COLECCIÓN

ASÍ HABLA EL EXTERNADO

3

DISRUPCIÓN TECNOLÓGICA, TRANSFORMACIÓN DIGITAL Y SOCIEDAD



DERECHO, INNOVACIÓN Y TECNOLOGÍA: FUNDAMENTOS PARA UNA LEX INFORMÁTICA

Editores:
Juan Carlos Henao
Daniel Castaño

Coordinadora general de la obra:
Constanza García Chaves

Universidad Externado de Colombia
135 Años

JUAN CARLOS
HENAO

DANIEL
CASTAÑO
Editores

DISRUPCIÓN TECNOLÓGICA, TRANSFORMACIÓN DIGITAL Y SOCIEDAD

TOMO III

DERECHO, INNOVACIÓN Y TECNOLOGÍA: FUNDAMENTOS PARA UNA LEX INFORMÁTICA

UNIVERSIDAD EXTERNADO DE COLOMBIA

Disrupción tecnológica, transformación digital y sociedad. Tomo III, Derecho, innovación y tecnología : fundamentos para el mundo digital / Diego Acosta González [y otros] ; Juan Carlos Henao, Daniel Castaño (eds.). -- Bogotá : Universidad Externado de Colombia. 2021.
1064 páginas ; 24 cm. (Así habla el Externado)

Incluye referencias bibliográficas.

ISBN: 9789587905854

1. Tecnologías disruptivas I. industria – Historia -- Innovaciones tecnológicas 2. Innovaciones tecnológicas -- Aspectos sociales 3. Ciberespacio --Aspectos sociales 4. Protección de datos -- Aspectos sociales --Innovaciones tecnológicas 5. Derecho informático -- Aspectos jurídicos – Colombia 6. Trabajo y trabajadores -- Aspectos jurídicos -- Colombia I. Henao Pérez, Juan Carlos, 1958- , editor II. Castaño, Daniel, editor II. Universidad Externado de Colombia III. Título IV. Serie

303.4833 SCDD 21

Catalogación en la fuente -- Universidad Externado de Colombia. Biblioteca. MLV.
abril de 2021

ISBN 978-958-790-585-4

© 2021, JUAN CARLOS HENAO Y DANIEL CASTAÑO (EDS.)
© 2021, UNIVERSIDAD EXTERNADO DE COLOMBIA
Calle 12 n.º 1-17 este, Bogotá
Teléfono (57 1) 342 0288
publicaciones@uexternado.edu.co
www.uexternado.edu.co

Primera edición: abril de 2021

Diseño de cubierta: Departamento de Publicaciones
Corrección: José Ignacio Curcio Penen
Composición: Precolombi EU-David Reyes
Impresión y encuadernación: Xpress Estudio Gráfico y Digital S.A.S. - Xpress Kimpres
Tiraje de 1 a 1.000 ejemplares

Impreso en Colombia
Printed in Colombia

Prohibida la reproducción o cita impresa o electrónica total o parcial de esta obra, sin autorización expresa y por escrito del Departamento de Publicaciones de la Universidad Externado de Colombia. Las opiniones expresadas en esta obra son responsabilidad de los autores.

TERESA GENOVEVA VARGAS O.*

La cadena de bloques y su importancia en el derecho probatorio

The blockchain and its importance in evidence law

RESUMEN

La tecnología de cadena de bloques ha suscitado especial interés para el derecho debido a sus características técnicas robustas, pero poco se ha avanzado sobre la forma como impactará el derecho procesal, y en particular, en la evidencia digital. En consecuencia, esta investigación aborda la categoría jurídica que ocupa la *blockchain* en el ordenamiento y su análisis como medio de prueba, objeto de prueba y medio para la preservación de pruebas. Además, se presentan las particularidades de los contratos inteligentes frente a la trasformación de la sana crítica estática a la sana crítica dinámica, gracias a la automatización.

PALABRAS CLAVE

Cadena de bloques, contratos inteligentes, evidencia digital, prueba electrónica, sana crítica dinámica, interpretación judicial.

ABSTRACT

The Blockchain technology has attracted particular interest to the law because of its robust technical features, but little progress has been made on how it will impact on procedural law, and in particular, on digital evidence. Consequently, this research the legal category that *blockchain* occupies in the legal system and its analysis as means of evidence, object of evidence and preservation of evidence. In addition, the particularities of intelligent contracts are presented, opposed to the transformation of healthy static criticism to healthy dynamic criticism for the automation.

KEYWORDS

Blockchain, smart contracts, digital evidence, electronic evidence, healthy dynamic criticism, judicial interpretation.

SUMARIO. Introducción. I. La tecnología de cadena de bloques. A. Concepto, fundamentos y arquitectura. B. Principios esenciales. C. Tipos de cadena

---

* Doctora en Derecho. Directora del Departamento de Derecho Informático y Nuevas Tecnologías de la Universidad Externado de Colombia. Correo-e: teresa.vargas@uexternado.edu.co.

de bloques. D. Cuestiones problemáticas. 1. El debilitamiento del protocolo por un ataque del 51%. 2. Rompimiento del consenso. II. La inmersión de la innovación en el derecho probatorio. A. El derecho probatorio y la inmersión del mensaje de datos. B. La tecnología *blockchain* como evidencia digital. III. De la cadena de bloques a los contratos legalmente inteligentes. A. La automatización de la voluntad. B. De la sana crítica estática a la sana crítica dinámica. Conclusiones. Bibliografía.

INTRODUCCIÓN

La tecnología *blockchain* ha adquirido una importancia trascendental en los últimos diez años, puesto que desde que apareció su primer prototipo a modo de criptoactivo, se han proyectado diversas modificaciones técnicas que hacen de esta tecnología una innovación que trasciende el sector financiero.

Los desarrollos en la materia pueden llegar a facilitar el proceso de análisis probatorio del intérprete judicial, al aplicar la tecnología al derecho. En ese sentido, el uso de *blockchain* agilizará el proceso judicial y permitirá contar con medidas de confiabilidad e integridad de la información, de suerte que sirva para preservar la evidencia digital desde la perspectiva de medio y objeto de prueba.

Aunque la cadena de bloques carece de regulación en Colombia, es esa su característica estrella, en tanto que su funcionamiento en el registro y almacenamiento supone un reto jurídico que aún está en debate. En ese orden de ideas, si se quiere brindar validez a lo almacenado en ella, se requiere una figura de autoridad que vale la pena tener en cuenta, ya que en Colombia no se ha llevado a cabo ningún cambio legislativo que aborde la cuestión. Por tanto, para probar en juicio la autenticidad de un documento estampado en *blockchain*, en caso de ser impugnado el valor probatorio, se debe proponer una prueba pericial, salvo que existan jueces que conozcan el funcionamiento de dicha tecnología. Respecto a este último punto no parece que se vaya a tardar demasiado, ya que simplemente se requeriría que un juez compruebe una estampación en cualquier verificador online, de cualquier *blockchain*.

La tesis planteada no es extraña, ya que en derecho comparado existen casos interesantes y recientes, por ejemplo Italia y el estado de Washington, donde se ha normativizado el reconocimiento de la Tecnología de Registro Distribuido (DLT) y la validez jurídica de sus sellos de tiempo, entre otras cuestiones.

Aunque en Colombia la tecnología *blockchain* aún no tiene ningún reconocimiento jurídico *sui generis*, más allá de la discusión que se ha venido dando respecto de los *smart contracts* y los desafíos a los vacíos de control gubernamental, conviene considerar el efecto que tendrán esas nuevas tecnologías en el perfeccionamiento de los negocios jurídicos.

Una particularidad que no existe en ninguna prueba basada en *blockchain* consiste en que su validación está dada por la contribución indirecta de diversas personas desconocidas y desinteresadas en su contenido, las cuales, por conducto de la programación de máquinas, validan el registro de un hecho o acto ocurrido en un determinado día y hora. A diferencia de cualquier otra prueba, en *blockchain* la actuación humana se da de forma escalonada por personas ajenas a lo que fue registrado y al propio registro que validan, de forma que quienes realizan ese proceso son las máquinas, que actúan de forma progresiva en la confirmación sucesiva de cada validación realizada anteriormente, garantizando una seguridad incorruptible.

Al final, la trazabilidad registrada en la prueba de cadena de bloques está constituida de forma automatizada por el procesamiento de las máquinas de minería que realizan todo el proceso de validación del sistema, mas no una actuación humana directa en que la persona entra en contacto con el contenido, el hecho y lo evalúa, para luego determinar la validación o no de su registro.

En el escrito se abordan los aspectos fundamentales de la cadena de bloques y la evidencia digital con el propósito de hallar un punto de encuentro entre la tecnología *blockchain* y el derecho probatorio. El concepto de mensaje de datos es determinante para explicar la legalidad en el uso de un libro distribuido, como prueba en el proceso, en donde, además de exponer sus bases normativas y jurisprudenciales, se hace referencia a los dilemas que surgen alrededor de la integridad del documento electrónico.

I. La tecnología de cadena de bloques

Uno de los retos más recurrentes al momento de abordar la innovación desde una perspectiva jurídica consiste en el entendimiento del abogado de la tecnología en sí misma. Más allá del componente regulatorio o de interpretación judicial, corresponde entender la evolución tecnológica y los principios prácticos de la innovación concreta de estudio. De ahí la importancia de dedicar un apartado a la explicación de la cadena de bloques y las dificultades que suscita desde la perspectiva técnica.

A. concepto, fundamentos y arquitectura

Por lo general, la definición de *blockchain* se resume en indicar que es un libro mayor distribuido que permite realizar la trazabilidad de operaciones; sin embargo, "[e]s engañoso percibir la tecnología *blockchain* solo un libro contable [...] es también algo más que la suma de sus partes" (Mougayar, 2017: 25). De manera que para entender la definición y dimensión de la cadena de bloques es necesario abordar sus componentes lógico y jurídico, a fin de determinar lo que significa ser una arquitectura fiable e íntegra.

En primer lugar, hay que decir que *blockchain* es un protocolo informático que tiene una base técnica importante, en tanto que implementa criptografía y algoritmos particulares para su funcionamiento, lo que lo clasifica como una "base de datos *back-end* que mantiene un libro mayor distribuido abiertamente" (Mougayar, 2017: 36).

Los programas informáticos comprenden una arquitectura de carácter centralizado, lo que significa que los componentes se encuentran alrededor del sistema y se conectan de forma central. Sin embargo, los avances de la web semántica permiten referirse a la existencia de componentes en sistemas distribuidos, los cuales forman una red de componentes conectados sin requerir de elementos centrales de coordinación. Ese es el caso de esta tecnología, ya que "todas las cadenas de bloques, como la que usa *blockchain*, están distribuidas, es decir, se ejecutan en ordenadores que ofrecen voluntariamente personas de todo el mundo" (Tapscott et al., 2018: 29).

En otras palabras, las personas no cuentan con un registro único de la información que le da sustento a la base de datos del sistema, sino que existen múltiples copias en la red de usuarios que dificultan su alterabilidad. De ahí su integridad, en el entendido de que un usuario único no podrá alterar el registro, si no es con el consenso de todos los usuarios del sistema.

Bajo esa noción técnica, *blockchain* es un conjunto de tecnologías que lo dotan de las propiedades que lo caracterizan, entre ellas, el avance de la estructuración de bases de datos, la aplicación de programación en *software*, la interconexión entre equipos y la criptografía. Si no fuera por el avance en el procesamiento de datos y la codificación matemática de la información que ha traído la primera década del siglo XXI, la cadena de bloques no podría ser lo que es hoy.

Así las cosas, conviene tener en cuenta que la cadena de bloques comprende una doble dimensión, puesto que se requiere separar los requerimientos técnicos del sistema, de la definición enmarcada en las necesidades del usuario,

en donde cabría la noción jurídica. Respecto de esta última hay que decir que la cadena de bloques "tiene un evidente significado ideológico y político disruptivo" (González Meneses, 2017: 19), puesto que su origen se remonta al movimiento anarcocapitalista de los años 50, de acuerdo con el cual, el liberalismo económico y el rechazo al Estado propendían a encontrar un mecanismo para lograr la descentralización económica, que se concretó más adelante con el movimiento criptoanarquista y mediante diversos manifiestos en los años 90.

Además, esta noción de descentralización y registros distribuidos en una sociedad no son nuevos, ya que en las Islas Yap, al interior de Micronesia, existe ese esquema en una moneda culturalmente ancestral en la sociedad yapese: se trata de una piedra circular, denominada rai, cuya trazabilidad se lleva de forma manual por un libro presente en cada una de las familias. Al hacerse un intercambio, se efectúa una ceremonia en la que se realiza la anotación de trazabilidad en cada libro prescindiendo de la necesidad del intercambio material de las piedras rai (Cora, 1975).

Entonces, se ha delimitado el concepto jurídico empresarial de la cadena de bloques para indicar que se trata de una "[r]ed de intercambio para mover valores entre iguales [y sirve de] mecanismo de validación de transacciones que no requiere asistencia de intermediarios" (Mougayar, 2017: 36). Ello es una consecuencia del estampado cronológico y la firma, que han sido antecedente de protocolo de seguridad en aspectos digitales.

Al final, la cadena de bloques viene a emular la idea de Internet, pero aplicando una corrección de fiabilidad; sin embargo, hay que tener claro que "no hay paradigmas previos para la tecnología *blockchain* [...] No es una nueva versión de TCP/IP" (Mougayar, 2017: 38), sino que se trata de la interconexión que la red ofrece para compartir un registro entre varios nodos del sistema.

B. PRINCIPIOS ESENCIALES

Como parte del desarrollo, la comunidad descentralizada ha esbozado una serie de principios esenciales con que cuenta la tecnología *blockchain* y que son fundamentales para entender el porqué de su expansión. La cadena de bloques tiene como base los siguientes principios:

a) *Integridad de la red*: al ser una plataforma con cifrado, en todas las etapas del proceso, y gracias al esquema de consenso de la red, el riesgo de cometer fraudes es prácticamente nulo;

b) *Poder distribuido*: no hay una autoridad central, en su lugar lo que se tiene es una red entre iguales que vela por la transparencia del sistema;

c) *El valor como incentivo*: cada uno de los nodos que mantienen el funcionamiento de la red recibe un incentivo como estímulo por su participación;

d) *Seguridad*: el sistema cuenta con un diseño que garantiza la confidencialidad y autenticidad de las operaciones;

e) *Privacidad*: las personas controlan sus propios datos en la cadena de bloques, ni siquiera se necesita conocer la verdadera identidad de los participantes porque lo que importa es la operación;

f) *Derechos preservados*: los derechos adquiridos por intermedio del esquema de *blockchain* son legítimos para la red que la conforma, e inalienables, en la medida en que es información irreversible, y

g) *Inclusión*: la tecnología ayuda a eliminar las brechas y amplía el acceso.

Además, estos principios tienen un punto de encuentro coherente con los principios generales de la prueba judicial, por lo que no basta quedarse con los principios del desarrollo técnico de *blockchain*, sino que es necesario mencionar la aplicación de lo trazado por el derecho procesal. En *blockchain* la noción de prueba se ve envuelta por los siguientes principios expuestos por Parra Quijano (1998):

a) *Veracidad*: la mayor virtud de la cadena bloques es su potencial para reconstruir los hechos, por lo que es posible definir una trazabilidad de operaciones relevantes para atender a un conflicto jurídico;

b) *Libre apreciación*: el juez realizará un juicio de convicción del sistema que, a través de la aplicación de la sana crítica, conlleve al convencimiento de los hechos;

c) *Libertad probatoria*: esta tecnología tiene la capacidad de probar circunstancias o hechos de cualquier naturaleza, por lo que, gracias a la libertad probatoria de los medios de prueba, será posible aportarla;

d) *Publicidad*: la cadena de bloques se caracteriza por el alcance social de su desarrollo y gestión. Todos los miembros de la red construyen los hechos y preservan su existencia, lo que aumenta el grado de persuasión judicial;

e) *Necesidad de la prueba*: el juez no se puede basar en su propia experiencia para fallar, motivo por el cual requiere de medios de prueba que lo lleven al convencimiento de los hechos alegados. Si bien la tecnología es un reto de interpretación, otorga un mayor grado de probabilidad respecto de los hechos que requieren ser probados, y

f) *Contradicción*: debido a la naturaleza de la cadena de bloques, resulta todo un desafío la aplicación del derecho de defensa y de contradicción; sin embargo, la interpretación que se proponga respecto de los medios técnicos puede ser debatida.

C. TIPOS DE CADENA DE BLOQUES

Si bien el primer prototipo de cadena de bloques que se conoció fue el de Bitcoin (el cual tiene una naturaleza pública), es posible adaptar el diseño a las necesidades específicas de un proyecto. De manera que la doctrina ha distinguido prototipos de cadena respecto de los permisos y acceso a la red: i) cadena de bloques pública; ii) cadena de bloques semiprivada, y iii) cadena de bloques privada.

Así pues, la cadena de bloques más popularizada es la de carácter público, la cual es totalmente descentralizada respecto del acceso a su base de datos y el ingreso a la red. Mientras la cadena de carácter semiprivado o de consorcio comprende la unión de varias entidades o participantes a fin de que el proceso de consenso sea controlado por un conjunto específico de nodos.

Por su parte, la cadena de bloques privada hace uso de las bondades tecnológicas de *blockchain*, pero propende a la centralización, de tal suerte que el objetivo es facilitar procesos de transparencia y autoría en una correcta gobernanza corporativa (Lu, 2018).

En ese orden de ideas, es posible evidenciar que si bien la naturaleza de *blockchain* es la descentralización, el protocolo cuenta con características de flexibilidad que permiten ajustar el algoritmo a las necesidades específicas de la red o de la compañía que lo requiera. No obstante, hay que tener en cuenta que ello se debe prever desde el diseño que da lugar a la arquitectura tecnológica, puesto que para alterar la naturaleza de una cadena de bloques se requiere el consenso de los nodos que la integran, situación que en la práctica no ocurre, por lo que, cuando hay desacuerdos, proporcionan fenómenos de bifurcación de la red.

D. CUESTIONES PROBLEMÁTICAS

El funcionamiento de la red presente en la cadena de bloques está revestido de una presunción de integridad, puesto que "[c]omo ya explicaba Nakamoto en su paper, los nodos honestos no van a validar transacciones irregulares, es decir, firmadas por una con una clave privada que no es correspondiente a la clave pública el beneficiario de la transacción que se pretende gasta"

(González-Meneses, 2019: 96). Sin embargo, ello no significa que sea ajena a los ataques o fraudes informáticos, por lo que se deben tener presentes los riesgos de seguridad del sistema, aunque las probabilidades de ocurrencia sean bajas.

1. El debilitamiento del protocolo por un ataque del 51%

La principal característica de una cadena de bloques está dada por el algoritmo de consenso establecido en el diseño del sistema, lo cual significa que todos los participantes de la red deben cumplir unas reglas específicas sin que una autoridad central tenga que intervenir. De manera que, cuando uno de los nodos infringe el acuerdo establecido en el algoritmo es excluido de la red y los otros nodos no validan sus operaciones. No obstante, cuando un nodo se hace a más del 51% del consenso, se estaría ante el riesgo de alterar el mecanismo de validación descentralizado.

Así lo señala la doctrina, al indicar que "si se quiere falsear la cadena de bloques es necesario tener al menos la misma capacidad de cálculo que el resto de la red y un tanto más para poder generar bloques falsos y darlos por ciertos en la red" (Márquez Solís, 2016: 360), lo que quiere decir que si se tiene control de más del 50% de la red se podrían validar operaciones que no son ciertas y romperse la cadena de bloques verídica cambiándola por una ilusoria. Para generar esta situación se debe crear una cadena completamente aislada de forma privada y luego presentarla de forma genuina dentro de la red como si fuera una cadena más larga (Sayeed y Marco-Gisbert, 2019: 361).

Un caso como este ocurrió en 2014 con el *pool* de minería Ghash.IO, que alcanzó un poder computacional en la cadena de Bitcoin equivalente al 40% de la red y se convirtió en una situación que encendió el debate. En su momento se indicó que una solución a la vulnerabilidad de ese tipo de consenso era obligar a que el procesamiento no implicara solo poder computacional, sino criptoactivos de alta prioridad, pues de no ser así, "si un *pool* realiza un ataque de este tipo no sería demasiado difícil averiguar su origen, más aún es un tipo de ataque que va en contra del interés económico del mismo atacante" (Márquez Solís, 2016: 361), en razón a que el costo del procesamiento para apoderarse de la red no sería proporcional a la ganancia que obtendría haciéndolo posible.

Sin embargo, pese a la estrategia planteada, preexiste el riesgo de denegación del servicio distribuida a través de un ciberataque, de manera que se inhabiliten los nodos de la red para participar en la confirmación de las operaciones presentes en la cadena de bloques. Por ello, nuevos prototipos de

blockchain buscan utilizar nuevos mecanismos de consenso y no el originado por Bitcoin, en donde se popularizó el *proof of work* (Márquez Solís, 2016).

2. Rompimiento del consenso

Como regla general, la tecnología descrita impide que un nodo pueda reversar operaciones o, reconstruir la historia de la cadena por el código de tiempo en cada bloque que lo enlaza con el anterior e impide el rompimiento de la cadena, pero puede darse una circunstancia de bifurcación que ponga en riesgo la integridad de una cadena pública de bloques; significa que existen desacuerdos dentro de las comunidades de *blockchain* que conducen a una división de la cadena.

Ahora bien, desde la perspectiva técnica, "[u]na bifurcación de *blockchain* se refiere a un cambio en las reglas de *blockchain* que efectivamente conducen a una separación en dos o más caminos potenciales" (Islam et al., 2019), circunstancia que puede ser temporal o permanente.

Un primer caso es el denominado *soft-fork*, el cual se da cuando hay una actualización del *software* del sistema: si existe un número de nodos que han actualizado el *software*, pero otros que no lo han hecho, la cadena de bloques se divide entre la versión 0 y la versión 1 del sistema. Para que se ajusten las operaciones de la actualización se tiene que alcanzar consenso con suficiente potencia de procesamiento de la red, pues de lo contrario la bifurcación falla y la cadena original continúa, lo que significa que se excluirían las operaciones realizadas o verificadas por los nodos actualizados.

En segundo lugar, el llamado *hard-fork* implica crear una nueva cadena de bloques separada, pero con base en la anterior existente. En esa medida, ambas cadenas de bloques funcionan en paralelo, pero con un conjunto diferente de reglas, ya que este mecanismo obedece a "problemas agudos, como el aumento del tamaño del bloque, el abuso grave de la red y el robo" (Islam et al., 2019).

De modo que se puede evidenciar la existencia de vicisitudes que se deben revisar en la interpretación judicial de una situación problemática, en la medida en que cada cadena de bloques tiene características, actores y reglas diferentes.

II. La inmersión de la innovación en el derecho probatorio

La aparición de los medios magnéticos y la evolución de la digitalización llevó a que se empezaran a presentar nuevos medios de prueba al proceso judicial,

de forma que las fotografía que antes se presentaban en formato físico, ahora se aportan en formato electrónico; las cartas escritas de puño y letra, o incluso a máquina, ahora se aportan en conversaciones de aplicaciones de mensajería instantánea; y los contratos que se firmaban y expresaban la voluntad en el tenor de las palabras, ahora se pueden expresar en clicks y se describen en términos de algoritmos y datos.

Acorde con este proceso que trae implícita la Cuarta Revolución Industrial, el Código de Procedimiento Civil generalizó los medios de prueba, entre los cuales no se excluyen los mensajes de datos, y se han venido dando bases legales y jurisprudenciales al respecto.

A. El derecho probatorio y la inmersión del mensaje de datos

El análisis de la prueba consiste en ir más allá de lo jurídico: así, se trata de estudiar la forma en que se hace valer el derecho sustancial mediante el derecho procesal, en el cual los medios de prueba son determinantes para que el juez analice la información que lo lleve al convencimiento de los hechos en el desarrollo del proceso (Ramírez Contreras, 2019). En esa medida, la evidencia es un elemento del proceso que permite construir inferencias a partir de las cuales el juez realiza un ejercicio intelectual que lo lleva al convencimiento para tomar una decisión mediante lo que se ha definido como un ejercicio racional.

En consecuencia, la doctrina está dividida respecto de lo que debe ser considerado tema de prueba: por un lado está la teoría de acuerdo con la cual el objeto de prueba son los hechos, y, por otro, la teoría que indica que el objeto de prueba son las afirmaciones de los hechos.

Es una discusión que se trae a colación porque es preciso delimitar lo que realmente se pretende al incorporar pruebas digitales al proceso. Si la parte aspira a probar las afirmaciones de los hechos (Devis Echandía, 1994), la prueba digital no sería idónea porque las manifestaciones que se dan de los hechos son de carácter subjetivo o interpretativo y difieren de lo que efectivamente expone la prueba digital, en tanto que esta presenta circunstancias de modo, tiempo y lugar, de hechos concretos y verificables. Por tal razón, el objeto de prueba son los hechos, como todas aquellas realidades que tienen trascendencia jurídica (Parra Quijano, 2006), función que cumple la incorporación de la evidencia digital aportada durante el proceso.

Lo anterior encuentra sentido con lo que indica el artículo 177 del Código de Procedimiento Civil colombiano, actual artículo 167 del Código General del

Proceso, de acuerdo con el cual, "incumbe a las partes probar el supuesto de hecho de las normas que consagran el efecto jurídico que ellas persiguen" (Ley 1564 de 2012). Por lo que en Colombia lo que se prueba son los hechos y no las afirmaciones sobre los hechos.

Al final, la verdad será aquella que el actor logre probar a través de los medios de prueba allegados al proceso judicial[1], y frente a ellos la autoridad judicial realiza un juicio de coherencia mediante el cual evalúa el grado de probabilidad de acertar en que los hechos aludidos son verdaderos.

Ciertamente, gracias al avance de la ciencia y la tecnología se ha dado una evolución de los medios de prueba. De hecho, fue la imprenta la que permitió la existencia del documento que ha venido evolucionando como concepto jurídico, a través de la historia, hasta llegar al documento electrónico (Vargas Osorno, 2016).

En el argot jurídico colombiano las primeras nociones de documento electrónico aparecieron en el artículo 251 del Código de Procedimiento Civil, que señalaba que documento se tienen todo objeto mueble de carácter representativo o declarativo, dentro del cual encajaban los soportes electrónicos o máquinas informáticas.

Luego, la Ley 527 de 1999 introdujo el concepto de mensaje de datos para referirse a que son admisibles como medios de prueba, y que su fuerza probatoria está dada por el Código de Procedimiento Civil, hoy Código General del Proceso, de suerte que si bien la legislación ya reconocía los documentos electrónicos como objetos muebles, al ordenamiento ingresó un nuevo concepto que brinda mayor seguridad jurídica respecto de "la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares" (Ley 527 de 1999, art. 2.º).

Como resultado del avance legislativo, el artículo 243 del Código General del Proceso destaca el mensaje de datos como un tipo de documento, y desarrolla su valoración probatoria. De acuerdo con el artículo 247, los mensajes de datos "deben ser valorados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que los reproduzca con exactitud", lo que entra en contradicción con el parágrafo del mismo artículo que indica que la simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos.

---

1 Son medios de prueba aquellos instrumentos que suministran al juez conocimiento sobre los hechos que integran el tema de prueba.

Por tal razón, para realizar un ejercicio de interpretación especial y entender cómo se debe aportar el mensaje de datos en el proceso judicial, se debe acudir a la Ley 527 de 1999, que en su artículo 11 indica que los mensajes de datos tienen fuerza probatoria y que para su apreciación se aplica la sana crítica. Sin embargo, el artículo 8.º indica que cuando se aporta como medio de prueba el original, la integridad del documento electrónico "está dada por la conservación de la información desde que se generó por primera vez en su forma definitiva" (Ley 527 de 1999), motivo por el cual, no sería válida la impresión en papel del mensaje de datos, por no presentarse en el mismo formato de origen.

La cuestión de la impresión del mensaje de datos fue resuelta por la Corte Constitucional, entendiendo que "no es aquí allegada al trámite como un verdadero mensaje de datos, sino como una impresión del mensaje de datos, de ahí que el legislador le otorgue también un tratamiento diferente en términos de su apreciación como evidencia" (Sent. C-604 de 2016), lo que significa que la impresión tiene un tratamiento diferenciado respecto del original en medio magnético.

En ese contexto, y gracias a la expansión de las tecnologías de la información y las comunicaciones, se empieza a moldear el concepto de mensaje de datos, ligado a la prueba digital como

> … aquella que permite acreditar hechos a través de los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase (Isaza, 2015).

De esa manera, para definir su eficacia probatoria el mensaje de datos debe ser susceptible de distinguir el soporte que lo integra, el contenido y su autor, ya que lo que finalmente se quiere representar es un hecho que ha tenido consecuencias jurídicas y se encuentra descrito en un componente lógico o digital.

Si bien el artículo 244 del Código General del Proceso indica que se presumen auténticos los mensajes de datos, en los casos en que el documento electrónico no sea fácilmente comprensible en lenguaje natural por sus características técnicas complejas, será necesario un perito técnico informático que certifique la autenticidad, cronología y procedencia del mensaje de datos.

Al respecto, la Corte Constitucional ha indicado que los mensajes de datos son medios de convicción y su fuerza probatoria es la otorgada a los documentos en general por el Código General del Proceso. No se le puede

negar capacidad demostrativa, efectos o validez jurídica por el solo hecho de tratarse de información en esa clase de soporte o por no haber sido presentada en su forma original.

El juez tendrá que ejercer la sana crítica para determinar la confiabilidad de la modalidad de conservación de la integridad de la información, y la efectiva identificación de las partes dentro del soporte. Al final, serán las técnicas utilizadas en el mensaje de datos las que aseguren la inalterabilidad, rastreabilidad y recuperación del contenido de los mensajes de datos.

B. LA TECNOLOGÍA *BLOCKCHAIN* COMO EVIDENCIA DIGITAL

La tecnología *blockchain* ha llegado como una plataforma innovadora que ha generado un alto grado de disrupción en la sociedad. Algunos autores lo definen como "una base de datos apoyada en tecnología *peer to peer* y por tanto compartida por múltiples nodos" (Tur Faúndez, 2018: 33), mientras que otros la ven como un "mecanismo de validación de transacciones que no requiere asistencia de intermediarios" (Mougayar, 2017: 36). No importa la definición que se acoja, el concepto de cadena de bloques puede ser tan amplio como la actividad que sobre el mismo se desarrolle.

Su aparición, por conducto de las criptomonedas, llevó a que los Estados fomentaran políticas de exploración y observación respecto de esta nueva tendencia tecnológica. Es claro que si bien las criptomonedas están basadas en la cadena de bloques, esta no se refiere únicamente a criptomonedas. Por el contrario, la integración de las bases de datos, la prueba de trabajo y el encriptamiento de la información dieron sentido al desarrollo de un protocolo que trasformará la sociedad.

En ese orden de ideas, la doctrina ha denominado a las *blockchain* como "protocolo fiable", porque se trata de una plataforma global con la que es posible operar de modo seguro, pues "nunca había habido transacciones fiables entre dos o más partes autenticadas por la colaboración de muchos y posibilitadas por intereses colectivos" (Tapscott et al., 2017: 16). El carácter innovador y el modelo abierto apuntaron a que se desarrollaran diversas clases de cadenas de bloques, con características particulares.

Por tal razón, *blockchain* promete convertirse en uno de los medios de prueba más importantes en los próximos años, especialmente por la noción de consenso, la cual es base estructural de la confianza distribuida y la participación colectiva en la validación de las operaciones. Ello ha llevado a que se considere como un sistema íntegro e inmutable, puesto que debido a las

condiciones de seguridad (Tur Faúndez, 2018: 34), se convierte en un medio de prueba ideal para llevar al juez a la convicción de los hechos.

Es por eso que se presenta la capacidad que puede llegar a tener la tecnología de cadena de bloques en el sistema judicial, en tanto que el "registro *blockchain* es un medio para documentar contenidos muy diversos, que puede servir como medio de prueba semejante a los documentos, en la medida en que los jueces consideren a la cadena (y sus partes) como un instrumento de carácter documental" (Ibáñez Jiménez, 2018).

La evidencia forense aplicada a la tecnología *blockchain* puede ser vista desde dos ángulos diferentes: 1. El aporte de un libro mayor distribuido al proceso judicial, para probar afirmaciones de los hechos o como objeto mismo de prueba, y 2. Considerar a *blockchain* como un mecanismo para preservar evidencias judiciales. El primer punto, observando la naturaleza de mensaje de datos y su aporte al proceso, y la segunda, como una herramienta al servicio de la integridad de las pruebas.

De modo que la cadena de bloques cuenta con una doble naturaleza jurídica: como medio de prueba y objeto de prueba, en tanto que puede ser presentada en el proceso judicial para evidenciar la existencia de un acuerdo o negocio jurídico, o un debate judicial respecto de la autenticidad de la cadena de bloques en sí misma.

En todo caso, la cadena de bloques puede ser presentada en el proceso judicial, ya que se trata de un documento electrónico que encaja en el ordenamiento jurídico como mensaje de datos y a partir de esa idea se tendrá que dar la interpretación judicial.

De hecho, la prueba aportada como cadena de bloques será un documento en forma de mensaje de datos que se ajusta a los términos del artículo 167 del Código General del Proceso colombiano. Las partes deben indicar que el hecho que quieren probar está descrito en un libro distribuido, y tendrá que aportar una de las copias para el expediente.

Lo anterior implica considerar las reglas existentes respecto de las limitaciones de apreciación probatoria, en particular el artículo 33 de la Constitución Política de Colombia y el artículo 8.º de la Ley 906 de 2004 (Código de Procedimiento Penal), en relación con el derecho a no ser obligado a declarar contra sí mismo, en los casos en que el mensaje de datos implique un testigo de acreditación. También se debe tener en cuenta el artículo 209 de la Constitución Política, ya que, si ha mediado alguna relación profesional con la cadena de bloques, aunque esta sea pública, podría estarse ante excepciones del deber de dar testimonio.

No se puede olvidar que la naturaleza abierta del libro distribuido flexibiliza la aplicación del derecho a la intimidad del artículo 15 de la Carta Política, toda vez que la parte que ha aceptado ceñirse a un negocio jurídico utilizando *blockchain* podría estar renunciando a la información derivada del acuerdo que pasa al dominio público. No habría limitaciones de acceso probatorio a una cadena de bloques de carácter público (como lo puede ser el protocolo Bitcoin) porque el artículo 74 de la Carta Política establece el acceso a la información pública.

El aporte de *blockchain* debe ser conducente, pertinente y útil, lo cual significa que debe haber idoneidad legal respecto de la copia del libro distribuido para probar el hecho que se aduce y efectivamente hacerlo. Aportar la totalidad del libro sería incoherente con la pertenencia y utilidad de la prueba, pues basta con el apartado que presente la operación que incumbe a las partes y su trazabilidad.

Es posible que se excluya a *blockchain* como medio de prueba en algunos aspectos sometidos a la tarifa legal, como ocurre respecto del caso del estado civil de las personas, que se debe probar a través del registro civil de nacimiento; si en el futuro el Estado decide elevar ese registro a un libro distribuido, la tarifa legal podría cambiar.

Al tratarse de una tecnología de características técnicas complejas se requiere un mayor grado de apreciación del juez, lo que se expresa en un ejercicio de investigación y análisis que justifique su convencimiento para emitir el fallo. De manera que se requiere exaltar la sana crítica como proceso de raciocinio, en donde existe un método de investigación científica correlacional al conocimiento jurídico del juez. Después de todo, "el juez debe asumir un plan para abordar el caso que se le somete a estudio" (Ramírez Contreras, 2019: 31).

Dentro de ese proceso intelectual se sugiere abordar una metodología que reconozca el estado del arte de los desarrollos tecnológicos de *blockchain*, y su concatenación con la exposición de los hechos a lo largo del proceso judicial. Se debe identificar la cronología de las vicisitudes y el momento exacto en que interviene la trazabilidad de la cadena de bloques.

El juez debe entender la correcta aplicación de la norma general (en el caso colombiano la relacionada con el mensaje de datos, como documento) y analizar minuciosamente las hipótesis presentadas por las partes. El ejercicio judicial no se debe limitar a analizar la cadena de bloques aportada en el proceso, sino aplicar la sana crítica respecto de todos los medios de prueba. No hay que olvidar que el registro en *blockchain* es solo una herramienta dentro del conflicto jurídico llevado a la jurisdicción.

En otras palabras, el juez tendrá que evaluar no solo la prueba que se deriva de la cadena de bloques, sino todas aquellas que se relacionen con el conjunto de hechos concatenados con el conflicto jurídico. Por ejemplo, en un negocio jurídico que genera contienda y se utiliza la evidencia digital en *blockchain*, solo se presenta la operación realizada, pero no se ahonda en otros elementos importantes como el consentimiento, el cual es elemento esencial en el negocio jurídico.

Cuando en los hechos que se quieren probar se relaciona una cadena de bloques, es necesario revisar la pertinencia de acudir a un perito experto que ilustre al juez acerca de los elementos técnicos del libro distribuido. En ese sentido, la Sentencia C-604 de 2016 de la Corte Constitucional colombiana se refiere al mensaje de datos para indicar que no se debe acudir a un perito cuando se reúnan las siguientes condiciones: i) si la información respectiva es accesible para su posterior consulta; ii) si el documento es conservado en el formato en que se haya generado, enviado o recibido, y iii) si se conserva toda la información que permita determinar el origen, el destino, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento, pues en esos casos no es necesario ahondar en los aspectos técnicos, toda vez que los mecanismos del medio de prueba garantizan su integralidad, inalterabilidad, rastreabilidad, recuperación y conservación.

Mediante esa sentencia la Corte explica que, por ser un mensaje de datos, la prueba digital de *blockchain* no requiere de un perito experto, puesto que ella misma brinda esos elementos de integralidad, inalterabilidad, rastreabilidad, recuperación y conservación.

Al ser *blockchain* una tecnología con altos estándares de cifrado imposibles de alterar, es incensario acudir a un perito experto que compare el documento original con el aportado en el proceso, incluso el registro de *blockchain* podría ser revisado y contrastado en cualquiera de las otras copias disponibles dentro de la red.

Con los estándares técnicos tradicionales existe la posibilidad de controvertir la integridad del mensaje y la trasmisión de la información mediante la tacha de falsedad y el desconocimiento del documento, pero con la tecnología de cadena de bloques se estaría ante un nuevo mecanismo que garantizaría el sellamiento del mensaje.

En relación con ello, en la Sentencia del 16 de diciembre de 2010, Rad. 2004-01074, la Corte Suprema de Justicia indicó:

> [Que] La integralidad de la información tiene que ver con que el texto del documento transmitido por vía electrónica sea recibido en su integridad por el destinatario, tarea que puede cumplirse técnicamente utilizando el procedimiento conocido como "sellamiento" del mensaje, mediante el cual aquel se condensa de forma algorítmica y acompaña al mensaje durante la transmisión, siendo recalculado al final de ella en función de las características del mensaje realmente recibido; de modo, pues, que si el mensaje recibido no es exacto al remitido, el sello recalculado no coincidirá con el original y, por tanto, así se detectará que existió un problema en la transmisión y que el destinatario no dispone del mensaje completo.

Así que el inconveniente realmente vendría a darse con la rastreabilidad del mensaje de datos, puesto que ello podría dificultar relacionar una parte con la operación realizada a través del libro distribuido. Una de las características de esa tecnología es la anonimidad. No habría inconveniente alguno si ambas partes reconocen su participación en la operación descrita en *blockchain*, pero si la situación problemática se da respecto de la operación misma y de *blockchain*, como un medio de prueba en donde la participación fue anónima o pseudoanónima, será necesario acudir a otro medio de prueba que satisfaga dicho requerimiento y permita establecer un nexo entre el demandando y su intervención en la cadena de bloques.

En algunos casos ello es posible con la ayuda de medios técnicos a través del análisis de tráfico TCP/IP, en donde es posible determinar el origen de una transacción en algunas cadenas de bloques como, por ejemplo, la del protocolo Bitcoin (Márquez Solís, 2016). Sin embargo, se han desarrollado otros protocolos de cadena de bloques que envuelven un enrutamiento del tráfico que impide identificar a las partes[2], y por ende, hacen imposible la rastreabilidad tanto del emisor como del receptor.

Ahora bien, habría que diferenciar entre las cadenas de bloques abiertas y cerradas, puesto que si estamos ante un *legal smart contract* puede que las partes no tengan acceso a la copia del libro distribuido, caso en el cual se debe solicitar en la demanda o contestación de la demanda, a fin de que el juez, en el auto que decreta pruebas, solicite al responsable de la administración de la cadena de bloques, copia auténtica de las operaciones correspondientes o un certificado que lo manifieste.

---

2 A través del uso de múltiples servidores y la encriptación en cada paso del camino.

Lo descrito hasta aquí alude a *blockchain* como medio de prueba pero, desde otra perspectiva, si el objeto de prueba es *blockchain*, será imprescindible contar con el aporte de dictámenes periciales que ilustren al juez acerca de la verdadera naturaleza que implica la cadena de bloques a la que aluden las partes. Ahora, si ambas partes están de acuerdo en cuanto a la copia aportada al proceso, se podría practicar la prueba de común acuerdo, delegando su práctica a un tercero en el que confíen ambas partes[3]. El testimonio experto del administrador de la cadena de bloques o el aporte de varias copias del libro distribuido permitirían cotejar la integridad o no de lo aportado por las partes.

Como consecuencia de la participación de un perito se tendrá que realizar un análisis forense en materia computacional que estudie las redes que emplea la cadena de bloques y su sistema estructural. Para tal fin se deben cumplir los protocolos establecidos en la materia, lo que implica evitar la contaminación, actuar metódicamente, controlar la cadena de evidencia y ceñirse a los principios de la informática forense. A diferencia de la evidencia digital tradicional, la tecnología *blockchain* elimina algunas barreras de análisis, puesto que esta prueba no es volátil, duplicable, alterable o modificable, como ocurre con las pruebas electrónicas regulares.

Pero es menester hacer claridad respecto de que para administrar la evidencia digital es necesario mantener el ciclo de vida, en tanto que las etapas de diseño, producción, recolección, análisis, reporte y presentación de la prueba digital son vitales para que el intérprete judicial llegue al efectivo convencimiento de la naturaleza, características y hechos que se han dado respecto de la cadena de bloques (Caballero Velasco y Cilleros Serrano, 2018).

Para finalizar se aborda uno de los temas más prácticos y técnicos en la materia, en consideración a que *blockchain* puede solucionar aspectos de conservación de integridad probatoria. El desarrollo de una cadena de bloques en el área de la cadena de custodia probatoria permite identificar, recolectar y preservar las pruebas digitales, lo que facilita la celeridad y economía procesal.

Se han desarrollado diversos mecanismos para identificar, tomar y preservar las pruebas digitales, pero prevalecen los inconvenientes respecto de una autoridad que garantice la seguridad de la evidencia digital y su cadena de custodia. Aunque útiles, las pruebas en forma de mensaje de datos tienen la característica de que pueden ser fácilmente manipulables y no existe un

---

3 Es una forma de aplicar lo establecido en el artículo 190 del Código General del Proceso.

esquema que avale la celeridad y la economía procesales, lo que todavía hace necesario acudir a peritos que certifiquen la integridad de la prueba.

En esa medida, el proceso mismo de aporte probatorio se ha quedado atrás frente a los avances tecnológicos; sin embargo, cada contexto tiene realidades diferentes y un sistema de evidencia digital que puede conllevar riesgos de seguridad, razón por la cual se deben evitar las vulnerabilidades en los sistemas de almacenamiento y custodia probatoria con el fin de impedir que los atacantes las puedan explotar y alterar de forma maliciosa la evidencia.

Una cadena de bloques destinada a este propósito debe tener:

1. *Escalabilidad*, en la medida que permita la gestión de gran cantidad de archivos;

2. *Integridad*, para que la evidencia no pueda ser modificada después de enviarla al sistema;

3. *Validez*, tratándose de una prueba coherente;

4. *Privacidad*, respecto del acceso restringido a solicitantes no autorizados, y

5. *Trazabilidad*, rastreando la fuente de la evidencia (Tian et al., 2019).

Al final lo que se pretende con la tecnología de cadena de bloques en el ámbito probatorio es mantener y documentar la historia cronológica del manejo de evidencia digital, en la medida en que registra de forma minuciosa cada detalle en el procesamiento de la prueba, desde el primer respondiente, las autoridades de investigación y el escenario judicial (Lone y Mir, 2019). Tal vez el mayor reto sea la conservación de la integridad de los datos, porque los datos digitales son susceptibles de ser alterados con facilidad; es el problema de la manipulación en medio del proceso de cadena de custodia.

Por ello se requiere de un sistema que se acomode a la inmaterialidad de la evidencia digital y se pueda integrar correctamente con otros sistemas de información. La tecnología de cadena de bloques puede garantizar la autenticación y verificación de datos almacenados, de manera que se pueda certificar la consistencia de los datos y su preservación.

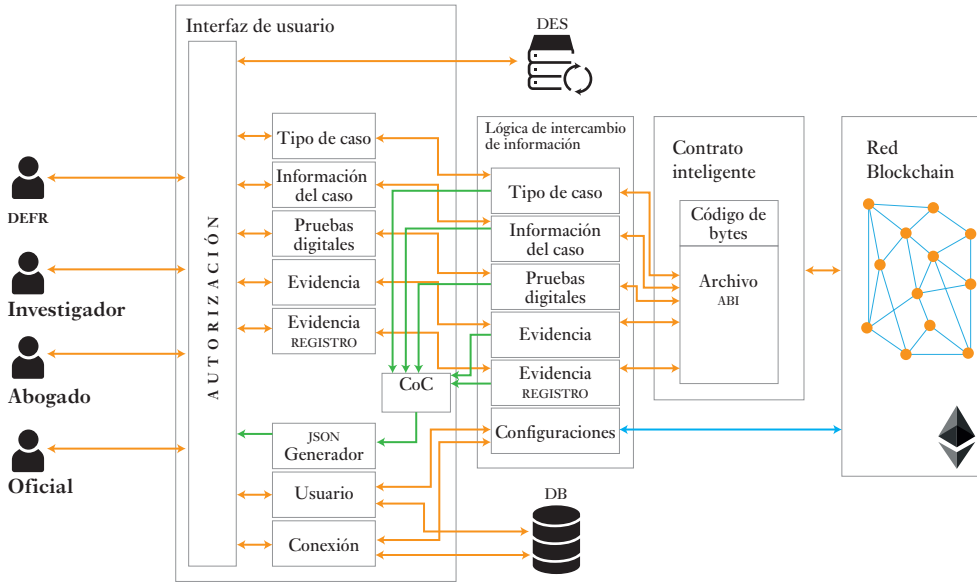
Se ha desarrollado un prototipo que pone lo descrito en práctica. Se trata de un piloto que combina la tecnología *blockchain* con el enfoque de Gabinetes de Evidencia Digital (DEC)[4], desarrollando un Gabinete de Evidencia Digital Blockchain (B-DEC), lo que sirve de herramienta para recolectar y producir evidencia electrónica.

---

4 Digital Evidence Cabinets (DEC).

Lo anterior funciona gracias a la implementación de un sistema basado en una red privada de Ethereum, que emplea el sistema tradicional de *hash* y el mecanismo de consenso *proof of authority*[5] para verificar transacciones. De esa forma, se puede contar con un sistema electrónico de cadena de custodia para la evidencia digital que no requiere de un minero ni de altas especificaciones de computación.

FIGURA 1. PROTOTIPO DE CADENA DE CUSTODIA



Modelo de Gabinete de Evidencia Digital Blockchain (B – DEC)

Fuente: Yunianto et al. (2019).

La imagen presenta el prototipo propuesto por una investigación publicada en la *Revista Internacional de Aplicaciones Informáticas*, en el que se describe el modelo de Gabinete de Evidencia Digital Blockchain (B-DEC) con cuatro interacciones dentro de la arquitectura.

En primer lugar, el *frontend*, que funciona como una interfaz que contiene la autorización de los derechos de acceso y comunicación para desarrolladores, investigadores, abogados y jueces. En segundo lugar, el *middleware* como etapa

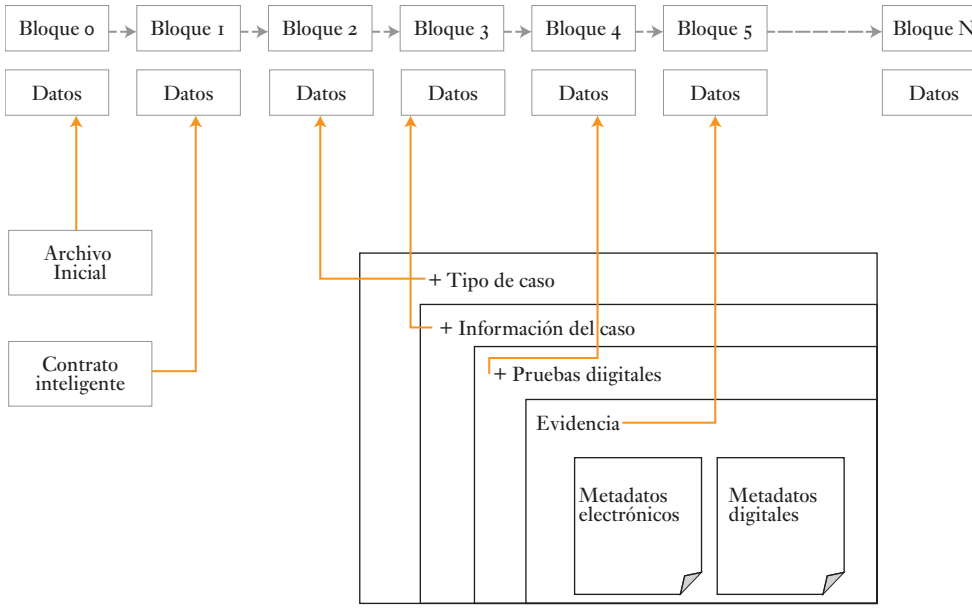
5 Hay diferentes sistemas de consenso en la tecnología de cadena de bloques. Algunos de los más recurrentes son: prueba de trabajo (PoW), Prueba de pila (PoS), PBFT, DPOS, Ripple y Tendermint.

de traducción entre la interfaz y el contrato inteligente, que conforma la tercera fase de *smart contracts*, en la que el contrato inteligente interactúa con la red de Ethereum y hace parte del contrato escrito en lenguaje de programación adaptado a las necesidades del usuario, para terminar con la *blockchain network* que sirve de red privada construida con Ethereum Virtual Machine (EVM) en transacciones de periodos interconectados.

Dentro del *frontend* están las autorizaciones para acceder al tipo de caso (*cabinet*), la información almacenada para cada caso (*rack)*, la escena del crimen y el almacenamiento de datos de las pruebas digitales (*bag*), y los registros técnicos necesarios para el funcionamiento del sistema.

En otras palabras, cada gabinete descrito de manera técnica dentro de la cadena de bloques tiene la capacidad de almacenar la evidencia digital de un caso. La gestión de la prueba por medio de este mecanismo permite localizar los elementos con facilidad y permitir o negar el acceso de las autoridades o las partes del proceso. Lo anterior se describe en la siguiente figura.

FIGURA 2. EVIDENCIA DIGITAL EN UNA CADENA DE BLOQUES



Fuente: Yunianto et al. (2019).

De esa manera se pueden diseñar esquemas de almacenamiento de evidencia digital que faciliten la actividad investigativa y judicial en los procesos. Si bien el prototipo descrito está en fase de desarrollo y aún requiere mejoras, la

arquitectura permite ajustar las necesidades de gestión de la evidencia digital y los documentos de la cadena de custodia a cada realidad jurídica.

En otro sentido se están desarrollando proyectos que integran el Internet de las cosas a la tecnología de cadena de bloques para abordar los desafíos en el ámbito forense del proceso de recolección, preservación e investigación de evidencia. Dado que cada vez hay más hogares integrados a "una serie de mecanismos instalados en la puerta de enlace de una casa inteligente, como creación de perfiles, monitoreo, y detección de anomalías" (Brotsis et al., 2019), se puede extraer evidencia digital para las actuaciones maliciosas.

Es el caso de la cadena de bloques CyberTrust, la cual pretende que los datos recopilados en los dispositivos del Internet de las cosas se almacenen en una base de datos de evidencia a cargo del proveedor de servicios de Internet (ISP). De esa forma los metadatos sobre ataques son almacenados en una cadena de bloques de orden cronológico. A través de este esquema se permite el acceso de entidades de investigación, como las autoridades de policía o los fiscales encargados, quienes adelantan la tarea de contexto, conservando la cadena de custodia y la historia cronológica del manejo de la evidencia digital.

Una cadena de bloques con este uso facilitaría la detección de intrusos en los sistemas informáticos, además de garantizar la recopilación y posterior correlación de evidencia forense de varias fuentes independientes. No es un secreto que, en la realidad judicial, el delito de acceso abusivo a los sistemas informáticos presenta dificultades para su investigación, en especial por las dificultades de evidencia digital respecto de la identificación del atacante, motivo por el cual *blockchain* ayudaría a mejorar la efectividad judicial en la que se involucren ataques mediante el uso del Internet de las cosas.

Aunque efectivo, un sistema de esta magnitud conlleva desafíos en materia de confidencialidad de la información, por lo que se debe establecer un protocolo que garantice la confidencialidad e integridad de las pruebas forenses durante la transmisión y el almacenamiento, y asegure la evidencia recolectada en sistemas seguros de información que requieran autenticación.

Así las cosas, se demuestra que *blockchain* tiene un amplio potencial como mecanismo de almacenamiento de elementos probatorios de carácter digital. Las características de su diseño tecnológico y la seguridad que ofrece, podrían llegar a impactar el sistema judicial de los próximos años.

En el estado actual no es posible utilizar mecanismos como el propuesto. Si bien el artículo 103 del Código General del Proceso invita a usar las TIC en el proceso judicial, este se refiere a las actuaciones judiciales de acuerdo con el Plan de Justicia Digital y no a los mecanismos de almacenamiento de las

pruebas. Sin embargo, según el parágrafo 3 del mismo artículo, si el Consejo Superior de la Judicatura establece que *Blockchain* es un sistema fiable para enviar, trasmitir, acceder y almacenar mensajes de datos, para el intercambio y acceso de información en el sistema judicial, podría darse vía libre a su implementación en el marco del Plan de Justicia Digital.

III. DE LA CADENA DE BLOQUES A LOS CONTRATOS LEGALMENTE INTELIGENTES

Una vez expuesto el análisis que tendrá lugar cuando el juez deba interpretar una prueba basada en *blockchain*, vale la pena referirse a la interpretación jurídica en caso de que las pruebas sean innecesarias por establecerse un mecanismo automatizado predefinido de hecho y consecuencia jurídica.

A. LA AUTOMATIZACIÓN DE LA VOLUNTAD

Desde el primer prototipo se tenía previsto que el diseño de cadena de bloques admitiera "una gran variedad de posibles tipos de transacciones […] Operaciones de fideicomiso, contratos vinculados, arbitraje de terceros, firma multiparte, etc." (Swan, 2015). De forma que no es extraño que hoy se haga referencia a contratos inteligentes para aludir a la automatización de múltiples negocios jurídicos como expresión del principio de autonomía contractual.

Sin embargo, se debe hacer claridad en cuanto a que el término contrato inteligente debe ser tomado con cautela, en el entendido de que es de naturaleza técnica y no jurídica. La noción del concepto viene dada por los desarrollos de la *blockchain* y se refiere a un elemento estructural del sistema. De manera que se puede diseñar un contrato inteligente sin que respecto de él se presenten partes u obligaciones contractuales, por lo que el concepto de *smart contract* se limita a las secuencias de código y datos, pero en realidad, "la categoría jurídica de contrato no existirá en tanto no se cumplan los requisitos que la ley exige para su validez y ello con independencia de la mayor o menor complejidad del programa que pueda, en su caso, formar parte del mismo" (Tur Faúndez, 2018: 51 y 52).

Entonces, en los negocios jurídicos se podrá prescindir del aspecto probatorio si las partes delegan el estudio de los elementos probatorios a un sistema automatizado y descentralizado basado en *blockchain*, que se conecte con los elementos externos para asignar consecuencias jurídicas concretas. Bajo ese supuesto el juez no tendría que estudiar un título ejecutivo expreso, claro y

exigible para emitir el mandamiento de pago, sino que el sistema de cadena de bloques lo autoejecutaría y descontaría el pago, evitando así congestionar el sistema judicial.

El valor jurídico de esta idea proviene del principio *pacta sunt servanda*, el cual se refiere a que lo pactado es ley entre las partes, aunque solo aplica al negocio jurídico, puesto que los terceros no pueden intervenir en la cadena de bloques, en tanto que no se representan a sí mismos como nodos dentro del *legal smart contract*.

En esa medida los contratos automatizados con el uso de la cadena de bloques podrán prescindir del accionar judicial, pero los terceros de buena fe conservan su derecho a exponer ante la administración de justicia cuestiones problemáticas referidos a dicho negocio jurídico, en el entendido de que no hacen parte del *pacta sunt servanda* establecido entre las partes.

B. De la sana crítica estática a la sana crítica dinámica

El artículo 176 del Código General del Proceso señala que las pruebas deben ser apreciadas en conjunto y de acuerdo con las reglas de la sana crítica, de manera que el juez tiene un margen de entendimiento propio que obedece al ejercicio de su función judicial, siempre que exponga razonadamente el mérito que le asigne a cada prueba.

En la jurisprudencia constitucional la sana crítica se identifica como "la interdicción de la arbitrariedad y la corrección de lo racional y razonable" (Sentencia C-202 de 2005), de modo que obliga al juez a dar las razones del fallo que emite, e implica la convicción del juez, que es razonada en el fallo del caso concreto.

De acuerdo con lo anterior, podría tenderse a una flexibilización del principio de la sana crítica en la apreciación de las pruebas frente a *blockchain*, en la medida en que las partes les resten importancia a los medios de prueba presentados ante el juez, y depositen su buena fe en lo que arroje el algoritmo del contrato legalmente inteligente con el objetivo de automatizar las prestaciones y las consecuencias del incumplimiento. Sin embargo, la sana crítica "no siempre ha sido entendida de la misma manera. En ella se ha verificado una suerte de movimiento pendular que la ha llevado desde la más completa libertad de ponderación judicial [...] hasta su identificación con principios y conocimientos objetivos de naturaleza científica" (Benfeld, 2015).

En tal sentido, habría una transformación del principio de la sana crítica en el que ya no es el intérprete judicial quien estudia y analiza los medios de prueba, sino que se trata de una sana crítica dinámica que se prevé por diseño y por defecto en la cadena de bloques que registra los datos del contrato legalmente inteligente.

CONCLUSIONES

La tecnología *blockchain* es una de las tecnologías emergentes con mayor grado de disrupción en la última dácada, pues se ha involucrado en diversos sectores de la sociedad, y el derecho ha sido uno de los últimos eslabones en ahondar esfuerzos para su desarrollo. El panorama general de *blockchain* indica que se debe diferenciar su doble naturaleza conceptual: la primera en sentido técnico, pues es así como nace dicha tecnología, pero también una segunda en sentido social, en la que el derecho impacta en mayor medida.

También, a lo largo del texto se expuso cómo la cadena de bloques es medio de prueba y objeto de prueba válido en el proceso judicial colombiano, en tanto que se caracteriza como un documento en forma de mensaje de datos que debe ser interpretado por el juez en el ejercicio de la sana crítica, en tanto que se debe tratar de un medio de prueba que cumpla con los criterios de pertinencia, conducencia y utilidad.

Si el libro distribuido es lo suficientemente claro no se requerirá de intérprete o perito que ilustre al juez respecto de lo aportado, sino que las características de confiabilidad, infalibilidad y seguridad de la tecnología de cadena de bloques son suficientes para presumir la integridad de la información contenida. No obstante, las partes pueden aportar una copia del libro distribuido o ponerse de acuerdo en cuanto al aporte de una única copia, pero, en virtud de su oficiosidad, el juez podría contrastarla con las otras copias disponibles.

El caso difiere cuando la cadena de bloques es objeto de prueba, puesto que allí se cuestiona su validez, en cuyo caso se requerirá de expertos que lleven al convencimiento acerca de los hechos verdaderos conforme a los criterios de análisis técnico.

Las características de la cadena de bloques permiten que sea una tecnología eficaz para la preservación de la evidencia judicial. Actualmente se están desarrollando algunos prototipos que permitirían utilizar la integración de capas operativas que almacenen las pruebas, conforme a las realidades sociales y, además, cuenten con un mecanismo de autenticación que facilite la actividad investigativa y judicial en los procesos, con una marca de trazabilidad.

Habrá que atender al desarrollo de la materia para abordar los diversos desafíos jurídicos que surjan, lo que se puede ilustrar con la trasformación del negocio jurídico a través de la implementación de contratos legalmente inteligentes, circunstancia en la cual el avance de la informática jurídica al servicio del derecho podría automatizar las prestaciones y la apreciación de los medios de prueba en ejercicio de una sana crítica dinámica. Empero, mientras no se llegue a ello como una realidad masificada socialmente, las instituciones y normas existentes en derecho probatorio son suficientes para enfrentar los litigios que involucren a la tecnología *blockchain*.

BIBLIOGRAFÍA

Benfeld, J. "Una concepción no tradicional de la sana crítica", *Revista de Derecho*, Valparaíso, 45, 2015, 153-176, disponible en [https://doi.org/10.4067/s0718-68512015000200006].

Brotsis, S. et al. "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments", 2019, disponible en [http://arxiv.org/abs/1903.10770].

Caballero Velasco, M. Á. y D. Cilleros Serrano. *El libro del hacker*, Anaya Multimedia, 2018.

Cora, G. *The Stone Money of Yap: A Numismatic Survey*, vol. 23, Smithsonian Institution Press, 1975.

Devis Echandía, H. *Compendio de derecho procesal civil*, 8.ª ed., Biblioteca Jurídica Diké, 1994.

González-Meneses, M. *Entender Blockchain: una introducción a la tecnología de registro distribuido*, 2.ª ed., Thomson Reuters Aranzadi, 2019.

González Meneses, M. "Entender Blockchain: una introducción a la tecnología de registro distribuido", 2017, disponible en [http://search.ebscohost.com/login.aspx?direct=true&db=cat05988a&AN=uec.252650&site=eds-live].

Ibáñez Jiménez, J. W. "Cuestiones jurídicas en torno a la cadena de bloques (*blockchain*) y a los contratos inteligentes (*smart contracts*)", *Revista Icade. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales*, 0(101), 2018, disponible en [https://doi.org/10.14422/icade.i101.y2017.003].

Isaza, H. E. "La prueba electrónica y el sistema interamericano", 2015, disponible en [http://search.ebscohost.com/login.aspx?direct=true&db=cat05988a&AN=uec.238602&site=eds-live].

Islam, A. K. M. N.; M. Mäntymäki y M. Turunen. "Why do blockchains split? An actor-network perspective on Bitcoin splits", *Technological Forecasting and Social Change*, 148, 2019, disponible en [https://doi.org/10.1016/j.techfore.2019.119743].

Lone, A. H. y R. N. Mir. "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer", *Digital Investigation*, 28, 2019, pp. 44-55, disponible en [https://doi.org/10.1016/j.diin.2019.01.002].

Lu, Y. "Blockchain and the related issues: a review of current research topics", *Journal of Management Analytics*, 5(4), 2018, 231-255, disponible en [https://doi.org/10.1080/23270012.2018.1516523].

Márquez Solís, S. "Bitcoin: guía completa de la moneda del futuro", 2016, disponible en [http://search.ebscohost.com/login.aspx?direct=true&db=cat05988a&AN=uec.244353&site=eds-live].

Márquez Solís, S. *Bitcoin guía completa de la moneda del futuro*, Ediciones de la U., 2016.

Mougayar, W. *La tecnología blockchain en los negocios : perspectivas, práctica y aplicación en Internet*, Ediciones Anaya Multimedia, 2017.

Parra Quijano, J. *Manual de derecho probatorio*, 8.ª ed., Librería Ediciones del Profesional, 1998.

Parra Quijano, J. *El documento electrónico y su alcance probatorio*, Bogotá, Universidad Externado de Colombia, 2006.

Ramírez Contreras, L. F. *Evidencia y prueba la construcción de las inferencias*, Legis, 2019.

Sayeed, S. y H. Marco-Gisbert. "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack", *Applied Sciences*, 9(9), 2019, 1788, disponible en [https://doi.org/10.3390/app9091788].

Swan, M. "Blockchain", *O'Reilly Media*, 2015, disponible en [http://shop.oreilly.com/product/0636920037040.do].

Tapscott, D. et al. "La revolución blockchain: descubre cómo esta nueva tecnología transformará la economía global", 2018, disponible en [http://search.ebscohost.com/login.aspx?direct=true&db=cat05988a&AN=uec.250020&site=eds-live].

Tapscott, D.; A. Tapscott y J. M. Salmerón. *La revolución blockchain : descubre cómo esta nueva tecnología transformará la economía global*, Deusto, 2017.

Tian, Z.; M. Li, M. Qiu, Y. Sun y S. Su. "Block-def: A secure digital evidence framework using blockchain", *Information Sciences*, 491, 2019, 151-165, disponible en [https://doi.org/10.1016/j.ins.2019.04.011].

Tur Faúndez, C. "Smart contracts: análisis jurídico", en C. Tur Faúndez. *Smart contracts : análisis jurídico*, Universidad de las Islas Baleares, Editorial Reus, 2018.

Vargas Osorno, T. G. *Bancos de datos jurídicos: pasado, presente y futuro*, Madrid, Universidad Complutense de Madrid, 2016.

Yunianto, E.; Y. Prayudi y B. Sugiantoro. "B-dec: Digital Evidence Cabinet based on Blockchain for Evidence Management", *International Journal of Computer Applications*, 181 (45), 2019, pp. 22-29, disponible en [https://doi.org/10.5120/ijca2019918580].

Congreso de la República. Ley 527 de 1999.

Congreso de la República. Ley 1564 de 2012.

Corte Constitucional. Sentencia C-202 de 2005, M. P.: Jaime Araújo Renteria.

Corte Constitucional. Sentencia C-604 de 2016, M. P.: Luis Ernesto Vargas Silva.

Corte Suprema de Justicia. Sentencia Rad. 2004-01074 de 2010, M. P.: Munar Cadena, Pedro Octavio.

Universidad Externado de Colombia
135 Años

La tercera edición de la colección "Así habla el Externado" examina el impacto que las tecnologías disruptivas y la transformación digital están teniendo sobre el conjunto de la sociedad, bajo una lente humanista e interdisciplinar, propia de nuestra institución. La Cuarta Revolución Industrial (4RI), que ha permeado todos los campos de la actividad humana y la sociedad, ofrece la inmensa oportunidad de reducir las brechas de conocimiento e ingreso económico y generar progreso social y democrático, pero puede también tener el efecto contrario. El lector y la lectora encontrarán en estos cuatro tomos reflexiones valiosas, en sus 74 escritos, para comprender en todo su alcance estas innovaciones y poder contribuir así a la construcción de realidades cada vez más incluyentes y participativas.

* * * * *

Este tomo III, titulado "Derecho, innovación y tecnología: fundamentos para una *Lex Informática*", tiene por objeto responder la siguiente pregunta: ¿de qué manera las nuevas tecnologías y la economía colaborativa están transformando el derecho, sus principios e instituciones? Para ello, el presente volumen estudia en detalle las promesas, retos y problemas jurídicos suscitados por la aplicación de la inteligencia artificial, el *Big Data*, el *Blockchain* y el *IoT* en distintos ámbitos del derecho público y privado. Los diferentes capítulos presentan debates en torno a la forma en que dichas tecnologías vienen afectando profundamente al mundo del derecho, con el fin de construir un marco conceptual que no solo sirva de base para sostener una discusión académica sólidamente fundamentada sobre estos temas, sino también para despejar las dudas jurídicas que pueden existir con el fin de facilitar y acelerar el desarrollo e implementación práctica de estas tecnologías, así como de contribuir a orientar la agenda académica sobre estos asuntos en América Latina.