crecimiento económico en su conjunto<sup>10</sup>, a pesar de ellos, no descarto que en un futuro el Banco Central dominicano emita una criptomoneda patrocinada por el Estado.

No obstante a la postura del Banco Central dominicano frente a las estas, más de cinco mil personas transan con estas en el país, de acuerdo con Guillermo García, experto en derecho bancario y dinero electrónico a través de ellas resulta muy fácil esconder dinero proveniente de actividades ilícitas<sup>11</sup>, lo que se traduce a que, la falta de regulación en este sector, se hace difícil, por partes de las autoridades,

7 Banco Central República Dominicana, Documento -COMUNICADO-, y “disponible en el sitio web: <https://cdn.bancentral.gov.do/documents/avisos/documents/aviso20170628.pdf> (11 de junio de 2020)

8 Idem

9 Blog de COINSUPER (Oficial), Documento - Exploring Different Perspectives on Blockchain and Cryptocurrencies -, y “disponible en el sitio web: <https://medium.com/@coinsuper/exploring-different-perspectives-on-blockchain-and-cryptocurrencies-cb55e431fdd3> (11 de junio de 2020)

10 Idem

11 INVERTIX, Documento - Más de 5,000 personas transan con criptomonedas en República Dominicana-, y “disponible en el sitio web: <https://invertix.com.do/mas-de-5000-personas-transan-con-criptomonedas-en-republica-dominicana> (13 de junio de 2019)

evitar delitos como lavado de activos o el financiamiento de actividades ilícitas. Además, que la no regulación de la moneda dificulta la labor de los controles establecidos para evitar o impedir que el dinero lavado circule dentro del sistema financiero.

## CONCLUSIÓN

A partir de la llegada de las criptomonedas a la República Dominicana, hemos visto como ha causado una disrupción en el sistema financiero, desde la instalación de un sistema de cajeros donde se puede intercambiar dinero metálico por activos virtuales como *bitcoin* o *ethereum* hasta la creación de un *hackaton* con el objetivo de entregar una solución tecnológica teniendo como premisas la seguridad y escalabilidad.

La regulación al ser incompatibles con estas tecnologías por ser descentralizadas, les plantea un reto a las instituciones de cómo hacer la intermediación financiera o la regulación en el futuro.

Dadas las condiciones que anteceden, el Banco Central dominicano debe empezar a explorar la tecnología de *blockchain*, en última instancia las criptomonedas, las oportunidades que ofrece son impresionantes para una futura autorregulación, para aumentar los niveles de transparencia estatal y para la supervisión y prevención de blanqueos de capitales dentro del sistema financiero.

Se habla desde su aparición por allá en el 2008 con la irrupción de *bitcoin*. Como tecnología disruptiva no cabe duda que traerá avances importantes en cambios y nuevas formas de interactuar entre los individuos de la sociedad y que falta aún por ver más y más sus bondades, ya esto se comienza a palpar en diferentes latitudes del mundo. Los fundamentos de esta tecnología (descentralización, inmutabilidad, transparencia) nos invita a soñar para transformar nuestro entorno y como nos relacionamos entre sí.

Hay varios puntos claves para que esto siga despuntando, para apropiarnos como corresponde debemos desaprender para volver aprender, quitar nos el miedo a innovar o por lo menos a intentar, los beneficios han venido por esta vía, otro aspecto importante radica en una falta de voluntad política por parte del legislador, en Colombia por ejemplo se está en fases de proyectos de ley como ya se mencionó, pero preocupa su nulo avance, y esta falta de normativa genera por una parte confusión y otra desconfianza por falta de respaldo legal y como un círculo vicioso esto afecta colateralmente a innovar. Es importante saber cómo sacar le el jugo a esta tecnología y que la sociedad se beneficie de ella. La confianza lo es todo.

**BIBLIOGRAFÍA**

- Abogados Digitales. Autor: José Torres Varela. Editorial: abogados digitales.tfdc.co
- [www.dinero.com/tecnología/artículo/payu-y-la-criptomoneda-de-facebook-libra](http://www.dinero.com/tecnología/artículo/payu-y-la-criptomoneda-de-facebook-libra)
- [www.superfinanciera.gov.co/jsp/publicaciones/publicaciones](http://www.superfinanciera.gov.co/jsp/publicaciones/publicaciones)
- [www.eltiempo.com/tecnoesfera](http://www.eltiempo.com/tecnoesfera)
- Memorias del XXII Congreso Iberoamericano de Derecho e Informarica (Blockchain, Bitcoin y Monedas Virtuales) RICO CARRILLO M. [http://fiadi.org/wp-content/uploads/2019/08/memorias\\_22\\_congreso\\_fiadi-apandetec\\_2018\\_vf.pdf](http://fiadi.org/wp-content/uploads/2019/08/memorias_22_congreso_fiadi-apandetec_2018_vf.pdf)
- <https://cdn.bancentral.gov.do/documents/avisos/documents/aviso20170628.pdf>
- <https://medium.com/@coinsuper/exploring-different-perspectives-on-blockchain-and-cryptocurrencies-cb55e431fdd3>
- <https://invertix.com.do/mas-de-5000-personas-transan-con-criptomonedas-en-republica-dominicana>



REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).  
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.  
ISSN 2530-4496 – AÑO 1, N° 8, 2020, PÁGS. 91-106

**EL IMPACTO DE *BLOCKCHAIN* Y EL COVID-19 EN LA DIGITALIZACIÓN  
DE LOS SISTEMAS DE PAGO.**

THE IMPACT OF *BLOCKCHAIN* AND COVID-19 ON THE DIGITIZATION  
OF PAYMENT SYSTEMS.

**Mariliana Rico Carrillo<sup>1</sup>**

Universidad Católica del Táchira (Venezuela)

1 Prof. Dra. Catedrática de Derecho Mercantil.  
Secretaria General de la Federación Iberoamericana de Asociaciones de Derecho e Informática



## RESUMEN

El *bitcoin*, la tecnología *blockchain* y las criptomonedas son esenciales en el proceso conocido como la digitalización de los sistemas de pago. Las criptomonedas, en su función de instrumentos de pago alternativos al dinero fiduciario cada día adquieren más importancia en la economía mundial. La escasez y disminución del uso del dinero efectivo, ha motivado a los bancos centrales de diversos países a estudiar la posibilidad de emitir monedas digitales basadas en el funcionamiento del *bitcoin* y las criptomonedas, con los retos y desafíos que esto implica tanto a nivel regulatorio como tecnológico. La utilidad de las monedas digitales emitidas por los bancos centrales ha sido destacada recientemente como consecuencia de los efectos de la pandemia mundial que estamos viviendo, al comprobarse que el tan temido COVID-19 se transmite mediante el contacto con el papel moneda. En el presente trabajo se analizan las implicaciones de la tecnología *blockchain* y el uso de las criptomonedas, así como los efectos del COVID-19 en la digitalización de lo sistemas de pago.

## PALABRAS CLAVE:

Dinero digital. Sistemas de pago. Criptomonedas. Blockchain. COVID-19

## ABSTRACT

Bitcoin, Blockchain and cryptocurrencies are an essential part of digitalization of payment systems. Cryptocurrencies, as an alternative to the use of fiat money, are becoming increasingly important. The shortage of cash in some countries has been the main reason for Central Banks to analyze the possibility of issuing digital currencies with the challenges that this implies at the regulatory and technological levels. Usefulness of digital currencies issued by Central Banks has been highlighted once again because of the effects of the global pandemic we are facing, as it has proven that the much-feared COVID-19 is transmitted through banknotes. This paper analyzes the implications of blockchain technology and the use of cryptocurrencies, as well as the effects of COVID-19 on the process of digitizing payment systems.

## KEYWORDS:

Digital Money. Payment Systems. Cryptocurrencies. Blockchain. COVID-19

## I. INTRODUCCIÓN

*El saldo de nuestra cuenta corriente no es menos virtual  
que los bitcoins que alberga nuestro monedero...*

Javier Maestre<sup>1</sup>

He querido comenzar este trabajo con la cita del reconocido jurista español Javier Maestre, ya que no hay nada más cierto que actualmente el respaldo del dinero en sus diferentes concepciones -fiduciario, escriturario, electrónico o digital- es virtual. Hoy en día, ni el dinero de curso legal o dinero fiduciario (que en la mayoría de los casos circula a través de transferencias electrónicas de fondos que se reflejan en nuestras cuentas bancarias) ni el dinero digital, representado a través de las famosas criptomonedas cuentan con un soporte físico que garantice su valor.

En el dinero fiduciario no existen las reservas en oro que tradicionalmente respaldaban la emisión de los billetes y monedas bancarios; en este caso, la confianza en su valor y uso como medio de pago la otorga el Estado a través de la autoridad a la cual se le asigna la función de emitir la moneda (los bancos centrales)<sup>2</sup>. En las anotaciones contables que tienen lugar cuando se produce una transferencia de fondos entre distintas cuentas bancarias, la confianza reside en la institución financiera encargada de ejecutar la operación. En el dinero digital, la confianza se deriva de la conocida tecnología *blockchain*, que permite su emisión y circulación de forma segura y controlada. En las monedas digitales (criptomonedas), la base de la confianza no se encuentra en la intervención de una autoridad pública o de una institución financiera determinada, sino en la propia tecnología y en la actuación de los sujetos que participan en la emisión, circulación e intercambio de este nuevo medio de pago.

El uso de las criptomonedas está desplazando al dinero fiduciario, tanto en forma de billetes y monedas como a sustituto legal: el dinero electrónico. La importancia y utilidad de este nuevo medio de pago digital han sido destacadas recientemente en diversos ámbitos ante los efectos producidos por la pandemia mundial que estamos viviendo, al comprobarse que el COVID-19 se transmite mediante el contacto con el papel moneda. Ante esta situación, diversos bancos centrales están analizando la posibilidad de emitir monedas digitales, con los retos y desafíos que esto implica, tanto a nivel regulatorio como tecnológico.

Las circunstancias descritas en los párrafos anteriores han motivado la elaboración del presente trabajo, orientado a estudiar las implicaciones de la tecnología *blockchain* en la digitalización de los sistemas de pago, así como la importancia del uso de medios de pago alternativos al dinero efectivo como una forma de evitar el contagio del COVID-19. Para cumplir estos objetivos me dedicaré, en primer lugar, al análisis del dinero electrónico como la fase inicial del proceso de digitalización de los sistemas de pago, que comenzó con la aparición de las tarjetas prepagadas y su regulación. La segunda etapa de este proceso está determinada por el desarrollo del *bitcoin* y la tecnología *blockchain*, que han permitido y difundido el uso de las conocidas criptomonedas o monedas virtuales, en la terminología empleada por las autoridades financieras europeas. La investigación finaliza con una mención al impacto del COVID-19 como catalizador de los sistemas de pago digitales, donde se hace una referencia al interés que ha despertado en los bancos centrales de distintos países la emisión de las monedas digitales para contribuir a la prevención del virus.

1 MAESTRE, Javier: “El mito del dinero virtual”, disponible en <http://www.maestreabogados.com/tag/moneda-electronica/> (última consulta: 15 de mayo de 2020)

2 El dinero fiduciario es la moneda que un gobierno ha declarado como dinero de curso legal sin estar respaldado por un producto físico. El valor del dinero fiduciario se deriva de la relación entre la oferta y la demanda y de la confianza en la autoridad emisora, más que del valor del respaldo material del dinero. El dinero fiduciario comenzó a dominar en el siglo XX, a partir 1971 con las políticas monetarias del presidente estadounidense Richard Nixon que pusieron fin a la época de las reservas en oro.

## II. LA DIGITALIZACIÓN DE LOS SISTEMAS DE PAGO: DEL DINERO ELECTRÓNICO A LAS CRIPTOMONEDAS

### 1. Precisiones terminológicas y conceptuales

#### 1.1. La electrificación y la digitalización de los sistemas de pago

Los avances tecnológicos experimentados desde finales del siglo pasado han producido importantes modificaciones en los tradicionales sistemas de pago, dando origen al proceso conocido como “electrificación”. En el sector de los medios de pago, este término se usa en forma amplia para hacer referencia al empleo de la electrónica y la informática, tanto en el diseño de nuevos medios de pago como en la representación de los ya existentes<sup>3</sup>.

Dentro del proceso de la electrificación encontramos la digitalización, que se refiere estrictamente a la eliminación del papel y su sustitución por un soporte digital, tal como sucede con el dinero electrónico en su concepción de dinero de curso legal, o al empleo de una tecnología digital determinada en la emisión del medio de pago, en el caso de las criptomonedas.

#### 1.2. Los sistemas de pago electrónicos

El empleo de la electrónica en los sistemas de pago comienza con las transferencias de fondos y el uso de las tarjetas, al producirse la sustitución de las órdenes de pago, tradicionalmente emitidas en papel por impulsos electrónicos, dando lugar a los denominados sistemas de pago electrónico (SPE).

Cuando se usan las transferencias como medios de pago, se emplea la denominación “moneda escrituraria” para hacer referencia a las anotaciones contables que tienen lugar como consecuencia del movimiento de fondos de una cuenta a otra. El uso generalizado de las transferencias como mecanismos de pago puso de manifiesto la importancia de las anotaciones contables, destacando que el dinero es “...simplemente información y como tal, puede residir en la memoria de los ordenadores...”<sup>4</sup>

La expansión del comercio electrónico en Internet y la necesidad de diseñar instrumentos de pago adecuados al desarrollo tecnológico produjo el primer avance importante en los sistemas de pago electrónico<sup>5</sup>, dando lugar al diseño de mecanismos como *Paypal* y el dinero electrónico, concebido como un sustituto legal de los tradicionales billetes y monedas bancarios. El dinero electrónico se erige como la primera etapa del proceso de digitalización de los sistemas de pago. Esta fase comenzó ya hace algunos años con la aparición de las tarjetas prepagadas, conocidas como monederos electrónicos y su regulación. En las siguientes líneas me ocuparé del estudio de esta forma de pago.

### 2. El dinero electrónico como sustituto del dinero de curso legal

En Europa, el dinero electrónico es regulado por primera vez en la Directiva 2000/46CE sobre entidades de dinero electrónico y su ejercicio, modificada nueve años después debido a los avances experimentados en el sector (Directivas EDE). El desarrollo tecnológico en este sector exigió la modificación del marco regulador, que se produjo con la aprobación de la Directiva 2009/110/CE del

3 Un estudio amplio sobre la electrificación en el ámbito de los medios de pago *vid.* RICO CARRILLO, Mariliana: *El pago electrónico en Internet. Estructura operativa y régimen jurídico*, Thomson Reuters-Aranzadi, Madrid, 2012.

4 DEL PESO NAVARRO, Emilio: “Transferencias electrónicas de fondos: proyección social y jurídica” *XI Encuentros sobre Informática y Derecho*, Instituto de Informática Jurídica, Universidad Pontificia de Comillas, Aranzadi, Madrid, 1997.

5 Un sistema de pago se define como un conjunto de instrumentos, procedimientos y reglas para la transferencia de fondos entre los participantes del sistema. Por lo general, se basa en un acuerdo entre el participante y el operador del sistema, donde la transferencia de fondos se realiza utilizando una infraestructura técnica acordada. El calificativo “electrónico” se añade para destacar que la circulación y representación del dinero se materializan a través de técnicas electrónicas. Los sistemas de pago electrónico, sus aplicaciones y funcionamiento en Internet han sido analizados en estudios previos. *Vid.* RICO CARRILLO, Mariliana: *El pago electrónico en Internet. Estructura operativa y régimen jurídico*, op. cit. p. 35.

Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades.

De acuerdo con las previsiones del artículo 2 de la segunda Directiva EDE, el concepto del dinero electrónico se refiere a un valor monetario, almacenado por medios electrónicos o magnéticos, que representa un crédito sobre el emisor y se emite al recibir de fondos del titular, con el propósito de efectuar operaciones de pago y es aceptado por una persona distinta del emisor.

De esta definición se derivan las características básicas de esta forma de pago: 1) la emulación legal del dinero tradicional, 2) el almacenamiento del dinero en un soporte electrónico, 3) la aceptación por empresas distintas del emisor, y 4) su emisión por un valor igual a los fondos recibidos (valor a la par).

Un elemento fundamental en el esquema del funcionamiento del dinero electrónico es su conversión a dinero de curso legal, que se establece con la finalidad de mantener la confianza de los titulares y usuarios de estos instrumentos de pago. Para lograr esta conversión, la Directiva EDE establece la obligación de reembolso a las entidades emisoras de dinero electrónico (EDE), quienes deben pagar el valor nominal equivalente en dinero de curso legal al titular del mismo, en cualquier momento que éste lo solicite.<sup>6</sup>

Al concebirse como una emulación del dinero fiduciario, la emisión de dinero electrónico es una actividad altamente regulada y corresponde exclusivamente a las EDE, quienes deben cumplir unos requisitos específicos con el objeto de ser autorizadas para funcionar como tales. Es importante mencionar que las EDE se consideran entidades de crédito y como tales están sometidas a un régimen de supervisión específico, y que el artículo 18 del referido texto legal prohíbe en forma expresa la emisión de dinero electrónico a cualquier persona física o jurídica que no cuente con la respectiva autorización.

En cuanto a la concepción del dinero electrónico como un sustituto del dinero fiduciario, es importante destacar que desde una óptica estrictamente jurídica los conceptos no son del todo identificables, ya que sólo el dinero de curso legal es de obligatoria aceptación como medio de pago. En este sentido, y al igual que sucede con los otros medios de pago alternativos al dinero fiduciario, el acreedor debe aceptar, previamente a la operación, el pago mediante dinero electrónico, sin estar obligado a ello.

Otra característica distintiva del dinero electrónico, de acuerdo con su concepto legal, es el almacenamiento previo del valor monetario en un soporte electrónico, lo cual implica que para su emisión es necesario tener una cuenta bancaria en una institución financiera, ya que son los fondos de esa cuenta los que permiten emitir este medio de pago. Este soporte electrónico puede ser un instrumento tangible (el chip de una tarjeta) o intangible (la memoria de un ordenador).

El análisis de estos elementos (regulación, emulación del dinero de curso legal, la obligación de reembolso, la provisión de fondos previa a la emisión, el control y la supervisión de la actividad) es trascendental para poder establecer las diferencias con el *bitcoin* y otras monedas virtuales y determinar la naturaleza jurídica de estos nuevos instrumentos de pago.

### 3. La aparición del bitcoin y las criptomonedas

El *bitcoin*, la tecnología *blockchain* y la popularización en el uso de las criptomonedas han producido toda una revolución en el proceso de digitalización de los sistemas de pago, determinada por el uso

---

6 Un estudio amplio de las características del funcionamiento del dinero electrónico puede consultarse en MARTÍNEZ NADAL, A: *Dinero electrónico: aproximación jurídica*, Civitas, Madrid, 2003.

de un “ecosistema”<sup>7</sup> de tecnologías, que ha dado origen a una segunda generación de los SPE, caracterizada por el uso de medios de pago basados en sistemas de confianza descentralizados y privados, lo cual marca una notable diferencia con los tradicionales SPE centralizados y públicos, al excluir la actuación de los intermediarios financieros.

La primera moneda virtual en aparecer en el mercado y que ha causado un mayor impacto en la economía es el *bitcoin*, cuyo uso y funcionamiento se basa en la tecnología *blockchain* (cadena de bloques en español), que permite realizar pagos electrónicos sin la intervención de un banco, una empresa de tarjetas de pago o otro intermediario típico de los sistemas de pago electrónicos como *Paypal*.<sup>8</sup>

#### 4. La intermediación como característica diferenciadora de los sistemas de pago electrónico de primera y segunda generación

Los SPE involucran el estudio de dos componentes básicos: la transferencia electrónica de fondos (TEF), como el sistema que permite efectuar el movimiento del dinero, y los instrumentos de pago electrónico (IPE), entendidos como los dispositivos que permiten a los usuarios emitir las órdenes de pago para activar la TEF, como sucede por ejemplo en las tarjetas de crédito, débito o en los monederos electrónicos. El dinero electrónico y otros sistemas de pago como *Paypal* requieren la presencia de un tercero para gestionar los pagos y procesar las TEF. La intermediación de este tercero (tradicionalmente una institución bancaria, hoy en día una *fintech*) infunde confianza en los usuarios.

La intermediación predominante en estos sistemas de pago nos permite distinguir una primera generación de SPE, cuya base es la centralización de la confianza en una tercera parte, de una segunda generación, caracterizada por la descentralización y la ausencia de terceros de confianza. Esta segunda generación surge como consecuencia del uso de la tecnología *blockchain*, que ha cambiado significativamente el paradigma tradicional de la confianza. Aunque el modelo centralizado continúa en uso, y sigue siendo predominante, *blockchain* permite realizar pagos descentralizados a través de monedas virtuales, donde la confianza reside en la propia tecnología y en la participación de los usuarios e intervinientes en la transacción, como sucede en las criptomonedas.

### III. BLOCKCHAIN: LA SEGUNDA FASE DE LA DIGITALIZACIÓN DE LOS SISTEMAS DE PAGO

El protocolo *blockchain* fue difundido en el año 2009 tras la publicación del documento técnico “*Bitcoin: a Peer to Peer Electronic Cash System*”, cuya autoría se atribuye al japonés Satoshi Nakamoto. Su funcionamiento se centra en el diseño de un SPE basado en el uso de la criptografía y la tecnología *peer to peer*, eliminando de esta manera la intermediación financiera, con la finalidad de ofrecer una alternativa de pagos diferente a los sistemas tradicionales.

Aunque la tecnología *blockchain* ha sido definida de diversas maneras, técnicamente es un protocolo que combina diversos servicios de confianza (criptografía, firmas digitales, sellos de tiempo) y establece un conjunto de reglas que aseguran la integridad de la transacción a través de la intervención de distintos sujetos, sin que ninguno de ellos pueda calificar como una tercera parte de confianza.

El concepto de moneda electrónica expuesto en el citado documento se fundamenta en el uso de la firma digital basada en criptografía de clave pública. El protocolo define el funcionamiento de una

7 En los distintos documentos que han analizado el funcionamiento de las MV se usa el término «ecosistema» para hacer referencia a la combinación de distintas tecnologías y a la presencia categorías nuevas y específicas de actores que no estaban presentes en los sistemas de pago tradicionales.

Vid. EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes- a fuerte análisis*, February 2015, p. 3. Disponible en <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> (última consulta: 14 de junio de 2018)

8 TAPSCOTT D. y A. TAPSCOTT: *Blockchain Revolution*, Penguin Random House, LLC, New York, 2016 p. 6.

cadena de firmas digitales donde una persona transfiere un valor monetario a otra en forma cronológica, mediante la firma de un *hash* de una transacción previa y la incorporación de la clave pública del próximo propietario, agregándolas al final de la operación, de modo que cuando los beneficiarios de la transacción accedan posteriormente a las firmas puedan verificar la cadena de propiedad.<sup>9</sup>

*Blockchain* permite que todas las transacciones sean verificadas y registradas en un bloque que está directamente vinculado con el bloque anterior, creando la respectiva cadena que otorga un carácter irreversible a las operaciones (inmutabilidad), que a su vez son validadas por la mayoría de los participantes en la red. En este caso, el consenso de las partes es el elemento fundamental que avala la seguridad de la transacción.

A diferencia de lo que sucede con las instituciones financieras, se trata es una red de acceso público y una nueva forma de colaboración *peer to peer*, esto implica cualquiera puede acceder a los registros en cualquier momento y que no existe una tercera parte que certifique las operaciones. En el ámbito de los medios de pago es una plataforma que se distingue por la inclusión y la disminución del costo de la transacción (en comparación con las tradicionales TEF y los SPE de primera generación), ya que no requiere cuentas bancarias, aprobaciones de crédito u otras inversiones, elementos característicos de la intermediación financiera que aunque aportan seguridad, aumentan el costo de la transacción.

#### IV. LOS ESQUEMAS DE MONEDAS VIRTUALES

La irrupción del *bitcoin* y otras monedas virtuales ha llamado la atención de las autoridades europeas, principalmente del Banco Central Europeo (BCE) como catalizador de los sistemas de pago y de la Autoridad Bancaria Europea (ABE) como ente supervisor de las actividades financieras. Ambas instituciones han elaborado distintos documentos a efectos de estudiar el funcionamiento de las monedas virtuales, tomando en cuenta principalmente las implicaciones del uso del *bitcoin* en el sistema financiero. La expresión moneda virtual (*virtual currency*) se usa en forma genérica diferenciar esta forma de pago del dinero electrónico como sustituto del dinero de curso legal.

Los informes del BCE se refieren en forma amplia a los esquemas de monedas virtuales (EMV) y datan de 2012<sup>10</sup> y 2015<sup>11</sup>. Estos documentos tratan diversos aspectos relacionados con los nuevos medios de pago, incluyendo la relevancia de los EMV para los bancos centrales y los riesgos para la estabilidad financiera y los sistemas de pago. Los trabajos de la AEB también están orientados a analizar el funcionamiento de las monedas virtuales, su infraestructura técnica, sujetos participantes, potenciales riesgos y beneficios. Sus conclusiones se recogen en el dictamen titulado *Opinion on “virtual currencies”*, de julio de 2014.<sup>12</sup>

En este apartado me enfoco en el estudio de las monedas virtuales, tomando como base los informes del BCE y las conclusiones del dictamen de la AEB de 2014, que, como veremos más adelante, han sido tomadas en cuenta en la redacción de la quinta Directiva en materia de prevención del blanqueo de capitales y la financiación del terrorismo<sup>13</sup>, aprobada en mayo de 2018<sup>14</sup>.

9 NAKAMOTO, Satoshi “*Bitcoin: a Peer to Peer Electronic Cash System*”, disponible en <https://bitcoin.org/bitcoin.pdf> (última consulta: 14 de junio de 2020)

10 EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op.cit.*

11 EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes- a further analysis*, February 2015, *op. cit.*

12 EUROPEAN BANKING AUTHORITY (EBA) *Opinion on “virtual currencies”*, July 2014. Disponible <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> (última consulta: 15 de julio de 2018)

13 Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.

Existen distintos tipos de monedas virtuales, unas son de uso abierto, otras limitadas a una comunidad determinada, algunas son de flujo unidireccional y otras de flujo bidireccional<sup>15</sup>. El término criptomoneda (*cryptocurrency*) se refiere a un tipo específico de monedas virtuales como el *bitcoin*, que son descentralizadas y de uso bidireccional<sup>16</sup>, características que se derivan del uso de la tecnología *blockchain*.

Antes de examinar las diferentes definiciones, insistimos que jurídicamente y en su concepción actual, no estamos hablando de dinero electrónico (ni mucho menos de dinero de curso legal) en el sentido que no existe una institución financiera que respalde su emisión. Las monedas virtuales (en adelante MV), son medios de pago de carácter privado, cuya delimitación conceptual es importante para conocer sus implicaciones jurídicas, para saber de qué estamos hablando y cuál sería la regulación aplicable (si es que existe alguna) o para saber qué es lo que en el futuro se va a regular.

## 1. La moneda virtual como dinero digital

Los distintos documentos que han tratado de definir las MV vinculan este concepto con la noción de dinero digital para diferenciar estos nuevos medios de pago del dinero electrónico como emulación del dinero fiduciario.

Uno de los primeros conceptos lo encontramos en el Informe del BCE de 2012 que define las MV como "...un tipo de dinero digital no regulado, emitido y generalmente controlado por sus desarrolladores, utilizado y aceptado entre los miembros de una comunidad virtual específica." En el texto de este documento se diferencian los distintos tipos de MV y se advierte que la definición se formula de manera abierta, en el entendido que puede ser adaptada en el futuro, si las características fundamentales de su funcionamiento cambian.

En su dictamen de 2014, la ABE define las MV como una "...representación digital de valor no emitida por un banco central o autoridad pública, ni necesariamente vinculada con el concepto de dinero fiduciario, que es utilizada por personas físicas o jurídicas como un medio de intercambio y puede transferirse, almacenarse o intercambiarse por medios electrónicos". La importancia de esta última definición es notable por sus efectos en la futura regulación de las MV, de hecho, ha sido incorporada en la quinta Directiva de prevención de utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo, (conocida por sus siglas en inglés 5AMLD, correspondientes a la expresión *Fifth Anti/Money Laundering Directive*), sobre la cual hablaré más adelante.

La influencia del dictamen de la ABE también la podemos observar en el informe del BCE de 2015, que se refiere a los avances de las MV e indica que el BCE ha estado examinando el desarrollo de estos SPE para analizar su relevancia en los sistemas de pago minoristas. Los lineamientos de la ABE están presentes en este nuevo informe al indicar que las MV como el *bitcoin*, no son formas de dinero tal como se definen en la literatura económica, sino "...una representación digital de valor, no emitida por un banco central, institución de crédito o institución de dinero electrónico, que en algunas circunstancias se puede utilizar como una alternativa al dinero."

14 La Directiva destaca que el anonimato de las monedas virtuales permite su uso indebido con fines delictivos como sistemas de financiación alternativa para los grupos terroristas que pueden ser capaces de transferir dinero hacia el sistema financiero de la UE o dentro de las redes de monedas virtuales ocultando transferencias o gozando de cierto grado de anonimato en esas plataformas (*Vid.* considerandos 8, 9 y 10 de la citada directiva).

15 En cuanto a los diferentes tipos de EMV, los informes del BCE advierten la presencia de tres: 1) los esquemas cerrados, que carecen de vínculo con la economía real; 2) los esquemas de flujo unidireccional, donde las monedas se pueden comprar a un tipo de cambio específico pero no pueden ser canjeadas; y 3) los esquemas de flujo bidireccional, que permiten a los usuarios comprar y vender MV de acuerdo con las tasas de cambio y se usan para la compra de bienes y servicios virtuales y reales. En este caso, las MV son similares a cualquier otra moneda convertible con respecto a su interoperabilidad en el mundo real. Esta categoría es la que se identifica con el término "criptomonedas". *Vid.* EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op.cit.*

16 EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes- a further analysis*, February 2015, *op. cit.*

Como bien puede observarse, tanto el BCE como la ABE y la propia Comisión Europea concuerdan al conceptualizar las MV como una representación digital de valor de carácter privado, aceptada como una alternativa de pago. Los principales rasgos distintivos de esta nueva forma de pago y su diferencia con el concepto de dinero electrónico se especifican en el siguiente apartado.

## 2. Características

### a) *La descentralización como elemento fundamental*

La descentralización es el elemento fundamental que caracteriza el funcionamiento de las MV. Tradicionalmente, la confianza en los sistemas de pago y en las operaciones electrónicas encuentra su base en la intervención de los denominados terceros de confianza. Estos terceros de confianza son de la más variada índole y van desde los intermediarios financieros tradicionales hasta las empresas especializadas en SPE como *Paypal*. En estos casos se habla de modelos de confianza centralizados, donde la seguridad reside en una determinada persona o institución.

En los SPE de segunda generación, los usuarios compran y venden las MV entre ellos sin ningún tipo de intermediación, ya que la confianza la proporciona la propia red a través de la infraestructura tecnológica. La información distribuida entre los diversos usuarios y la presencia de los denominados «mineros»<sup>17</sup> aportan seguridad y confianza a la transacción. En los modelos descentralizados, la tecnología *blockchain* y la confianza en la red sustituye a los bancos e intermediarios financieros.

### b) *La criptografía como elemento de seguridad y la inmutabilidad de la transacción*

En materia de pagos efectuados a través de medios electrónicos, la criptografía ha adquirido singular importancia en los últimos años, gracias a su uso en los sistemas de pago propios de las operaciones bancarias y financieras, con la finalidad de lograr la identificación entre el receptor y el emisor del mensaje y mantener la confidencialidad de la información<sup>18</sup>.

Los sistemas de cifrado asimétrico permiten la generación de firmas digitales, que es el mecanismo de seguridad que utiliza el protocolo *blockchain*. Gracias al empleo de estas técnicas criptográficas, las partes pueden realizar diversas transacciones sin la intervención de terceros confiables, ya ellas mismas verifican la cadena de bloques desde su origen hasta el final. Las operaciones se registran en un bloque que está directamente vinculado con el bloque anterior, creando la respectiva cadena que otorga el carácter de inmutabilidad a las transacciones.

Las transacciones firmadas se envían a la red, lo que significa son públicas y aunque no se proporciona información sobre las partes involucradas, se pueden rastrear<sup>19</sup>. La información queda registrada de manera permanente y es replicada de forma distribuida en los distintos servidores que forman parte

17 Los «mineros» son los sistemas informáticos que validan las transacciones. El proceso de minería se lleva a cabo a través de equipos extremadamente rápidos que pueden realizar cálculos matemáticos complejos con la finalidad de verificar la validez de las transacciones. Vid. EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op. cit.*, p. 23

18 El propio BCE ha destacado la importancia del uso de técnicas criptográficas en el ámbito de los pagos a través de Internet, en el Informe sobre Dinero Electrónico de 1998 se menciona la criptografía como el medio idóneo para autenticar las transacciones y proteger la confidencialidad e integridad de la información en los instrumentos de dinero electrónico. Vid. EUROPEAN CENTRAL BANK (ECB) *Report on Electronic Money*, August 1998.

19 A través de la tecnología *blockchain*, cuando una persona envía una moneda se registran todos los datos de la transferencia: dirección de red desde la que salen las MV, la dirección de envío, cantidad y momento exacto de la transacción. A través de la dirección de red se puede rastrear la transacción, aunque esta siga siendo anónima, ya que lo que se identifica es la dirección de red y no el usuario. La Directiva 5AMLD se refiere a la dirección de red como la dirección de las monedas virtuales. Para combatir los riesgos relacionados con ese anonimato, el considerando 9 indica que las Unidades de Inteligencia Financiera (UIF) nacionales deben tener acceso a la información que les permita vincular las direcciones de las monedas virtuales con la identidad del propietario de la moneda virtual.

de la red. La inmutabilidad está directamente relacionada con la prevención del doble gasto, es decir, evitar que se copie o falsifique una moneda, especialmente si se considera que no existe un intermediario que valide las transacciones.

### *c) La presencia de nuevos actores*

El uso de la tecnología *blockchain* implica la presencia de nuevos actores en el mecanismo de pago. Al igual que en la economía real, en una economía virtual hay una amplia gama de actores económicos que intervienen en las transacciones de diferentes maneras<sup>20</sup>.

En el esquema del funcionamiento de las MV básicamente encontramos los siguientes participantes: 1) los creadores originales del sistema que permite emitir las monedas (inventores), que son los individuos u organizaciones que desarrollan la infraestructura técnica que soporta la red; 2) los usuarios que intercambian, adquieren o invierten las monedas; 4) los mineros, que resuelven los *hashes* y validan las transacciones a efectos de impedir el doble gasto y la falsificación de las monedas, recibiendo a cambio pequeñas cantidades de MV; 5) los proveedores que ofrecen billeteras digitales a los usuarios para almacenar sus claves criptográficas de MV y los códigos de autenticación que permiten realizar las transacciones, denominados en la terminología jurídica “proveedores de servicios de custodia de monederos electrónicos”<sup>21</sup>.

Al lado de estos sujetos se encuentran las entidades que participan en el intercambio de MV por dinero fiduciario, transferencias de fondos, otros medios de pago (tarjetas, dinero electrónico), u otras monedas virtuales, en el supuesto que éstas sean convertibles<sup>22</sup>, los intermediarios que ponen en contacto a las distintas personas que desean comprar o vender en los distintos mercados donde se cotizan las MV, y los proveedores de bienes y/o servicios aceptantes de MV.

Como explicaremos en el siguiente epígrafe, la aprobación de la Directiva sobre prevención de blanqueo de capitales, somete a **los proveedores de servicios de cambio de MV por monedas fiduciarias** y a los proveedores de servicios de custodia de monederos electrónicos al cumplimiento de los requisitos de supervisión y vigilancia indicados en la norma comunitaria.

### *d) Su uso como medio de pago*

Las MV pueden utilizarse como medio de pago para obtener bienes y servicios. El grado de aceptación varía de un esquema a otro y depende de los participantes del mercado (es decir, de su red de aceptación) ya que su uso puede ser amplio o estar limitado a una comunidad específica de individuos<sup>23</sup>.

En esencia, los EMV funcionan de manera muy similar a los sistemas de pago minoristas, excepto por el hecho que los intermediarios financieros no están involucrados en el proceso de pago. En los EMV están presentes los tres elementos principales de un sistema de pago minorista: 1) se utiliza un instrumento de pago que debe ser aceptado entre las partes, 2) el procesamiento y la compensación implica una instrucción de pago entre el acreedor y el deudor, y 3) los débitos y créditos se liquidan en la cuenta del usuario<sup>24</sup>.

20 *Vid.* EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op. cit.*,

21 Estos proveedores permiten el acceso a los distintos esquemas de MV y son definidos en la 5AMLD como una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales.

22 Algunos esquemas de MV son convertibles (o abiertos) y, por lo tanto, se pueden intercambiar por dinero fiduciario a un tipo de cambio, mientras que otros no son convertibles (o cerrados), es decir, son específicos de una comunidad en particular y no pueden intercambiarse. *Vid.* EUROPEAN BANKING AUTHORITY (EBA) *Opinion on “virtual currencies”*, July 2014, *op. cit.* p. 13.

23 EUROPEAN BANKING AUTHORITY (EBA) *Opinion on “virtual currencies”*, July 2014, *op. cit.*

24 *Vid.* EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op. cit.*

### 3. Iniciativas regulatorias. Las monedas virtuales en la Directiva sobre prevención de blanqueo de capitales

Durante el mes de mayo de 2018 fue aprobada la quinta Directiva sobre prevención de utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo (5AMLD). Esta norma es el primer texto legal de carácter vinculante a nivel comunitario que establece un marco jurídico aplicable al funcionamiento de las plataformas de cambio de MV, al someter a su regulación a **los proveedores de servicios de cambio de MV por monedas fiduciarias** y a los proveedores de servicios de custodia de monederos electrónicos. Una de las novedades más importantes de la 5AMLD es precisamente la inclusión de **estos proveedores** en su ámbito de aplicación, **por lo tanto**, como entidades obligadas están sometidas al deber de aplicar las correspondientes medidas preventivas y de notificar toda transacción sospechosa relacionada con las MV.

Otro aspecto a destacar de esta Directiva es la incorporación en un texto jurídico vinculante del concepto de MV elaborado por la AEB. El artículo 1 de la 5AMLD modifica el texto de su predecesora, la Directiva 2015/89 (4AMLD) con la finalidad de añadir el concepto de MV, que a efectos legales se entiende como una:

....Otro aspecto a destacar es la incorporación del concepto de MV, originalmente formulado en el dictamen de la AEB de 2014 en un texto legal de carácter vinculante para todos los Estados miembros de la UE. "... una representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos.

## V. LAS MONEDAS VIRTUALES FRENTE AL DINERO ELECTRÓNICO

Los SPE basados en el uso MV difieren sustancialmente de los esquemas de dinero electrónico en diversos aspectos, en los que destacan la forma de emisión, la intervención de las entidades financieras, la vinculación con el dinero de curso legal y la determinación del valor de la moneda.

Una de las diferencias fundamentales entre estos dos SPE es que las MV no tienen como contraparte física el dinero de curso legal, como sucede con el dinero electrónico, por lo tanto, los sujetos participantes y el régimen jurídico es notablemente diferente. Las MV no involucran la participación de los actores financieros tradicionales, el emisor generalmente es una empresa privada no financiera, es por ello que las normas de regulación y supervisión del sector financiero no son aplicables. En los EMV el control íntegro lo asume el emisor, quien gobierna la red y administra la emisión y circulación del dinero.

En cuanto a la vinculación con el dinero de curso legal, en el dinero electrónico existe la obligación de reembolso impuesta por ley a las EDE, lo que significa su convertibilidad obligatoria en dinero fiduciario. La circulación del dinero electrónico es restringida, es por ello que al recibirlo, su titular debe remitirlo a la entidad emisora para proceder a su convertibilidad. En las MV no necesariamente existe tal vinculación, ya que éstas pueden circular sin restricción y también se pueden intercambiar unas por otras sin ser convertidas en dinero fiduciario. Aunque es posible el intercambio de MV por dinero fiduciario, este vínculo no está regulado por la ley.

El respaldo del dinero electrónico es el dinero de curso legal, es por ello que se requiere que el valor monetario esté almacenado previamente en un soporte electrónico; el respaldo de las MV es la confianza en la tecnología y en los participantes en la red: el consenso es el aval de la transacción.

A efectos de evitar el doble gasto, en el caso del dinero electrónico el aceptante del medio de pago debe remitir la moneda a la entidad emisora y ésta debe verificar que la moneda no ha sido cobrada

previamente antes de proceder a la conversión a dinero de curso legal. En el esquema de las MV el control del doble gasto lo proporciona la tecnología *blockchain*.

Respecto a su valor, las MV no solo funcionan como medios de pago, también se pueden intercambiar unas por otras. Su valor se basa en un tipo de cambio específico que puede fluctuar sobre la base de la demanda y oferta, es decir, pueden conservar, aumentar o disminuir su valor. El valor del dinero electrónico es fijo, se emite por un valor igual a los fondos recibidos y sólo es convertible en dinero efectivo a su valor nominal.

## VI. EL IMPACTO DEL COVID-19 EN LA DIGITALIZACIÓN DE LOS SISTEMAS DE PAGO

### 1. El COVID-19 como catalizador del dinero digital

Estudios recientes han demostrado que el intercambio de billetes mano a mano representa un alto grado de riesgo para la transmisión del COVID-19. Los resultados en este sentido son alarmantes, ya que se ha comprobado que el virus puede permanecer vivo en la superficie de los billetes por un periodo de 17 días, de modo que el contacto con el papel moneda puede ser un vehículo idóneo para el contagio.

Ante esta situación, en febrero de 2020 la Reserva Federal de los Estados Unidos de América (FED) adoptó una serie de medidas para poner en cuarentena los dólares físicos provenientes de Asia como un mecanismo de precaución para disminuir la propagación del virus. Otros países han restringido la circulación del dinero efectivo y recomiendan hacer los pagos a través de transferencias electrónicas de fondos, dinero digital o criptomonedas. Todas estas circunstancias demuestran que la pandemia se presenta como un posible catalizador en la digitalización de los sistemas de pago, con sus correspondientes ventajas, riesgos y consecuencias.

### 2. Las monedas digitales emitidas por los bancos centrales

La escasez del dinero efectivo en algunos países y los problemas generados por esta situación en los distintos sectores de la economía motivaron inicialmente a las autoridades de los bancos centrales a estudiar la posibilidad de emitir una moneda digital accesible al público general como un instrumento de pago alternativo seguro, sólido y fácil de usar.

El COVID-19 y los resultados de los estudios indicados anteriormente han aumentado el interés de los bancos centrales en emitir monedas digitales, con los retos y desafíos que esto significa tanto a nivel regulatorio y tecnológico como en la economía en general.

Las implicaciones económicas y jurídicas de la emisión de monedas digitales por parte los bancos centrales son analizadas por el Banco de Pagos Internacionales (BPI) en el informe titulado “Las monedas digitales emitidas por bancos centrales”<sup>25</sup>, publicado por este organismo en marzo de 2018. En este documento, elaborado en conjunto por el Comité de Pagos e Infraestructuras del Mercado y el Comité de los Mercados, el BPI presenta un análisis inicial de los posibles efectos de las monedas digitales emitidas por los bancos centrales en los pagos, la política monetaria y la estabilidad financiera. El BCE también ha evaluado recientemente los costos y beneficios derivados del uso del dinero digital emitido por los bancos centrales ante la escasez del del dinero efectivo<sup>26</sup>.

El concepto de las monedas digitales emitidas por los bancos centrales -conocidas por la abreviatura

25 Disponible en [https://www.bis.org/cpmi/publ/d174\\_es.pdf](https://www.bis.org/cpmi/publ/d174_es.pdf) (última consulta: 25 de mayo de 2020)

26 «*Innovation and its impact on the European retail payment landscape*», *European Central Bank*, diciembre 2019. (última consulta: 25 de mayo de 2020), disponible en <https://www.ecb.europa.eu/pub/pdf/other/ecb.other191204~f6a84c14a7.en.pdf> (última consulta: 25 de mayo de 2020).

CBDC, correspondiente a la expresión *Central Bank Digital Currency*- está inspirado en la tecnología *blockchain*, el uso del *bitcoin* y otras criptomonedas. Diversos Estados están trabajando actualmente en la implementación y diseño de las CBDC o dinero digital fiat. Países como Inglaterra y Suecia ya cuentan con proyectos específicos en esta área<sup>27</sup>.

La conveniencia de mejorar los actuales sistemas de pago al por menor mediante el uso de las monedas digitales ha sido destacada recientemente por las autoridades del Banco de Inglaterra. En un discurso pronunciado en febrero de este año, su vicegobernador, Sir Jon Cunliffe, afirmó que las CBDC podrían aportar grandes beneficios a los bancos centrales y a la economía en general. Además de esto, también indicó que la reglamentación en esta materia debe seguir el ritmo de los avances tecnológicos<sup>28</sup>, lo cual debe venir acompañado de un estudio económico, tecnológico y jurídico.

Las apreciaciones de Cunliffe siguen el mismo enfoque adoptado en el informe del BPI, que indica que los bancos centrales y otras autoridades encargadas de velar por la estabilidad de la política monetaria deben seguir vigilando las innovaciones digitales y analizar cómo se verían afectadas sus propias operaciones en el caso que se apruebe la emisión y circulación de las CBDC.

Para finalizar este estudio considero importante destacar que el informe del BPI también menciona la importancia de cumplir las obligaciones previstas en las normas sobre prevención del blanqueo de capitales y de la financiación del terrorismo y satisfacer los requisitos en materia de políticas públicas de otros regímenes supervisores y fiscales. En este sentido, el BPI es consistente con las orientaciones de la legislación europea aprobada en 2018 (la quinta Directiva en materia de prevención del blanqueo de capitales y la financiación del terrorismo) que como vimos anteriormente, incluye en su articulado un concepto legal de MV -entendidas como una representación digital de un valor monetario- a efectos de someter a su regulación a **los proveedores de servicios de cambio de MV por dinero fiduciario** y a los proveedores de servicios de custodia de monederos electrónicos. Estos sujetos, al igual que las instituciones financieras tradicionales, tienen el deber de aplicar las correspondientes medidas preventivas y de notificar toda transacción sospechosa relacionada con las monedas digitales.

---

27 En 2016, el banco central de Suecia (Riskbank) comenzó el proyecto de las CBDC denominadas *e-krona* concebidas como una solución a la fuerte caída del uso del dinero en efectivo. *Vid.* <https://es.cointelegraph.com/news/what-is-e-krona-and-why-will-nothing-ever-be-the-same> (última consulta: 25 de mayo de 2020). Sobre el proyecto inglés, *vid.* discurso de Andy Haldane, disponible en <https://www.bankofengland.co.uk/speech/2015/how-low-can-you-can-go> (última consulta: 25 de mayo de 2020)

28 CUNLIFFE, Jon. *It's time to talk about money. Speech Bank of England*, disponible en <https://www.bis.org/review/r200304f.htm> (última consulta: 10 de junio de 2020).

**BIBLIOGRAFÍA**

- CUNLIFFE, Jon: *It's time to talk about money. Speech Bank of England*, disponible en <https://www.bis.org/review/r200304f.htm> (última consulta: 10 de junio de 2020).
- DEL PESO NAVARRO, Emilio: “Transferencias electrónicas de fondos: proyección social y jurídica” *XI Encuentros sobre Informática y Derecho*, Instituto de Informática Jurídica, Universidad Pontificia de Comillas, Aranzadi, Madrid, 1997.
- FERNADEZ BURGUEÑO, Pablo: “Retos legales del bitcoin, ethereum y los smart contracts”, en *Hacia una Justicia 2.0 volumen X*, Actas del XX Congreso Iberoamericano de Derecho e Informática, volumen II, 2016 pp. 345-356.
- NAKAMOTO, Satoshi “*Bitcoin: a Peer to Peer Electronic Cash System*”, disponible en <https://bitcoin.org/bitcoin.pdf>
- MAESTRE, Javier: “El mito del dinero digital”, disponible en <https://www.maestreabogados.com/bitcoin-mito-dinero-virtual/> (última consulta: 10 de junio de 2020).
- MARTÍNEZ NADAL, Apo.lonia: *Dinero electrónico: aproximación jurídica*, Civitas, Madrid, 2003.
- RICO CARRILLO, Mariliana: *El pago electrónico en Internet. Estructura operativa y régimen jurídico*, Thomson Reuters Aranzadi, Madrid, 2012.
- TAPSCOTT D. y A. TAPSCOTT: *Blockchain Revolution*, Penguin Random House, LLC, New York, 2016 p.

## **BIBLIOGRAFÍA**

- Abogados Digitales. Autor: José Torres Varela. Editorial: abogados digitales.tfdc.co
- [www.dinero.com/tecnología/artículo/payu-y-la-criptomoneda-de-facebook-libra](http://www.dinero.com/tecnología/artículo/payu-y-la-criptomoneda-de-facebook-libra)
- [www.superfinanciera.gov.co/jsp/publicaciones/publicaciones](http://www.superfinanciera.gov.co/jsp/publicaciones/publicaciones)
- [www.eltiempo.com/tecnoesfera](http://www.eltiempo.com/tecnoesfera)
- Memorias del XXII Congreso Iberoamericano de Derecho e Informarica (Blockchain, Bitcoin y Monedas Virtuales) RICO CARRILLO M. [http://fiadi.org/wp-content/uploads/2019/08/memorias\\_22\\_congreso\\_fiadi-apandetec\\_2018\\_vf.pdf](http://fiadi.org/wp-content/uploads/2019/08/memorias_22_congreso_fiadi-apandetec_2018_vf.pdf)
- <https://cdn.bancentral.gov.do/documents/avisos/documents/aviso20170628.pdf>
- <https://medium.com/@coinsuper/exploring-different-perspectives-on-blockchain-and-cryptocurrencies-cb55e431fdd3>
- <https://invertix.com.do/mas-de-5000-personas-transan-con-criptomonedas-en-republica-dominicana>

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).  
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.  
ISSN 2530-4496 – AÑO 1, N° 8, 2020, PÁGS. 107-120

**BLOCKCHAIN Y PROTECCIÓN DE DATOS PERSONALES**

BLOCKCHAIN AND PERSONAL DATA PROTECTION

**Olivia Andrea Mendoza Enríquez<sup>1</sup>**

Centro de Investigación y Docencia Económicas CIDE

1 Profesora Asociada del CIDE



**RESUMEN:**

El Blockchain es una tecnología innovadora que permite hacer más eficiente la vida de las personas, a partir de un variado campo de acciones, que entre otras cosas permiten realizar transacciones que generan confianza y la disminución de gastos de operación para las organizaciones. Existen grandes apuestas en torno al blockchain, para varios sectores como el financiero o el registral.

No obstante, a pesar de los evidentes beneficios, se advierten algunos obstáculos al cumplimiento de las normas en materia de protección de datos personales en el servicio de blockchain, vinculados al ejercicio de los denominados derechos ARCO, en específico a los derechos de rectificación y cancelación de los datos personales, así como la dificultad para determinar los actores que asumen la figura de Responsable del tratamiento de datos, por lo que este trabajo formula un análisis de las implicaciones del cumplimiento del derecho de protección de datos personales en el servicio de blockchain, desde una visión del modelo europeo en la materia y de las normas mexicanas aplicadas al caso.

**PALABRAS CLAVES:**

*Cumplimiento*, derecho de protección de datos personales, blockchain, derechos ARCO.

**ABSTRACT:**

The blockchain is an innovative technology that allows to make people's lives more efficient, from a varied field of actions, which allow transactions that generate trust and decrease operating expenses for organizations. There are big benefits around the blockchain, for various sectors such as the financial or the registry.

However, despite the obvious benefits, there are some obstacles to compliance with the regulations on the protection of personal data in the blockchain service, linked to the exercise of the so-called ARCO rights, specifically to the rights of rectification and cancellation of personal data, as well as the determination of the figure of Responsible for data processing, so this work formulates an analysis of the implications of compliance with the right to protection of personal data in the blockchain service, from a model perspective European in the matter and the Mexican norms applied to the case.

**KEYWORDS:**

*Compliance*, personal data protection right, blockchain, ARCO rights.

## I. INTRODUCCIÓN

La tecnología denominada blockchain, apunta a ser la más innovadora del momento, lo cual abre las puertas a nuevas posibilidades de usos, que sin duda alguna, resolverán grandes problemas para las organizaciones, a través de la garantía de no alteración de la información, el almacenamiento distribuido, el rastreo preciso de datos, o la ejecución de contratos sin la intervención de terceros, entre otros.

Si bien el término de blockchain apareció por primera vez en 2008 con el *whitepaper* que dio lugar al bitcoin, y publicado por el usuario Satoshi Nakamoto, esta tecnología innovadora ya había sido imaginada y descrita por Nick Szabo, cuando hablaba del funcionamiento de los *smart contracts*.<sup>1</sup>

El blockchain consiste en términos generales, desde una perspectiva meramente técnica, en la implementación de un registro distribuido de transacciones mantenido por una red descentralizada de nodos, garantizando la integridad del registro, por medio de protocolos criptográficos, que sustituyen la necesidad de utilizar terceras partes de confianza que garanticen la seguridad de la información.<sup>2</sup>

Dichas características técnicas, permitirían un sinnúmero de usos tanto para el sector público como para el privado, eliminando costos de operación y otorgando certeza a los actores dentro de las transacciones a través del blockchain.

No obstante lo anterior y pese a los pronósticos optimistas sobre el blockchain, se advierten algunos desafíos en el cumplimiento de las normas, específicamente concernientes al derecho de protección de datos personales, relativos principalmente, a la garantía de los derechos de rectificación y cancelación de los datos, los múltiples Responsables en el tratamiento de datos personales y la portabilidad de los datos, aspectos que se detallarán en los siguientes apartados.

Es así, que en este trabajo se abordará el concepto de blockchain desde una perspectiva legal, las implicaciones del derecho de protección de datos personales para esta tecnología, los principales desafíos que se presentan a partir del modelo europeo de protección de datos personales y de la legislación en la materia aplicable para el caso de México, para así aportar algunas conclusiones, cuyos enunciados no son definitivos y los cuales estarán sujetos al vertiginoso desarrollo e innovación del blockchain.

## II. CONCEPTO DEL BLOCKCHAIN DESDE UNA PERSPECTIVA JURÍDICA

Como ya se ha dicho, el término blockchain apareció formalmente con el reconocimiento de las bitcoin<sup>3</sup> y a través del *whitepaper* publicado por Satoshi Nakamoto.

La expresión “tecnología blockchain” suele usarse en las cadenas públicas y por todos los desarrolladores y usuarios; la denominación “tecnología de contabilidad distribuida” o DLT (*Distributed Ledger Technology*), se utiliza en el ámbito del desarrollo privado, y está más bien alejada de bitcoin como

1 La primera vez que se tiene constancia de forma pública sobre los *smart contracts* es a través de **Nick Szabo**, jurista y criptógrafo, quien mencionó públicamente el término en un documento en 1995. Dos años después, en 1997, desarrolló un documento mucho más detallado explicando los *smart contracts*. No obstante, era imposible hacer realidad los *smart contracts* con la infraestructura tecnológica de ese momento, ya que para ejecutarlos, era necesaria la existencia de transacciones programables y un sistema financiero que las reconociera. Disponible en el sitio web: <https://academy.bit2me.com/que-son-los-smart-contracts/> (Fecha de consulta 30 de abril del 2020).

2 Rodríguez Garagorri, Margarita, Análisis de tecnologías de bitcoin y blockchain, Universidad Oberta de Catalunya. Disponible en el sitio web: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72606/6/mrgaragorriTFM1217memoria.pdf> (Fecha de consulta 10 de junio del 2020).

3 Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para Internet. Bitcoin puede ser el único sistema de contabilidad triple existente. Disponible en el sitio web: <https://bitcoin.org/es/faq> (Fecha de consulta 3 de junio de 2020).

criptomoneda; mientras que “tecnología bitcoin” es el término más ambiguo, y refiere a tres conceptos: la tecnología de contabilidad distribuida en su conjunto, la blockchain de bitcoin en particular, e incluso los protocolos que han permitido el desarrollo de todas las criptomonedas.<sup>4</sup>

Es así que, si bien el término blockchain pareciera tener una connotación meramente técnica, resulta necesario analizar sus características y vincularlas a las implicaciones legales que este servicio presenta.

Para iniciar este apartado, es necesario dar una aproximación conceptual al blockchain, pudiendo afirmar que es una contabilidad pública entre pares que se mantiene mediante una red distribuida de ordenadores y que no requiere ninguna autoridad central ni terceras partes que actúen como intermediarios.

Hasta este punto entonces, es conveniente identificar que el funcionamiento del blockchain requiere un esquema colaborativo entre pares, lo cual, a la luz del Derecho, permitiría identificar varios actores involucrados, al menos en el tratamiento de datos personales. Esto con la salvedad de conocer si la contabilidad, incluye información que permita identificar o haga identificable a una persona.

También llama la atención la posibilidad de no requerir de una autoridad central que garantice o supervise el servicio de blockchain, ya que esto implicaría muy probablemente la adecuación de marcos legales nacionales, por ejemplo, en materia financiera.

Dicho lo anterior, continuamos con la conceptualización técnica, al identificar tres componentes fundamentales: una transacción, un registro de transacciones y un sistema que verifica y almacena la transacción. Los bloques se generan a través de *software* de código abierto y registran la información sobre cuándo y en qué secuencia ha tenido lugar la transacción. Este «bloque» almacena cronológicamente información de todas las transacciones que tienen lugar en la cadena, de ahí el nombre de cadena de bloques o blockchain. Dicho de otro modo, una blockchain es una base de datos con información horaria estampada e inmutable de cada transacción que se replica en servidores de todo el mundo.<sup>5</sup>

Estos componentes no son tarea menor para el Derecho, ya que estamos frente a transacciones que se realizan en el ciberespacio, que en principio encontrarían diversas jurisdicciones y autoridades competentes para conocer de conflictos que ahí surjan; es decir, si bien el blockchain es un servicio descentralizado, algunos usos requerirían la intervención, supervisión o incluso acreditación de autoridades. Por ejemplo, transacciones del sector financiero, transacciones vinculadas a prestación de servicios contratados por el Estado, o incluso la misma supervisión que las autoridades nacionales en materia de protección de datos personales tuvieran que hacer, frente al tratamiento de información de carácter personal.

Por otro lado, el registro de transacciones tiene una intersección legal, ya que por ejemplo, frente a la solicitud de derechos de rectificación y/o cancelación del dato<sup>6</sup>, tendríamos que el registro está distri-

---

4 Ocampo Muñoz, Gustavo, Nuevos desafíos para la protección de datos personales en el blockchain. Disponible en el sitio web: <https://revistas.juridicas.unam.mx/index.php/derechoinformacion/article/view/13881/15338> (Fecha de consulta 1° de junio de 2020).

5 Reporte de investigación, Situación. Economía Digital. Tecnología de cadena de bloques, blockchain. Disponible en el sitio web: [https://www.bbvaresearch.com/wp-content/uploads/2015/08/Situacion\\_Economia\\_digital\\_jul-ago15-Cap4.pdf](https://www.bbvaresearch.com/wp-content/uploads/2015/08/Situacion_Economia_digital_jul-ago15-Cap4.pdf) (Fecha de consulta 12 de junio de 2020).

6 En relación con el derecho humano de protección de datos personales, tanto el modelo normativo europeo como la legislación nacional, reconocen que el derecho de protección de datos personales cobra vida a través de los denominados derechos ARCO (acceso, rectificación, cancelación y oposición) frente al tratamiento de datos personales. Es importante decir que el Reglamento Europeo de Protección de Datos Personales, habla del derecho de portabilidad del dato, el cual ha sido recogido en el ámbito mexicano, en la Ley General de Protección de Datos Personales en Posesión de

buido por un sinnúmero de actores en el servicio, denominados pares, lo cual en la práctica haría compleja la salvaguarda del derecho de protección de datos personales, teniendo en cuenta que cada par, fungiría como Responsable, en términos de este derecho y en algunos casos como Encargados. En el mismo componente, también resultaría importante analizar los aspectos tecnológicos que garanticen la confidencialidad de la información.

El último componente del blockchain relativo a un sistema que verifica y almacene la transacción, también presenta desafíos legales, sobre todo relacionados con la inmutabilidad de la información y el almacenamiento en bloques, ya que al igual que en el punto anterior, hacen complejo desde la perspectiva técnica, el poder rectificar información ahí almacenada, cancelarla o incluso asegurar la portabilidad<sup>7</sup> en materia de datos personales.

En consideración al acceso a los datos almacenados, la cadena de bloques puede clasificarse en pública o privada. En la primera no hay ninguna restricción para la lectura de datos ni para la realización de las operaciones por parte de los usuarios; en cambio, en la segunda, tanto la lectura como las operaciones se limitan a participantes determinados.

En cuanto a la capacidad para generar bloques, se dividen en aquellas sin permisos y con permisos. En la primera no hay restricciones para poder realizar transacciones y crear nuevos bloques, de modo que se ofrecen monedas o activos digitales nativos de la red como recompensa a los usuarios que quieren mantener la red; son descentralizadas, como bitcoin. Las segundas son desarrolladas por entidades generalmente privadas, en muchos casos para uso interno, y los usuarios de éstas necesitan permisos por parte de los administradores de la red para interactuar con el protocolo; son centralizadas, es decir, controladas por la entidad, y no por los usuarios.<sup>8</sup>

Como podrá advertirse, son precisamente las capacidades para generar bloques privadas, las que permitirían un cumplimiento de los derechos de acceso y rectificación de los datos personales, o al menos facilitarían el cumplimiento del nivel normativo impuesto por el modelo europeo y mexicano de protección de datos personales, sin que existieran imposibilidades técnicas para tal fin.

A partir de la conceptualización del blockchain, también podemos advertir que existen otros aspectos legales a considerar, tales como la responsabilidad de los programadores y de las corporaciones frente a errores del código, la necesidad de armonizar los contratos de prestación del servicio a las normas domésticas, a fin de garantizar la validez, y el cumplimiento de requisitos en materia fiscal, que prevengan, por ejemplo, blanqueo de activos.

El blockchain se asocia normalmente a las criptomonedas, pero también abre las puertas a nuevas posibilidades, pensando por ejemplo, en la programación a través de blockchain para un ejercicio de recursos públicos de forma eficiente y transparente o incluso, para fines de votaciones virtuales que fortalezcan a democracia en los países. En el sector privado, uno de los actores más interesados en el abanico de usos del blockchain es el financiero, ya que la tecnología permitiría reducir al mínimo, los riesgos asociados por ejemplo, al uso de la banca en línea o incluso permitiría la instrumentación de

---

Sujetos Obligados (legislación aplicable al tratamiento de datos personales en manos del sector público), el cual, a criterio de algunos autores, podría ser la continuación de los derechos ARCO. Desde una opinión de la autora, la portabilidad sería una forma de manifestación del derecho de acceso de los datos personales.

7 En términos de la Agencia Española de Protección de Datos Personales, este derecho complementa al derecho de acceso, ya que permite a las personas obtener los datos que han proporcionado a una entidad/empresa/organización (responsable del tratamiento) en un formato estructurado, de uso común y de lectura mecánica. El derecho a la portabilidad también implica que los datos personales de ese usuario podrían transmitirse directamente de una entidad o empresa a otra, sin necesidad de ser entregados al propio usuario, siempre que ello sea técnicamente posible. Información consultada el 12 de junio del 2020. Disponible en el sitio web: <https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-el-derecho-la-portabilidad> (Fecha de consulta 10 de junio de 2020).

8 Op. Cit. Nota 4.

*smart contracts* dotando de certeza en el cumplimiento de las responsabilidades y obligaciones a las partes que intervengan.

### III. NATURALEZA JURÍDICA DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES

El derecho de protección de datos personales es un derecho humano reconocido en instrumentos internacionales como el Convenio 108 del Consejo de Europa, y que encuentra su antecedente más importante, en el artículo 12 de la Declaración Universal de Derechos Humanos.<sup>9</sup>

A manera de introducción de este apartado, se debe decir que la Constitución Política de los Estados Unidos Mexicanos, no reconoce de forma expresa el derecho a la privacidad, pero el constituyente sí incluyó en el artículo 16 ciertas protecciones aisladas sobre distintos aspectos relacionados con la privacidad, como el derecho a no ser molestado en el ámbito familiar, domicilio, papeles y posesiones, sin una orden firmada por autoridad competente.<sup>10</sup>

A diferencia del derecho a la privacidad, el derecho de protección de datos personales sí está reconocido de forma expresa en la carta magna en el citado artículo 16 constitucional, el cual señala:

Artículo 16. ...

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros...<sup>11</sup>

Es así entonces, que en 2007 se reconoce por primera vez, el derecho de protección de datos personales como un derecho constitucional en México.

No obstante lo anterior, debemos recordar que en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002, ya se hablaba de disposiciones relativas al tratamiento de datos personales en el sector público para el caso de México<sup>12</sup>.

La evolución normativa de este derecho ha sido paulatina, pero con pasos sólidos, ya que a partir de la reforma al sexto constitucional, se han desarrollado dos normas secundarias que dictan derechos, deberes y obligaciones en materia de protección de datos personales, tanto para el sector privado, como el público en México: Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) y la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (2017), respectivamente.

---

9 Si bien el artículo 12 de la Declaración Universal de Derechos Humanos no reconoce de forma expresa el derecho de protección de datos personales, sí reconoce el derecho a la no injerencia en la vida privada de las personas, lo cual establece las bases para el derecho a la privacidad, que no podría entenderse, sin un derecho que dote de control a la persona, sobre su información de carácter personal, y que como hemos dicho, este control se manifiesta a través de los derechos de acceso, rectificación, cancelación y oposición (ARCO) frente al tratamiento de datos personales.

10 García Ricci, Diego, Artículo 16 constitucional. Derecho a la privacidad. Disponible en el sitio web: <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf> (Fecha de consulta 2 de junio del 2020).

11 Constitución Política de los Estados Unidos Mexicanos. Consultada el 30 de mayo del 2020. Disponible en el sitio web: [http://www.diputados.gob.mx/LeyesBiblio/pdf/1\\_080520.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf) (Fecha de consulta 3 de junio del 2020).

12 Es el Capítulo IV de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en el que se dictan disposiciones generales sobre el tratamiento de datos personales, señalando la información de carácter personal, como una limitante para el ejercicio del derecho de acceso a la información en el sector público. Disponible en el sitio web: [http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG\\_abro.pdf](http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf) (Fecha de consulta 10 de junio del 2020).

Asimismo, a partir de 2018 México forma parte del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), lo cual obliga a acatar un nivel de cumplimiento acorde al modelo europeo de protección de datos personales, en el cual el Reglamento Europeo de Protección de Datos Personales desempeña un rol importantísimo, frente al tratamiento de datos personales a través de nuevas tecnologías e Internet.

Es así que México cuenta con un robusto marco legal en materia de protección de datos personales, que sería aplicable a aquella información de carácter personal que sea tratada a través del servicio de blockchain.

No obstante lo anterior, las normas nacionales, al no estar apoyadas por medidas regionales como el establecimiento de bloques económicos, comerciales o políticos, en algunas ocasiones quedan rebasadas frente al poder de las corporaciones o de la *lex mercatoria*, por ejemplo, frente a los fenómenos como la extraterritorialidad de la norma (Patriot Act de EUA), la simultaneidad de fenómenos vinculada con la ubicuidad en la prestación del servicio, las múltiples jurisdicciones interactuando, la reducción del concepto de Estado-Nación frente a los derechos humanos exigibles en el ciberespacio, etc.

Es así que el reto del derecho de protección de datos personales no es nada menor, frente a innumerables beneficios que permite el blockchain, pero a la vez, frente a diversas complejidades para la salvaguarda de este derecho, atendiendo las características propias del funcionamiento de la tecnología de bloques.

Aunado a esto, la suscripción de tratados internacionales por parte de México, cuyo contenido contravienen derechos humanos reconocidos en la Constitución, representan otros desafíos para la salvaguarda del derecho de protección de datos personales en el blockchain. Ejemplo de ello, lo encontramos en el Capítulo sobre Comercio Digital del Tratado de Libre Comercio entre Estados Unidos de Norteamérica, Canadá y México (TMEC), el cual señala que frente a la posible aplicación de diversas normativas en materia de protección de datos personales, el tratamiento de la información se ceñirá a las normas de privacidad dictadas en el marco del Foro de Cooperación Económica Asia Pacífico (APEC), siendo importante mencionar que dichas normas derivadas del foro económico Asia-Pacífico, no están armonizadas del todo, por ejemplo con el Reglamento Europeo de Protección de Datos Personales, siendo necesario entonces, considerar la suscripción de acuerdos de puerto seguro, frente a riesgos en torno a la garantía del derecho humano de protección de datos personales desde el modelo de regulación europeo y mexicano. En este punto, no es menos importante mencionar características de los derechos humanos como la progresividad y la herramienta de interpretación reconocida en nuestra carta magna relativa al principio *pro persona*, lo cual haría evidente la contravención a la constitución respecto de reducir el nivel de protección a disposiciones menos proteccionistas y derivadas de un foro económico, que no desarrollan en su justa dimensión, la protección de datos personales como un derecho humano, y que lo reconocen más bien, como un derecho de los consumidores.

#### **IV. PROTECCIÓN DE DATOS PERSONALES EN EL BLOCKCHAIN**

Dicho lo anterior, y entrando a aspectos específicos sobre el cumplimiento de las disposiciones normativas en materia de protección de datos personales en el blockchain, podemos identificar que derechos como el de rectificación y cancelación en materia de protección de datos personales, hacen casi imposible su salvaguarda, frente a bloques inmutables, inamovibles, y permanentes, que sostienen la cadena de funcionamiento del blockchain.

Aunado a esto, formas de ejercicio del derecho de acceso a datos personales, como el de la portabilidad del dato, se vuelven bastante complejos, frente a la distribución de bloques en manos de diversos usuarios.

Entonces hablar de derechos de supresión, desindexación o el propio derecho al olvido, se vuelve casi imposible frente a tecnologías como el blockchain y es así, ante diversos panoramas, que la pregunta empieza a surgir, ¿qué debe prevalecer?, el funcionamiento técnico del blockchain que abre un abanico de posibilidades para eficientar los procesos y la vida de los humanos, o la garantía sobre todas las cosas del derecho humano a la protección de datos personales, en aras de salvaguardar la dignidad humana, sustento de la Declaración Universal de Derechos Humanos, y elemento esencial de reflexión a partir de las atrocidades cometidas durante la Segunda Guerra Mundial. Para algunos la respuesta será clara y no habrá un criterio unificador que otorgue una justificación sobre la respuesta, aunque desde la óptica legal, es evidente que la conformación de los estados constitucionales de derecho, las atrocidades de la guerra y el reconocimiento de los derechos humanos, tienen una razón de ser, para garantizar la subsistencia de las personas.

Es decir, a pesar de los innumerables beneficios del blockchain, se advierten grandes incompatibilidades que no podrán quedar por debajo de un derecho humano, constitucionalmente garantizado, como es el derecho de protección de datos personales en México.

Esto, sin duda alguna, un freno bastante complejo para el abanico de usos que permitiría el blockchain, por lo que será un desafío permanente, lograr la compatibilidad de la tecnología, con la salvaguarda de la máxima esfera de los componentes del derecho a la protección de datos personales.

En este sentido, para analizar la dimensión que cobra el reconocimiento del derecho humano a la protección de datos personales y su impacto al blockchain, y como ya se ha hablado en líneas anteriores, resulta pertinente decir que, para el caso de México, el desarrollo normativo en materia de protección de datos personales, ha tenido gran influencia del modelo europeo en la materia, por lo que este tema podrá ser abordado desde dos visiones específicas y aplicables al caso: el Reglamento Europeo de Protección de Datos Personales y la legislación mexicana sobre la materia.<sup>13</sup>

El Reglamento General de Protección de Datos personales (RGPD), es la norma general sobre el derecho fundamental a la protección de datos en la Unión Europea. Su principal objetivo es dar mayor control a las personas físicas sobre el tratamiento de sus datos personales, para lo que refuerza la armonización de las normas nacionales en materia de protección de datos.<sup>14</sup>

El RGPD identifica actores que intervienen en el tratamiento de datos personales para disponer obligaciones sobre dicho tratamiento y un actor importantísimo es el denominado Responsable<sup>15</sup>. El principal desafío en el blockchain, es que resulta casi imposible determinar un solo Responsable, cuando

13 El 12 de junio de 2018 se publicó en el Diario Oficial de la Federación el decreto por el cual se aprueban en México el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del 28 de enero de 1981 ( Convenio 108), y su Protocolo Adicional del 8 de noviembre de 2001, relativo a las autoridades de control y a los flujos transfronterizos de datos. El Convenio 108 del CE es uno de los documentos más importantes a nivel internacional que logra constituirse como una norma vinculante y que busca generar un estándar para el tratamiento de datos personales, cuya característica única es que ha quedado abierto a países no miembros de la Unión Europea, que deseen suscribirlo. Un motivo poderoso para la suscripción del Convenio, se encuentra en la necesidad de crear relaciones comerciales que conllevan flujo transfronterizo de datos personales, y esto a fin de que un país tercero logre arreditar el nivel adecuado de protección, y pueda recibir información de carácter personal, sin necesidad de suscribir un acuerdo de puerto seguro.

14 Información disponible en el sitio web:

<https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAkN-jEwNjY7Wy1KLizPw8WyMDQwsDU0MTkEBmWqVLfnJIZUGqbVpiTnEqAMUH2Hw1AAAAWKE#:~:text=Su%20principal%20objetivo%20es%20dar,materia%20de%20protecci%C3%B3n%20de%20datos.> (Fecha de consulta 9 de junio del 2020).

15 La figura de Responsable está definida en el RGPD en el artículo 4 numeral 7, señalando que es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

su característica principal es que existen diversos actores que garantizan el funcionamiento de distribución de bloques, por lo que en principio, estaríamos frente a muchos Responsables en materia de protección de datos personales, sin poder determinar quién de todos ellos, estaría obligado, por ejemplo, a garantizar el derecho de rectificación de datos personales contenidos en el blockchain. Esto sin advertir las imposibilidades técnicas de modificar un bloque que alteraría la cadena completa de bloques. En el blockchain, por lo menos se identifican actores como los propietarios de la Red, los desarrolladores, los nodos que participan en la Red y los usuarios interesados. Todos accediendo a la información distribuida en bloques, que puede contener datos personales. Es así que resulta complicado en primer lugar identificar a los Responsables y en segundo lugar a los Encargados<sup>16</sup> del tratamiento de datos personales, con las obligaciones que cada uno tendría frente a las normas en materia de protección de datos personales.

Algunas autoridades en materia de protección de datos personales y grupos de trabajo especializados en el ámbito europeo, se han pronunciado por la necesidad de definir los actores en el blockchain, identificando los supuestos en los que se fungiría como Responsable de datos personales.

Es así que, en septiembre de 2018, la Autoridad Francesa de Protección de Datos (CNIL) publicó un estudio acerca de la compatibilidad de la tecnología Blockchain con el Reglamento General de Protección de Datos de la UE<sup>17</sup>. La CNIL distingue entre quienes tienen permiso para escribir en la cadena (participantes) y los que validan una transacción y crean bloques de información aplicando las reglas de Blockchain para que éstos sean aceptados (mineros). Si un grupo de participantes con un propósito común decide llevar a cabo actividades de tratamiento usando sistemas Blockchain, será por tanto preciso identificar al responsable del tratamiento. Este tema podría ser solventado, creando una entidad y nombrándola como responsable del tratamiento, o bien nombrando al participante que tome mayoritariamente las decisiones del grupo como responsable. De lo contrario, todos ellos podrían ser considerados como Responsables conjuntos de tratamiento. En cuanto a la figura correspondiente a los Encargados de tratamiento, según la CNIL, podrían ser:

- 1) Los desarrolladores de contratos que procesan datos personales en nombre del participante (el responsable de tratamiento).
- 2) O los mineros, que son quienes validan el registro de los datos personales en el sistema blockchain.<sup>18</sup>

Frente a la dificultad de los diversos Responsables y Encargados del tratamiento de datos personales en el blockchain, resultaría conveniente entonces operar una red de blockchain privada, ya que al controlar a los actores, daría pauta a un cumplimiento normativo frente a los derechos de acceso, rectificación, cancelación y oposición, de forma más sencilla, identificando el rol que jugaría cada actor.

Por otro lado, una opción técnica para garantizar derechos como el de supresión, reconocido en el GDPR, es la posibilidad de aplicar procesos de anonimización irreversible, con el objetivo de que el dato sea tan inaccesible que pudiera darse una equivalencia a la supresión. En esta opción, el dato personal permanece en el blockchain, pero su acceso sería prácticamente imposible.

Respecto al derecho de rectificación de datos personales, como se ha dicho en líneas previas, la inmutabilidad del dato contenido en los bloques, representa un desafío de cumplimiento normativo, pero podría explorarse la posibilidad de generar nuevos registros que contengan la información actualizada

---

16 El artículo 4 numeral 8 del RGPD, señala que el Encargado es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

17 Disponible en el sitio web: <https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles> (Fecha de consulta 2 de junio del 2020).

18 Candano Bea. Nuevo estudio de compatibilidad entre el blockchain y el GDPR. Disponible en el sitio web: <https://www.linkedin.com/pulse/nuevo-estudio-de-compatibilidad-entre-blockchain-y-el-bea-m-candano/> (Fecha de consulta 3 de junio del 2020).

y de esa forma anular registros anteriores con información incorrecta.

Por otro lado, y como vimos al principio de este documento, el blockchain permite materializar la suscripción de *smart contracts*, situación que trae a la luz la necesidad de incluir esquemas de intervención humana, cuando las decisiones automatizadas propicien daños a las partes; es decir, un derecho de revisión o impugnación frente a decisiones automatizadas que contravengan los derechos de los que intervienen en el contrato.

Por otro lado, la necesidad de intervención de diversos pares (que pueden estar en cualquier parte del mundo), nos colocaría frente a posibles transferencias internacionales de datos personales, que deberán atender los requisitos de la norma europea y mexicana en dicha materia. En este rubro, frente a transferencias internacionales de datos hacia países no seguros, será necesario instrumentar medidas como los acuerdos de puerto seguro.

Derivado de todo lo anteriormente explicado, resulta importantísimo garantizar una configuración del blockchain desde su origen, en términos de garantizar el cumplimiento de las normas en materia de protección de datos personales, y en este sentido, la privacidad por diseño ayudaría a lograr este objetivo.

Para el caso de México, la legislación nacional en materia de protección de datos personales, reconoce la obligación de elaborar evaluaciones de impacto a la privacidad, cuando se pretenda poner en funcionamiento tecnologías que signifiquen un tratamiento relevante e intensivo de datos personales (como podría suponer en algunos casos el blockchain), por lo que se deberá estar sujeto a las disposiciones normativas de la ley nacional.

Cuando hablamos de posibles soluciones que ayuden al cumplimiento normativo en materia de protección de datos personales, no podemos obviar la necesidad de desarrollar e incluir códigos de ética en el funcionamiento del blockchain.

Por otro lado, considerar minimizar el tratamiento de datos personales o incentivar que la información se genere anonimizada, reduciría la responsabilidad de cumplimiento de las normas en materia de protección de datos personales.

Finalmente, la enorme ventaja que parece aportar los tipos de blockchain privados, permitirían la identificación de roles de Responsables y Encargados en el tratamiento de datos personales, para la salvaguarda de derechos de acceso, rectificación, cancelación y oposición frente al tratamiento de datos personales.

A pesar de los obstáculos pendientes de superar por parte de la autoridad garante del derecho de protección de datos personales en México, cuando de supervisar a actores que operan en el ciberespacio se trata, otra opción no solo de cumplimiento, sino de auditoría, se encuentra en la facultad del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos, para asegurarse del cumplimiento del derecho de protección de datos personales en territorio nacional, a través del procedimiento de verificación.

Es necesario también adecuar los marcos legales nacionales, comprendiendo el funcionamiento de la tecnología y teniendo en cuenta cuáles son las implicaciones de los derechos humanos para los Estados, que como ya hemos visto de forma general, van desde la progresividad de estos derechos, hasta su salvaguarda incluso en el ciberespacio.

## V. CONCLUSIONES

1. El blockchain permite hablar de un abanico de opciones que efficientan los procesos para las organizaciones, reducen los costos de operación y generan confianza y certeza entre los usuarios.
2. No obstante, el blockchain representa desafíos para el cumplimiento de algunas disposiciones nor-

mativas, principalmente relacionadas con el derecho de protección de datos personales.

3. El derecho de protección de datos personales ha tenido una evolución normativa importante en México, el cual se ha construido bajo la lógica del modelo europeo de protección en la materia. Esto trae como consecuencia, la obligatoriedad del cumplimiento de normas como el Convenio 108 del consejo de Europa, el Reglamento Europeo de Protección de Datos Personales y las leyes nacionales en la materia.
4. Si bien es complejo asegurar el cumplimiento de las disposiciones en materia de protección de datos personales en el blockchain, ya que tiene características aparentemente incompatibles con dicho cumplimiento, los derechos humanos no pueden estar por debajo de los desarrollos tecnológicos, por lo que se deberá pensar en esquemas de privacidad por diseño, para asegurar el cumplimiento normativo y de salvaguarda a este derecho humano.
5. El derecho de protección de datos personales cobra vida a través de los derechos de acceso, rectificación, cancelación y oposición frente al tratamiento de datos personales, por lo que el blockchain deberá ser diseñado, desarrollado e implementado, con la lógica de cumplimiento de estos derechos. Técnicas como la cadena de bloques privada, permitiría asegurar el cumplimiento frente a derechos ARCO, considerando que una de las características del servicio, es la inmutabilidad de la información, lo cual, en principio, haría casi imposible la salvaguarda de derechos como el de cancelación del dato o la rectificación, por lo que en la medida de control sobre los bloques, podría residir la posibilidad del nivel de cumplimiento normativo en materia de protección de datos personales.
6. Frente al cumplimiento normativo en materia de protección de datos personales, existen dos figuras importantes para tener en cuenta: Responsables y Encargados. En términos del funcionamiento técnico del blockchain, es complejo determinar los actores que intervienen en el tratamiento de datos personales bajo estas figuras, ya que prácticamente cualquier actor podría ser Responsable o Encargado, por lo que se debe considerar al momento de desarrollar cadenas de bloques, técnicas que permitan discernir entre estas dos figuras y por ende, entre el grado de responsabilidad en torno a la salvaguarda del derecho de protección de datos personales.

**FUENTE DE CONSULTA**

- 1. Agencia Española de Protección de Datos Personales. Disponible en el sitio web: <https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-el-derecho-la-portabilidad>
- 2. Candano Bea. Nuevo estudio de compatibilidad entre el blockchain y el GDPR. Disponible en el sitio web: <https://www.linkedin.com/pulse/nuevo-estudio-de-compatibilidad-entre-blockchain-y-el-bea-m-candano/>
- 3. Commission Nationale de l'Informatique et des Libertés Personnelles. Disponible en el sitio web: <https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles>
- 4. Constitución Política de los Estados Unidos Mexicanos. Disponible en el sitio web: [http://www.diputados.gob.mx/LeyesBiblio/pdf/1\\_080520.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/1_080520.pdf)
- 5. García Ricci, Diego, Artículo 16 constitucional. Derecho a la privacidad. Disponible en el sitio web: <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf>
- 6. Guías Jurídicas Reglamento Europeo de Protección de Datos Personales. Disponible en el sitio web: <https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEA MtMSbF1jTAAAkNjEwNjY7Wy1KLizPw8WyMDQwsDU0MTkEBmWqVLfnJIZUGqbVpiT-nEqAMUH2Hw1AAA AWKE#:~:text=Su%20principal%20objetivo%20es%20dar,materia%20de%20protecci%C3%B3n%20de%20datos.>
- 7. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Disponible en el sitio web: [http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG\\_abro.pdf](http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf)
- 8. Ocampo Muñoz, Gustavo, Nuevos desafíos para la protección de datos personales en el blockchain. Disponible en el sitio web: <https://revistas.juridicas.unam.mx/index.php/derechoinformacion/article/view/13881/15338>
- 9. Reporte de investigación, Situación. Economía Digital. Tecnología de cadena de bloques, blockchain. Disponible en el sitio web: [https://www.bbvaresearch.com/wp-content/uploads/2015/08/Situacion\\_Economia\\_digital\\_jul-ago15-Cap4.pdf](https://www.bbvaresearch.com/wp-content/uploads/2015/08/Situacion_Economia_digital_jul-ago15-Cap4.pdf)
- 10. Rodríguez Garagorri, Margarita, Análisis de tecnologías de bitcoin y blockchain, trabajo fin de máster, Universidad Oberta de Catalunya. Disponible en el sitio web: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72606/6/mrgaragorriTFM1217memoria.pdf>
- 11. Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?. Disponible en el sitio web: <https://academy.bit2me.com/que-son-los-smart-contracts>
- 12. <https://bitcoin.org/es/faq>

