Blockchain Y Derecho Civil
Blockchain and Civil Law

Por: **David Ellister Zamora S.**
Universidad de Panamá
Facultad de Derecho y Ciencias Políticas
Panamá
david_z_s@hotmail.com
https://orcid.org/0000-0002-8781-1222
DOI https://doi.org/10.48204/j.aderecho.n53.a4860
Entregado: 31 de mayo de 2023

Aprobado: 3 de agosto de 2023

Palabras claves: *blockchain*, cadena de bloques, datos, derecho civil, *hash*, nodos, mineros, prueba de trabajo.

Keywords

Blockchain, data, civil law, hash, nodes, miners, proof of work.

1. Introducción

La disruptiva tecnología *blockchain* como medio para atribuir valor a la *internet*, introduce un cambio de paradigmas en ciertos aspectos sociales y económicos. En principio, fue creada como un sistema de pagos electrónicos basado en pruebas criptográficas, las criptomonedas, y poco a poco su funcionalidad ha resultado de interés para el derecho, debido a los distintos efectos jurídicos que ocasiona su utilización.

Abordaremos algunos antecedentes y evolución del *blockchain*, su definición y características, cómo se genera un bloque y se incorpora en la cadena, su utilidad en la vida cotidiana, así como también cierta problemática que ocasiona la conformación de una cadena de bloques.

Introduction

The disruptive blockchain technology as a means of attributing value to the Internet introduces a paradigm shift in certain social and economic aspects. In principle, it was created as an electronic payment system based on cryptographic evidence, cryptocurrencies, and little by little its functionality has become of interest to the law, due to the different legal effects caused by its use.

We will address some background and evolution of the blockchain, its definition and characteristics, how a block is generated and incorporated into the chain, its usefulness in daily life, as well as certain problems that cause the formation of a chain of blocks.

2. Antecedentes y evolución

Para congeniar la trayectoria entre los antecedentes y la evolución de la tecnología disruptiva *Block-chain,* iniciamos con la publicación del artículo: *"Bitcoin: A Peer-to-Peer Electronic Cash System"* del 31 de octubre de 2008, mejor conocida como *"The Bitcoin whitepaper"*, atribuida a la persona o grupo denominado Satoshi Nakamoto, documento curioso por su paradójico seudo-anonimato y por relevar información para que algún programador pudiera crear un sistema similar al allí propuesto.

En ese entonces, el propósito de la red de bloques era masificar una versión de moneda puramente electrónica que permitiera que los pagos fuesen enviados directamente a los participantes, sin la intervención de alguna institución financiera.

Su filosofía se fundamentaba en la prevención del doble-gasto, proponiendo la implementación de una red de usuario-usuario (*Peer to Peer: P2P*), es decir, una premisa de descentralización auspiciada por firmas digitales encriptadas de los propios participantes, para así prescindir de los terceros de confianza.

De tal modo, *blockchain* comparte su origen con la aparición del *Bitcoin* (₿)[1] en enero de 2009 (Falbo y Di Catelnuovo, 2019; Mora y Palazzi, 2019), es decir, la primera criptomoneda (Arecha, 2019; Marqués-Pascual y Sintes-Olivella, 2020), manteniéndose como constante entre las

[1] En cuanto a los antecedentes del *Blockchain:* el *B-money* fue una propuesta temprana creada por *Wei Dai* para un sistema de efectivo electrónico anónimo y distribuido en 1998. Primera referencia de las consultadas por Satoshi Nakamato.

monedas virtuales y la más popular en la actualidad[2], pero más que por usanza, destacó por su seguridad e inmutabilidad al momento de registrar las transferencias.

Ahora bien, los antecedentes de la red *blockchain* se remontan a la invención patentada en 1979 por Ralf Merkle: *"Árboles de Merkle"*[3] (AM*),* y por otro lado, la producción de Whitfield Diffie y Martin Hellman sobre el intercambio de claves en 1976, lo que hoy en día conocemos como "criptografía"[4].

Sin embargo, la idea de encadenar información surge en 1991 de la mano de Stuart Haber y W. Scotto Stornetta, como una solución para codificar documentos digitales asignándoles un sello para que no fuesen modificados para luego agregarlos a la cadena de bloques con seguridad criptográfica, para almacenar los documentos con sello de tiempo como mecanismo de doble seguridad.

En 1992, se incorporó el diseño AM para permitir que varios documentos se reunieran en un solo bloque, pero ello no fue utilizado y la patente caducó en 2004 (*La Historia de Blockchain*, 2018).

Por ahora, diríamos de forma muy superficial, que "*blockchain"* es un árbol de datos encadenado a través de los distintos *hashes*[5], que se producen luego de implementar las claves insertadas durante la transacción, lo que se traduce a su vez en una encriptación.

---

[2] El trayecto que comprende entre los años 2007 al 2011, *Bitcoin* parecía más una leyenda urbana. Mantenía un número reducido de usuarios, lo que pareció empeorar en el año 2011, cuando se aprovechó su seudo-anonimato para figurar como la versión económica de los terroristas y otros delincuentes.

[3] Consiste en una estructura de *hash* conformado en una ramificación que evidencia ciertos datos concatenados por medio de *hashes* con el fin de verificar de forma segura que los contenidos se encuentran relacionados. "(…) se van acumulando los hashs de las transacciones contenidas en los bloques, que terminan en un único hash de todos ellos" (García Mexía, 2018, p. 54.)

[4] "La criptología es la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original. Utiliza generalmente un algoritmo matemático para cifrar datos y hacerlos ininteligibles para cualquier persona que no posea una información secreta (clave criptográfica) necesaria para el descifrado de dichos datos. La utilización de sistemas criptográficos para encriptar los mensajes permite conseguir confidencialidad de las comunicaciones electrónicas" (Camacho Clavijo, 2005, p. 527).

[5] Todos los documentos o datos digitales (archivo, video, correo electrónico, audio, etc.) son susceptibles de generar un *hash*, una especie de firma digital o resumen del dato que siempre será la misma, mientras no se modifique el documento (agregar una tilde, cambiar el membrete, etc.). La función *hash* consiste en aplicar un procedimiento matemático a un documento o conjunto de documentos determinados que da como resultado treinta caracteres aproximadamente entre letras y números, resultado que deberá ser el mismo siempre que se solicite el procedimiento sobre el -mismo- documento, siendo necesario solamente la alteración de un bit, para que este número sea diferente. Su utilidad radica en descifrar la arquitectura de un documento o dato que constituye la cadena de bloques y el modo como se almacena la información, debido a que cada bloque tiene su propio *hash* basado en la transacción.

En cuanto a su evolución, destacamos que en el 2013 se desarrolló la primera aplicación de almacenamiento seguro en *blockchain,* llamado prueba de existencia (*proof of existence*), siendo posible almacenar de manera directa los *hashes* de documentos digitales sin necesidad de utilizar espacios destinados a otros fines (Arecha, 2019). De este modo se pasó del concepto exclusivo de criptomoneda y se amplió con miras a los mensajes de datos.

Adicional a ello, como proyecto en 2013 y hecho realidad en junio de 2015, surge *Ethereum,* una cadena de bloques descentralizada con funcionalidad en contratos inteligentes, creada por el joven ruso canadiense Vitalik Buterin, lo que dio paso a la versión *blockchain* 2.0, incluyendo el pago por la creación o ejecución de un contrato inteligente en *tokens*[6] (que representan derechos sobre bienes para así automatizar procesos en los diferentes sistemas empleados).

Con una visión más de plataforma o *software* y por medio de su protocolo de *"prueba de trabajo",* se crean bloques en 15 segundos[7], ahora despegando como plataforma de negocios y actividades financieras, especialmente en Estados Unidos y Europa, sirviendo para múltiples actividades.

Actualmente se comenta de *blockchain* 3.0, con el propósito de ejecutar contratos inteligentes en *Ethereum* con el pago de *bitcoins* o similares, lo que se conoce como la verificación del pago simplificado (*Simplified Payment Verification: SPV*), el intercambio de valores entre cadenas (Hernández, Arroyo y Diaz, 2019).

3. Noción de *blockchain*

Al momento de abordar el tema de la cadena de bloques, distintos autores manifiestan una diversidad de definiciones inspiradas en sus características, en su funcionalidad o en su utilidad pragmática.

Dunayevich y Franca (como se citó en Mora y Palazzi, 2019), anotan que: "A grandes rasgos, Blockchain se puede pensar como una base de datos, una bitácora digital donde solo se puede ingresar nueva información y donde toda la existencia no se puede modificar" (p. 202).

[6] "*Originalmente, los tokens son fichas, monedas sin curso legal o recibos, que se utilizan como sustitutos de una moneda real. En el ámbito de la tecnología Blockchain, un token es un activo digital emitido por una empresa o institución que puede tener valor en sí mismo o representar cualquier activo dentro de una comunidad, como propiedades o activos financieros"* (García Mexía, p.49).

[7] Una diferencia notable entre los Bitcoin y el Ethereum, es que la primera de ellas tiene un límite de 21 millones de unidades, mientras que la segunda de ellas no tiene límite conocido hasta la fecha, aunque mantiene un límite anual de 18 millones unidades.

Por otra parte, García Mexía (2018) señala que:

> "En la tecnología Blockchain se utilizan un conjunto de protocolos y técnicas criptográficas, gracias a los cuales los datos de la aplicación y los registros de operación se constituyen como una cadena de bloques de información unidos entre sí de forma descentralizada y pública, almacenándose en unos equipos interconectados a través de una red de ordenadores distribuidos, los nodos, para evitar cualquier punto central de fallo" (p. 43).

Para Falbo y Di Castelnuovo (2019):

> "(…) es un sistema de almacenamiento de datos que utiliza una base de datos distribuida, de manera tal que toda información, contenida en ´bloques´ para el sistema, se replica idénticamente en cada computadora que interviene como un nodo, esto es, usuario y servidor al mismo tiempo" (p. 90 y 91).

O como considera Marqués-Pascual (2020): "Se trata de una enorme base de datos distribuida en múltiples ordenadores que almacena información continuamente sobre quién negocia con qué, sin que se agote nunca el espacio donde se almacena" (p. 25).

De una forma algo más tangible, Ibáñez (2018) denomina *blockchain*:

> "(…) al conjunto de soportes o máquinas que implementan este software y donde se desenvuelve su funcionamiento; y, sobre todo, a la propia red interconectada de los nodos, puntos de conexión o máquinas, que, gestionadas por personas o, en su caso, por otras máquinas de forma automática (en última instancia, claro, bajo control de personas físicas o jurídicas) configuran una red, plataforma o espacio de intercambio de información para vincular bloques o series de datos enlazados criptográficamente" (p. 20).

Es importante destacar que la cadena de bloques no destaca por almacenar datos, aunque ello sea una función consecuente de su utilización[8]. En ocasiones, ni siquiera guarda los documentos en sí, sino las transacciones, tomando en cuenta que *blockchain* funciona por mecanismos criptográficos.

[8] Regularmente solamente se almacenan los digestos criptográficos y no funciona como una nube de archivos, sino de los *hashes*, sirven para demostrar que los documentos son los originales comparándolo con los *hashes* de los documentos que los usuarios deben almacenar tecnológicamente.

La información no debe ser encriptada para ser visualizada, y su utilidad radica más bien en visualizar quién lo ha ordenado registrar, las partes que intervienen en la transacción y conocer de qué trata su contenido. Tampoco puede revisar situaciones reales, como, por ejemplo, la existencia de los objetos materiales negociados, su calidad, cantidad, etc.

Tenemos que su nombre deriva de la composición de una cadena de información representada en bloques y que se incorporan sucesivamente en el registro o bitácora, donde cada bloque guarda una directa y necesaria relación con el bloque anterior, por lo que corregir, modificar, o alterar la información contenida en la bitácora tendría que llevarse a cabo agregando una nueva información, pero ello no elimina la información anterior, porque se preserva el registro en los nodos que conforman la red como pares propios de esta tecnología distributiva (DLT: *distributed Ledger Technology* o Tecnología Libro Mayor Distribuido), un sistema descentralizado que permite llevar a cabo un flujo automatizado -tecnología en la que circulan las monedas digitales y se despliegan otras funciones como los contratos inteligentes-.

El encadenamiento de los bloques se debe a que los datos -de forma individual- se encuentran en bloques y estos a su vez están emparentados con información resumida del bloque anterior (*hash*), ocasionando al mismo tiempo una vinculación, seguridad y automatismo, lo que no es más que la ausencia de un servidor central o nodo exclusivo que se encargue del dato.

En otros términos, todos los nodos son servidores centrales, quienes a su turno reparten una copia de la información a cada uno de los nodos[9].

En ese sentido, una dirección ordenada por el iniciador para ejecutar una transacción y una dirección de destino, se integran en un bloque, que no es más que el compuesto de varios datos o transacciones que se sellan en un período corto de tiempo en toda la red (cada 10 minutos aproximadamente) (Faliero, 2017), junto con una marca de tiempo (*time stamp*) que indica el instante en que el bloque fue creado (Mora y Palazzi, 2019).

Este procedimiento convierte a *blockchain* como el complemento y valor de *internet*, que le ofrece una versión de confianza y valor por medio de la criptografía dentro del conocimiento distribuido de forma horizontal, no siendo viable pensar en el surgimiento de una nueva innovación

[9] Es una cadena de transacciones, que se van anotando en un nodo, que intenta construir un bloque con todas las transacciones que va leyendo y el primero que consigue resolver el problema matemático, su bloque forma parte de la cadena y el resto de intentos de los otros nodos se desecha. El reto solucionado se transmite por toda la red para que todos los nodos de la red tengan la misma copia del mismo conjunto de datos desde la creación del *blockchain* y garantizar la integridad de su uso.

sin su implementación.

Y es que, con la implementación de la cadena de bloques -como regla general-, no existe un modelo jerárquico entre los participantes, todos son *"pares"* y mantienen la información de forma distributiva.

Para asimilar la dinámica de la cadena de bloques como tecnología de bitácora distributiva (DLT), resulta conveniente recordar los famosos programas *Ares Galaxy, Napster* y *eDonkey*, que, si bien distan de ser similares a *blokchain*, resultan un práctico ejemplo, ya que ahí se compartían datos por medio de toda la comunidad horizontal entre pares (*peer 2 peer: P2P*): películas, videos, audios, archivos, software, etc.

Estos archivos podían ser descargados siempre y cuando, al menos uno de los usuarios mantuviera el documento requerido y se encontrara en línea. Entre sus similitudes podríamos destacar: que se realizan y comparten datos entre pares (nodos que no son más que ordenadores conectados a la red) de carácter público y mantienen información distribuida disponible para otros nodos, la exploración de archivos entre nodos y la existencia de un servidor central, etc., pero estos programas no brindaban un valor a *internet*, porque no tenían un punto de fidelidad o de valor que codificara la transacción (Ibáñez, 2018).

3.1. Generación de un bloque y su incorporación en la cadena

Conocer el funcionamiento del sistema *blockchain* no es una tarea sencilla; no obstante, cuando nos adentramos a un sistema que transforma las relaciones sociales y comerciales, al menos conviene hacer cierto enunciado de la actividad que en ella se despliega. Nos enfocaremos en las que utilizan criptoactivos.

El sistema *blockchain* debe su nombre a las etapas que debe implementar: generar un bloque para ser insertado en una cadena de homólogos.

Toda información que requiere ser agregada a la cadena de bloques nace por medio de una operación denominada *"transacción",* esta es iniciada por medio de un nodo integrado a la red, agrupándose con otras transacciones en espera para cerrar un bloque e incorporarse a la cadena.

La operación comienza cuando el nodo iniciador genera la transacción o los datos, constituyendo la creación de una información digital (también puede constituir la intención de transferir una criptodivisa o un contrato, generar una noticia, etc.), transacción que al mismo tiempo

funciona como firma digital[10] o huella digital por parte del iniciador (identificado en la gran mayoría de sus veces por un seudónimo) al introducir un cifrado criptográfico.

Esta transacción es susceptible de la función *hash*, lo que corresponde a un oficio que permite conocer la identidad digital de un dato electrónico con utilidad para reconocer que no ha sido alterado, respondiendo así al mismo contenido y a los mismos caracteres alfanuméricos, particularidad necesaria para incorporar un bloque sellado con una marca de tiempo a la cadena de bloques.

Este bloque sellado de diversas transacciones y de diferentes usuarios de la comunidad, se une a otro bloque, manteniendo como parte de su contenido el *hash* del iniciador produciendo un: *"encadenamiento"*, y así sucesivamente, cada bloque mantiene el código *hash* de su bloque precedente, lo que no puede ser modificado sin destruir la cadena, construyendo así una base de datos distribuida e inmutable: una cadena de bloques.

Esto quiere decir que, si se intenta realizar cambios a un bloque, tendrían que modificar cado uno, situación que no se daría con discreción, ya que, por tratarse de una red distributiva, los demás participantes procederían a su rechazo.

Adicional a ello, la cadena tiene un nexo entre *hashes* que los vinculan entre sí, un número arbitrario conocido como código *nonce* (*number that can only be used once*) que funciona junto con el *hash* como elemento de control que prohíbe la manipulación de la información.

Complementando lo anterior, el cálculo del *nonce* se obtiene de una prueba de trabajo (*PoW: Proof of Work*), que no es más que la labor de solucionar un problema matemático, trabajo que demanda tiempo y energía, realizado por los mineros[11]. Resuelto el problema, el nodo ganador comparte su trabajo con la comunidad para que verifiquen la solución y se tenga por correcta, para lo que se requiere de la aprobación de al menos 51% de los mineros para cada bloque, lo que se

[10] La firma digital consiste en una clave privada, generalmente es un número aleatorio de 256 bits (código binario de 256: 0 y 1) que se suelen traducir al lenguaje humano en sistema hexadecimal (en caracteres que van del 0 al 9 y de la A a la F).

[11] Se aclara que no todos los sistemas *blockchain* aplica la dinámica de los mineros.

denomina verificación en consenso[12], para después sellar y crear el bloque adhiriendo a la red[13].

Descifrar el *nonce* es una actividad que se intenta llevar a cabo por una gran cantidad de computadoras de distintas personas, que están conectadas a la red como un nodo *(hardware* y *software*), uno por uno, los *"mineros",* resolviendo una ecuación informática para luego cerrar el bloque a cambio de una recompensa.

La recompensa por resolver el problema puede variar según la red que se utiliza, por ejemplo, el *Bitcoin* ofrece 12,5 de *bictoins* recién generados, el *Etherium* ofrece 2 *Ether*, lo que en ocasiones también se remunera por comisiones voluntarias pagadas por quienes inician la transacción.

El objetivo de la recompensa es que los usuarios se motiven a suscribir sus datos por haber empleado un recurso computacional en los procesos de escaneo del *hash* y, a la vez, encuentren utilidad en la propia red para llevar a cabo sus transacciones.

En suma, cada bloque contiene: el número y la lista de las transacciones de varios usuarios, el peso del bloque, el *hash* del bloque, el hash del bloque anterior que lo vincula en cadena, la hora de creación del bloque (*time stamp*) y la transacción de recompensa por haber sellado el bloque, empero, solamente se agrega un bloque al mismo tiempo a la red.

Una vez insertado el bloque a la cadena, la idea central es que cada bloque pueda ser consultado de forma pública, dar fidelidad de los datos integrados, no sin antes que todos los que participan en la cadena revisen que la transacción es cierta por medio de los mecanismos criptográficos.

[12] "Se podría definir el consenso como el mecanismo por el cual se acuerda que un bloque puede ser incluido en la cadena. De esta forma, cada nuevo bloque que sea coherente con el histórico de la cadena será aceptado e incluido, mientras que los que no sean coherentes no lo serán. Es mediante el proceso de consenso como se decide si un bloque es coherente o no. De alguna manera, los nodos participan en la decisión sobre si incluir un bloque en la cadena o no. Esto tiene consecuencias de enorme valor, como, por ejemplo que eliminamos la necesidad de un tercero de confianza, siendo los propios nodos los que deciden qué transacciones son válidas". (Instituto Cuatrecasas, 2019, p. 301).

[13] Cada bloque es más difícil de crear que el anterior por medio de la minería, antes duraba horas y días debido a que era una tarea realizada por ordenadores caseros. Actualmente dura 10 minutos -aproximadamente-, por ser una actividad más o menos industrial a través de la masificación de servidores especializados para la minería. La incorporación de Ethereum trajo consigo el desarrollo del sistema basado en cadena de bloques públicas y contratos inteligentes, que por medio de la utilización del protocolo de *"prueba de trabajo"* se crea un bloque cada 15 segundos. Es preciso anotar que cada bloque contiene varios datos de varias transacciones. Cada bloque almacena entre 2000 a 4000 transacciones aproximadamente.

- **Las pruebas de trabajo**

Las pruebas de trabajo, en sus inicios, buscaban reducir los *spams* que se enviaban a los correos electrónicos de forma masiva y automática, y así, evitar el bombardeo y masificación de mensajes electrónicos a varias direcciones, solicitando como intercambio resolver una prueba de trabajo que no eran más que cálculos para enviar el resultado al servidor y dificultar el envío masivo de *e-mails*.

La prueba de trabajo (*proof-of-work*) busca que no sea tan fácil ni rápido producir una transacción. Es el proceso de formación de cada bloque que se necesita para cerrar y sellar el grupo de datos mediante una operación algorítmica y que proporcione como resultado un dato preexistente y específico en su contenido, lo cual funciona como su identidad numérica, procedimiento que realizan aleatoriamente los nodos[14]: "(…) exige a todos los nodos que encuentren una cifra especial vinculada a cada boque denominado "nonce" y el que lo logra es quien incorpora el próximo bloque a la cadena. Este procedimiento se denomina 'prueba de trabajo' (proofofwork, en inglés)" (Arecha, 2019, p. 69).

Este trabajo de los nodos se traduce en verificar la autenticidad de las claves con las cuales se firmaron las órdenes de transferencia, la disponibilidad de los fondos para realizarlas y así se cierra un bloque para ser incorporado en la cadena de bloques.

Para que ello no sea tan fácil, *"La prueba-de-trabajo envuelve la exploración de un valor que al calcular un hash, tal como SHA-256, el hash empiece con un número de bits en cero"* (Nakamoto, 2008, p. 3).

Esto explicado por Falbo y Di Catelnuovo (2019) consiste en escanear en búsqueda de un valor que, cuando es *hasheado*, es decir, que se genera el número que comienza con un número de cero bits, solo permita incorporar a la cadena un bloque un *hash* que comience de igual forma con en ese número determinado de ceros: "00" ó "000", "00000", con el propósito de que ese *hash* sea inferior a un determinado número.

Entonces esto crea otra capa de seguridad y de allí vienen la cantidad "0" con la que debe empezar los *hashes* de cada bloque para variar el resultado, dado que la cantidad de 0 esta predefinida por la *blockchain* y cambia cada 2016 bloques, así que variando el número al final debería encontrar algún número válido que se genere varios *hashes* hasta dar con uno que cumpla

[14] De coincidir dos o más nodos con la misma labor puede darse una *"bifurcación"*, *"ramificación"* o "*fork"* lo que posteriormente llevará a una estructura con un extremo descontinuado, lo que se conoce como: bloque huérfano.

con los requisitos, situación que dificulta alteraciones en la cadena.

- **Tipos de pruebas de trabajo**

Según la permisión de los nodos para operar en la red, existen tres tipos de pruebas de trabajo.

La primera de ellas son las permisionadas *(permissioned*) que requieren de un permiso para que el sujeto pueda utilizar la red y ejecutar como minero, por ejemplo, *Blockchain Hiperledger* (auspiciada por la Fundación Linux y un consorcio entre las que se encuentran IBM, Intel, J.P. Morgan y American Express) y el sistema de liquidación de transacciones desarrollado por el Banco suizo, Deutche Bank y Santander, etc.; la red de pagos de JP Morgan: Interbank Information Network, que por lo general tienen algún mecanismo de control, ya sea para el acceso de la *blockchain* por los antiguos participantes a los nuevos, o bien por medio de ciertas restricciones al momento de realizar una transacción o una prueba de trabajo (Marqués-Pascual y Sintes-Olivella, 2020), reservada a ciertos nodos autorizados, lo que resulta muy paradójico con relación al sistema de las criptomonedas que utilizan el sistema de criptografía asimétrica pública para realizar la transferencia.

Por otro lado, están las no permisionadas *(permissionless)* cuyo *software* puede ser descargado y ejecutado con una computadora conectada a *internet*, insertándose como un nuevo minero en la red, por ejemplo, las cadenas de bloques de las monedas electrónicas no requieren de permisión para integrase como nodo (*Bitcoin, Ethereum, Dash,* etc.).

Por último, existen cadenas de bloques híbridas, donde una es pública dirigida al consumidor y otra es autorizada para transacciones corporativas detrás de escena.

En otro orden de ideas, es importante destacar que los *blockchain*, en esencia, presentan la misma dinámica, pero en cuanto al sellado del bloque la estrategia puede variar, por lo que los nodos deben acordar su "mecanismo de consenso" para incorporar el bloque a la cadena, aunque lo ordinario sería que todos compitieran como pares para lograr sellar el bloque.

Esto quiere decir que no todos los *blockchain* adoptan la misma manera del sistema *bitcoin* de selección, en donde el primer minero que resuelva la operación matemática es el encargado de agregar el próximo bloque, situación que ha llevado a la doctrina a enlistar algunas modalidades de las pruebas de trabajo (Arecha, 2019; Santiago y Palazzi, 2019):

1. Prueba de trabajo útil (*proof-useful-work*): necesita una prueba de trabajo utilizada para resolver problemas reales, haciendo referencia al sistema *Primecoin* que utiliza las pruebas de trabajo para encontrar secuencias de números primos con ciertas características.
2. Prueba de participación (*proof-of-stake*): la red selecciona un nodo para confirmar la validez de la nueva información enviada a la cadena de bloques, en función de su participación proporcional en la red, en el que muchas veces se considera a aquellos nodos que tienen mayor cantidad de criptomonedas, lo que evidencia que tienen especial interés en la subsistencia de la plataforma *blockchain, PeerCoin*.
3. Prueba de participación delegada (*delegated proof-of-stake*): los participantes en la red pueden delegar su cuota de participación a un representante, en el que se permite que la red pueda controlar quienes son sus representantes, y así, evitar una excesiva centralización debido a la acumulación de riquezas. Aquí los usuarios eligen a su delegado y testigos para cerrar y verificar los bloques por medio del voto electrónico según el historial de la actividad presentada (*Steem, Bitshares,* etc.).
4. Prueba de autoridad o Prueba de gasto (*proof-of-burn*): este protocolo requiere que el nodo realice directamente un gasto emitiendo una transacción a una dirección cuya clave secreta no se conoce, por lo que no se recupera el dinero, lo que equivale a su destrucción.
5. Prueba de depósito (*proof-of-deposit*): en lugar de gastar, el nodo debe enviar el gasto a una dirección donde quedará depositada por algún tiempo.
6. Prueba de autoridad (*proof-of-autorithy*): donde ciertamente algunos nodos están autorizados para sellar el bloque, turnándose entre ellos para agregar a la cadena, estos que no son los habitualmente utilizados para las monedas digitales. En este sistema existe una limitación de quienes pueden validar los bloques. Podría decirse entonces que los nodos certificadores son internos y, en efecto, centralizados (ejemplo: Blockchain Federal Argentina)[15].

[15] Este *blockchain*, junto con Alastria de España, si bien son permisionados, son asemejadas a una tercera categoría de "semipúblicas", puesto que sus actividades no son lucrativas, su ingreso es indiscriminado (multisectoriales), pero por otro lado, la facultad de registrar los bloques es selectiva y reservada por los autorizados (prueba de trabajo de autoridad).

Es importante destacar lo anterior, dado que a la luz del crecimiento del sistema de bloques, se han creado diferentes métodos para aceptar la formación y validez de un bloque mediante la prueba de trabajo, ya sea seleccionado el nodo que resuelva primero la operación, seleccionado por los participantes, o en contraprestación de alguna carga o condición, lo que resulta útil para mantener en pie la cadena de bloques, pero que al mismo tiempo podría centralizar y desnaturalizar cada vez más esta tecnología:

> "En este supuesto, la selección del modelo de blockchain va a depender de la naturaleza de los agentes de escritura y de la capacidad para acceder a la información que han de tener los usuarios del sistema blockchain. Sin los agentes de escritura, entonces habremos de optar por un blockchain público como Bitcoin o Ethereum. Por el contrario, si los agentes de escritura son conocidos, entonces utilizaremos una blockchain permisionada o autorizada (como es el caso de Ripple o Hyperledeger Fabric) (…)" (Santiaga y Palazzi, 2019, p. 101).

Ahora bien, mientras más sencilla sea la prueba de trabajo, menos costoso será formar parte como de la red como nodo, esto debido a que la labor de resolver los algoritmos se torna menos compleja y se reduce significativamente el consumo de energía, sin tecnología avanzada, como el hecho de crear *"granjas"* de computadoras debido a la sencillez del sistema.

3.2. Características del *blockchain*

La red de cadena de bloques, en su forma original, mantiene características que lo distinguen de otras tecnologías, entre las más relevantes están:

- Trazabilidad: las transacciones llevadas a cabo necesitan del aval de los pares para así llevar a cabo la secuencia, dejando constancia de la fecha y hora en que se incluyó el registro en la cadena de bloques.
- Inmutabilidad: en principio, la información no se puede alterar o cambiar ni eliminar sin advertir a los otros nodos de la red, nada desaparece o es modificado en la *blockchain.* Esto permite conocer el origen de los datos generados y se tiene por cierta la información que en ella es insertada. En caso que se declaren falsas, se tendrá conocimiento de quien las falseó o incorporó en caso de nodos no incógnitos.

- Trasparencia: las transacciones son públicas y visibles en la red, lo que permite la consulta gracias a la información que se encuentra dispersa entre los pares que participan, considerados como nodos sin conocimiento de jerarquización (P2P), característica de gran utilidad para minimizar imprecisiones o errores comunes, toda vez que la red almacena los datos en distintos paquetes (bloques), creando una réplica[16] mediante la actualización en paralelo en la totalidad de la red *blockchain*, facilitando la posibilidad de ser auditable[17].
- Red descentralizada: elimina la dependencia de confiar en una verdad absoluta sin ser verificada. *Blockchain* solamente permite agregar y no borrar información, porque todos los participantes de la red mantienen copia y no existe un nodo centralizador de la información o con privilegios superiores para negar transacciones de los usuarios.
- Evita la intermediación: el rol de los terceros encargados de dar confianza pasa a los nodos, pues el propio sistema que valida las transacciones y distribuyen los datos donde todos tienen una copia de ella de manera inmediata y universal, a tal efecto, deviene sin objeto la existencia de los terceros fiscalizadores donde la resolución de ecuaciones convierte a la información como válida por naturaleza.
- Seguro: si se quiere modificar el contenido de un bloque, debería no solamente modificar el bloque, sino también los bloques que fueron posteriormente generados al bloque que se pretende modificar, tornando extremadamente difícil la alteración, ya que cada bloque arrastra en su identidad una porción de la identidad del bloque que le precede; es por ello el apelativo de "cadena".

  Esto aunado a que los bloques presentan la fecha en la que se lleva el registro, convirtiéndolo resistente a los ataques informáticos, fallos o falsificación.

  Desde otro punto de vista, en *blockchain* los pares mantienen los códigos suficientes para certificar la autenticidad de un usuario, sin que necesariamente se utilice su nombre real en la red, por lo que el consenso es la forma confiable que evidencia la identidad de un usuario[18].

[16] La ausencia o ataque de alguno de los nodos tiene copias de seguridad (*backups*) en otro nodo, propio y natural del sistema.

[17] Cabe destacar que el contenido puede ser encriptado para no ser leído por los que no estén autorizados para ello.

[18] En el caso de *Bitcoin*, por ejemplo, la información IP no se almacena, y las claves de cifrado se utilizan en lugar de la información personal dando por válido la autenticidad de un usuario del sistema donde la identificación del usuario es su dirección *Bitcoin*, por lo que las partes permanecen en seudo-anonimato a pesar de que las transacciones sean públicas.

4. Utilidad del *Blockchain*

Una vez recorridas las características y los pasos para formar la cadena de bloques, resulta de importancia resaltar la utilidad que propone esta tecnología.

A nuestros días ha sido vista como la segunda versión de internet, dado que resuelve problemas socio-económicos por su capacidad de efectividad, inmutabilidad, descentralización, trazabilidad, en especial para transmitir información sin control o barreras, como el propio conocimiento, puesto que en la actualidad *blockchain* permite realizar transacciones de documentos electrónicos, archivos de todo tipo, criptomonedas, etc.

Del mismo modo, la confianza digital que registra, permite conjugar el mundo virtual con la realidad, ya que, a través de su implementación, se otorga valor a las transacciones realizadas por medios tecnológicos que no se limitan al registro y transferencias de criptomonedas, encontrando como provecho la organización, compartir datos veraces, ejecutar transacciones y dar seguimiento a los servicios (Arecha, 2019).

Sin duda, su funcionalidad reduce los costos y la complejidad en cuanto a actividades que requieren de la participación de terceros de confianza, dado que su coordinación descentralizada es transparente, lo que da paso a la transformación de ciertos modelos de negocios por simplificar procedimientos, encausando nuevas ideas para la refinanciación y reestructuración de pasivos, firma digital, certificaciones, contratación electrónica, etc.

En Argentina se ha contemplado la posibilidad de incorporar la tecnología *blockchain* para el resguardo documental de la propia Plataforma de los documentos notariales en soporte digital (Falbo, 2019), y en el 2018, se registró la primera operación inmobiliaria en *blockchain* de *Bitcoin* integrando los detalles como el precio, el plazo y la cantidad de cuotas a pagar, como un contrato digital, incluyendo hipervínculos de fotos del terreno, en concepto de Boleto de Compraventa registrado en *blockchain.*

Blockchain motivó a empresas para que optaran por cambiar su modelo de negocios con el fin de incrementar su productividad; por ejemplo, *Hyperlager Proyect*, un consorcio de empresas que explora soluciones por medio del proceso de cadena de bloques; igual es el caso de R3 CEV, consorcio de firmas y 40 bancos que proyectan soluciones para los procesos financieros por medio de la tecnología *blockchain* (servicios financieros, seguros, activos digitales, cuidados de la salud, etc.).

Se comenta el posible registro único del expediente clínico distribuido, con información que se va recopilando (García Mexía, 2018) con los documentos dispersos en cada centro médico a los cuales el paciente ha asistido, cumpliendo con su función de información actualizada desde cualquier parte del mundo, evitando diagnósticos errados, o doble diagnóstico, y a su vez, garantizando la confidencialidad, ya que la información sería exclusiva por ser el paciente el destinatario de la información.

El *internet* de las cosas (IoT) con billones de dispositivos conectados al mismo tiempo en *internet* en modelos centralizados que no soportarían la carga de datos, la cadena de bloques podría ser la forma directa de comunicación que almacenaría las órdenes para que se puedan apreciar y registrar.

También la gestión de bienes digitales, como la compra de un boleto digital de cine o de transporte, en donde se registre la compra en *blockchain.* Otro ejemplo es la trazabilidad de mercaderías, el control alimentario, la autenticación de servicios *open data,* las transacciones financieras descentralizadas y la trazabilidad de activos, la identidad digital (García Mexía, 2018)[19], las investigaciones médicas, la oferta pública a escala internacional *(Initial Public offering*: *IPO*), el intercambio de mercaderías entre productor y consumidor final de forma directa y que regule su forma de producción.

También se comenta la aplicación de la cadena de bloques en la producción de energía registrando la demanda en tiempo real y elaborar la logística para producir lo necesario; de igual forma en la publicidad y el periodismo permitiendo conocer el origen de la difusión[20] y los intervinientes en dicho proceso; contratos mercantiles, certificaciones académicas y títulos universitarios, etc.

Con la cadena de bloques, las aerolíneas podrían crear sistemas de lealtad y fidelización, identidad de los pasajeros, trazabilidad, etc. y se habla también de los pagos regulares de los salarios o incentivos programados a largo plazo para su ejecución

[19] También resultaría útil para los refugiados que no disponen documento de identificación personal, para acceder a servicios médicos, financieros, educación o evitar el tráfico de los seres humanos, fenómeno conocido como la *"inclusión digital plena".*

[20] Explicada por Marqués-Pascual que la mera utilización de *blockchain* no elimina o identifica los *fake news*, debido a que el sistema es inmutable, pero si se puede conocer a los propagadores de las noticias falsas o datos falsos.
Entre las facilidades: conocer de dónde surgen las noticias (verdaderas o falsas), plasmar un sistema retributivo por su trabajo directamente con el consumidor para ahorrar intermediarios o sistema de puntación. Con ello se puede reconocer el trabajo de aquellos periodistas que hacen su trabajo de manera correcta.

También promueve la efectividad del reclutamiento del recurso humano calificado, mediante hojas de vida digitales con documentos complementarios y la verificación de la identidad en *blockchain* (certificados médicos, experiencia laboral, estudios, estado civil, etc.) lo que en resumen agilizaría el proceso de selección, sin consultas o validaciones de terceros.

En la educación es utilizado como utensilio de fiabilidad de la certificación *online* para la emisión de títulos, preservar y publicar el conocimiento en formato digital y acreditar asistencia.

Sirve para potencializar las estrategias de gobierno, por mencionar algunos ensayos: *"SmartDubai"* implementa la tecnología *"Blockchain for Goverment"* para mejorar la seguridad nacional, acrecentando un sistema de biografía digital de los distintos acontecimientos de los individuos (estudios, trabajo, viajes, familiares, etc.).

Estonia la utiliza para realizar servicios notariales. En China los tribunales admiten como prueba los registros de propiedad intelectual y derechos de autor realizados en la plataforma en caso de demandas, y en Australia, los vídeos policiales se almacenan en cadenas de bloques y por este medio realizan el seguimiento del suministro de grano (García Mexía, 2018).

Por su parte, Panamá ha manifestado su interés en aplicar cambios a los procesos de licitación pública con la tecnología *blockchain* por su "*inmutabilidad, trazabilidad y seguridad"*, para optar por un proceso más transparente y eficiente, para evitar aspectos de discrecionalidad en las negociaciones de obras públicas permitiendo la participación de pequeñas y medianas empresas, con el apoyo de una normativa especial (Panamá usará *Blockchain* en contrataciones públicas y fortalecerá transparencia, 2019); también sería de utilidad para la logística portuaria, eliminando a los intermediarios que no aportan valor.

Podría decirse entonces que "Blockchain promete ser una garantía tecnológica para que los usuarios puedan tener nuevamente un rol orgánico y no uno de consumo pasivo; para que los ciudadanos sean verdaderos dueños de sus datos, optimizar procesos, reducir costos, y que la información pública esté realmente disponible para la comunidad" (Mora y Palazzi, 2019, p. 319), cambiando la forma de comercializar, transmitir datos, conocer el origen y trayecto de los datos, identificar productos espurios o conocer la verdad[21].

[21] En fin, se habla del acceso inmediato de una serie de documentos desde cualquier parte del mundo por medio de la red *blockchain*, se solucionan los costes de todo tipo y con información fidedigna, que se ampara por la reproducción automática de las distintas copias que existen en la red.

4.1. *Blockchain* y la pandemia *(SARS-CoV-2)*

El sistema de cadena de bloques pudo tener mayor expansión durante la pandemia ocasionada por el *"coronavirus" (Sars-Cov-2*[22]*),* al dejar en evidencia la necesidad de poner en marcha un sistema transparente y confiable a disposición de los ciudadanos, con un mejor control en cuanto a la producción de requerimientos que demandan los diferentes Estados, añadiendo certidumbre y precisión a los requerimientos.

Ejemplo de ello, el control de la calidad y la cantidad de los insumos, el correcto seguimiento de la cadena de suministro (fármacos, mascarillas, guantes, equipos, etc.) desde su origen/producción, distribución, transporte hasta su entrega; el seguimiento de datos médicos, asesoramiento ciudadano o incorporando transparencia a los trámites registrados por la administración.

Podría rastrear la utilidad de las donaciones en todas sus etapas, inclusive hasta la confirmación del personal hospitalario al recibir los mismos; se tendría de forma inmediata el trayecto y propagación del virus con datos reales como consecuencia del incremento de la data y así reducir los errores eliminando las atribuciones excesivas de entes que pueden validar, borrar o editar la información.

En igual sentido se incluyen servicios certificados de aduana, información médica, el registro de identificación de síntomas, o al menos, pretender que sea una vía para procesar los reclamos de seguro sin intervención humana, y al mismo tiempo, reducir el uso desmesurado del papel.

Blockchain proporcionaría agilidad para certificar el estado de salud luego de realizadas las pruebas de la enfermedad y llevar los registros de recuperados, pacientes en cuidados intensivos y las defunciones, generar permisos de circulación de forma fehaciente y consultable, o simplemente compartir datos entre países, sin infringir la privacidad para tomar las mejores decisiones, todo ello, basado en datos electrónicos amparados por el registro *blockchain*, en un momento que se requiere evitar el contacto físico y agilizar los procesos sin eliminar información vital.

[22] Declarada pandemia por la OPS el 11 de marzo de 2020.

5. Su relación con el derecho civil

El derecho civil es la rama del derecho privado con mayor amplitud en la vida cotidiana. En general, regula las relaciones entre personas, desde su nacimiento hasta su muerte, incluyendo las relaciones patrimoniales como parte de los atributos de la personalidad.

Blockchain parece abarcar el comercio, la contratación y hasta temas de salud. Entendiendo el concepto de derecho civil, desde una perspectiva amplia, los sistemas de bloques provocan relaciones con efectos jurídicos regulados, así sea por el uso y las buenas costumbres o las voluntades legítimas de las partes -aunque sea dicho de paso, permite las transacciones de objetos ilícitos, lo cual también ocurre con los medios tradicionales-.

La incidencia del blockchain en nuestros días, marca nuevos paradigmas del cómo vemos las cosas, toda vez que la tecnología de almacenamiento con carácter distributivo tiene gran incidencia para el derecho:

> "Para los juristas, las características de la propia DLT suponen una revolución de los conceptos vertidos en el derecho de internet, por un lado, porque esta tecnología irá afectando, y afecta ya de forma incipiente, a todos los sectores del comercio y de la industria, e incluso al modo de relacionarse las personas en las relaciones entre particulares y con las empresas, lo que acarreará la necesidad de adecuar o adaptar múltiples normas en todas las disciplinas jurídicas; y por otro lado, porque el derecho de internet y sus principios, donde naturalmente se ha de encuadrar el derecho de la DLT en la medida en que esta tecnología usa necesariamente internet como medio de desenvolvimiento natural, quedan ampliamente superados; lo que implica una necesaria renovación y actualizaciones que faciliten un régimen integrado y eficiente en los diferentes niveles normativos afectados por las características específicas de esta tecnología" (Ibáñez, 2019, p. 19).

Para el autor *in comento* los cambios se extienden a la mutación del concepto de mercado, el modo de generar transparencia, las relaciones jurídicas entre administradores y administrados para lograr procesos eficientes, la reducción de la carga burocrática, la dinámica contractual a distancia, nuevos conceptos de privacidad y confidencialidad, la constitución y administración de los sistemas de identidad digital seguros y transparentes y el concepto de fe pública extraregistral, etc. (Ibáñez, 2019), temas que obviamente interesan al derecho civil.

Muchos países han realizado esfuerzos para regular y limitar la transacciones mediante criptomonedas, prototipo de la tecnología *blockchain*, como es el caso de la Unión Europea, mediante Directiva (UE) 2018/843 vigente desde el 10 de enero de 2019, con la finalidad de abarcar todos los usos de las monedas virtuales, también es cierto que la Comisión Europea ha publicado su "estrategia para la implementación de la tecnología *blockchain* en la Unión Europea" puesta en marcha desde enero de 2020 para incitar a la cooperación e inversión de los proyectos que utilicen *blockchain* como una tecnología DLT.

De igual forma, la Comisión Europea lanzó el observatorio y Foro *Blockchain* de la Unión Europea en febrero de 2018, y el 10 de abril de 2018, los 21 Estados miembros de la UE, Noruega y Liechtenstein, crearon la Asociación Europea *Blockchain* (EBP) con la finalidad de potencializar la tecnóloga para crear un mercado único digital y promover una gobernanza transparente por medio de la tecnología DLT, proyecto al que se han adherido otros países como Grecia (2018), Rumania (2018), Dinamarca (2018), Chipre (2018), Hungría (2019), Croacia (2019), etc.; interesados en participar en la creación de servicios públicos transfronterizos como el acceso a investigaciones universitarias desde cualquier país de la región, el notariado de documentos para automatizar la verificación de cumplimiento en procesos urgentes, la identidad digital soberana con todos los datos personales integrados (carrera profesional, vida laboral, propiedades, etc.) y el intercambio de datos de confianza para el año 2020, en donde cada Estado dispondrá de nodos nacionales.

Claro está que en Estonia el avance es parte de la madurez social, ya que *internet* es un derecho humano básico desde el 2000. Esta óptica, hasta cierto punto, permite una regulación de los espacios de contratación electrónica y de los servicios de la sociedad de la información a través de la asimilación de las tecnologías en nuestras vidas como efecto de la pronta asimilación de los Estados, sin la urgente necesidad de adoptar normas poco imperativas por utópicas.

Desde nuestra perspectiva, la tecnología ofrece un desarrollo que no puede ser regulado con facilidad, como sucedió con *internet*, eso aunado a los intereses políticos y económicos que podrían no estar de acuerdo en aplicar sistemas descentralizados.

Lo cierto es que se requiere de la implementación de estándares globales como sucedió en 1996 con la Ley Modelo de Comercio electrónico de la (CNUDMI/UNCITRAL), o que al menos los gobiernos opten por la aplicación de espacios de prueba (*Regulatory sandbox)* para determinadas transacciones o actividades que emplean esta invención y apoyan al desarrollo.

6. Problemas actuales

Uno de los inconvenientes que presenta la tecnología *blockchain*, es el excesivo consumo energético que demandan los ordenadores mineros para continuar con su constante labor de solución matemática y que inclusive puede ser efectuado en vano.

Para Hernández, Arroyo y Díaz (2019), la información es inmutable pero el espacio que ocupa en el disco duro lo convierte en una tecnología que no está al alcance de todo el público en general: "(…) las transacciones son lentas y costosas, propensas a la congestión y que no pueden escalar con la demanda, así como que el consenso descentralizado detrás de la tecnología es frágil y consume grande cantidad de energía" (Arrecha, 2019, p. 65).

Además, diversos son los comentarios sobre la *"escalabilidad"* que requiere la red para ser más efectivo. La carga de trabajo que debe realizar cada nodo con respecto a la cantidad de transacciones pendientes, requiere de esfuerzos adicionales para disminuir los tiempos de espera y gastos que son poco prácticos.

Adicional a lo anterior, el sistema de bloques ofrece una seguridad informática la cual no necesariamente coincide con la seguridad jurídica. Recordemos que el desarrollo de la cadena de bloques ofrece una seguridad y una confidencialidad basada en la mayoría de las veces en el *seudo-anonimato*[23], lo que al mismo tiempo parece constituir un discurso de doble moral; entendiendo que la seguridad jurídica es un principio que se fundamenta en la certeza del derecho para así hacerlo valer, por lo que corresponde al menos un grado de publicidad para hablar de *"reconocimientos de derechos"* desplegados en esta tecnología.

Así, la plataforma cuando trata criptodivisas dificulta la aplicación de las normas *compliance* por presentar una forma de trazabilidad no fundada en la transparencia (Faliero, 2017), lo que permite ensayar una espuria equivalencia entre confidencialidad y seguridad, dando pie a su utilización para el financiamiento de actividades ilícitas.

A tal efecto, consideramos que el sistema *blockchain* no puede funcionar para facilitar el anarquismo por desconocer límites, por ejemplo, el sistema no reconoce el mundo real, como la ilicitud del objeto del contrato, sí la causa responde realmente a la motivación del individuo, que exista una parte débil en el contrato, entre otros principios como: *"buena fe", "propiedad", "caso*

[23] Las transacciones pueden ser anónimas si las credenciales son seudónimos, pero la transacción realizada si es pública.

fortuito", "fuerza mayor", "excesiva onerosidad", "transmisión de derechos", "las buenas costumbres", etc. aspectos que únicamente pueden ser insertados con el conocimiento informado de los participantes.

Accenture[24], multinacional dedicada a la consultoría de servicios tecnológicos y tercerización, investigó sobre la posibilidad de cambiar la información contenida en los bloques[25] patentando una cadena de bloques *"editable",* opción que podría ser implementada por las redes privadas como una suerte de *"freno de emergencia"* por una autoridad central de la red (privada), con permiso previo y siguiendo determinadas normas de gobernanza (Marqués-Pascual y Sintes-Olivella, 2020, p. 41), lo que deja en duda si la tecnología de las cadenas de bloques, al abandonar su fin de descentralizado altera su propósito de confianza.

El caso 2016 de *Decentralized Autonomous Organization* (*The DAO*) basado en *Ethereum*, guarda relación con la desconfianza en la cadena de bloques. Resulta que los códigos informáticos en la cadena de bloques fueron vulnerados desviando los fondos recaudados a una dirección de su selección, extrayendo una suma considerable de *ether (equivalente a 50 millones de dólares)*, situación que fue remediada a través de una actualización desplegada por varios gestores de la comunidad (entre ellos su creador: Vitalik Buterin) que devolvía la cantidad robada, acción que dividió opiniones entre quienes aceptaron la acción y la mayoría que no estaba de acuerdo, porque se afectaba el principio de inmutabilidad del código y debía mantenerse así, evidenciando que los sistemas no eran tan descentralizados.

Esto no quiere decir que la tecnología no sea provechosa por ofrecer algunas desventajas, muy por el contrario, sería oportuno ahondar sobre ello para optimizar la red de bloques y remediar sus debilidades y sentar ciertos criterios para tal efecto.

---

[24] En el referido sitio web: https://www.accenture.com/us-en/insight-editing-uneditable-blockchain *"Editing the Uneditable: Blockchain needs to adapt to an imperfect world",* se enlistan algunos beneficios de la inmutabilidad del sistema, pero al mismo tiempo intenta lograr empatía con las instituciones de servicios financieros que se enfrentan a requerimientos regulatorios, donde la absoluta inmutabilidad puede tornarse engorroso en las áreas de: almacenamiento de datos, errores operacionales como la codificación o transacciones erradas, información confidencial que por ley requiere, luego, ser removida como la privacidad de los datos del consumidor o de los derechos de los accionistas, documentos clasificados, actos ilegales o incorrectos etc.

[25] La posibilidad de cambio del historial de blockchain por medio de ataques conocidos como "historia-revisión" (*history-revision attack*) en donde la historia real es sustituida por una cadena alternativa como producto de falsificación, situación que requiere de un alto esfuerzo lo cual parece tildarlo de imposible, pero como anota Johana Faliero "la amenaza es muy real debido a que la viabilidad de un ataque de estas características se deriva de la Ley de Moore, que empíricamente postula que el poder de cálculo se duplica cada año más o menos, y por ello, cada vez se torna más cercana la posibilidad que ello ocurra" (Faliero, 2017, p. 78.)

7. Conclusiones

1. El sistema *blockchain* debe su nombre a las etapas que debe implementar: generar un bloque para ser insertado en una cadena de homólogos.
2. La utilidad de la tecnología *blockchain* es versátil, dado que su inicio se dio con las criptomonedas, luego se implementó como soporte de los contratos electrónicos. También funciona para la trazabilidad de registros, elimina los terceros de confianza en casi toda operación existente, realiza sellados de tiempo, en fin, es una tecnología que agrega valor a las transacciones digitales e internet.
3. La composición de una cadena de información representada en bloques y que se incorporan sucesivamente en el registro o bitácora, dificulta la gestión de corregir, modificar, o alterar la información contenida en la red preservada en los nodos, esto lo convierte en una tecnología distributiva como sistema descentralizado.
4. *Blokchain* se caracteriza por ser trazable, inmutable, transparente y descentralizada, evita la intermediación y aporta seguridad y confianza a las transacciones.
5. *Blockchain* refleja su utilidad al reducir costos y la complejidad de los procesos, incrementando la productividad de los nuevos modelos de negocios, reflejándose en actividades relacionadas con la restructuración de pasivos, certificaciones electrónicas, cuidados de la salud, la gestión de bienes digitales, el seguimiento de la cadena de suministro y la efectividad en el reclutamiento del recurso humano, etc.
6. La cadena de bloques descentralizada es el espacio en el que los usuarios tienen un rol orgánico y no uno de consumo pasivo. Los ciudadanos son verdaderos dueños de sus datos, optimizan procesos y la información pública esté realmente disponible para la comunidad, cambiando la forma de comercializar, transmitir datos, conocer el origen y trayecto de los datos, identificando productos espurios y conociendo la verdad del trayecto.
7. Como la mayoría de los avances tecnológicos, su aceptación deriva de una necesidad social que supera la actividad legislativa, lo que parece ser la constante en un momento en que la era contemporánea pasa a ser efímera, y que, sin percibirlo, nos aproximamos a la era digital. Su regulación puede darse inclusive de forma práctica, con el requerimiento de estándares globales, como sucedió en 1996 con la Ley Modelo de Comercio electrónico de la (CNUDMI/UNCITRAL), o que al menos los gobiernos opten por la aplicación de

espacios de prueba (*Regulatory sandbox)*, para determinadas actividades que emplean esta invención.

8. La cadena de bloques presenta ciertas desventajas que deberían ser atendidas para maximizar su nivel de efectividad y lanzar su escabilidad como herramienta, entre ellas: su excesiva implementación de recursos tecnológicos y económicos que podría convertirlo en una red selectiva, estimular su seguridad jurídica y dosificar los esfuerzos que se plantean con respecto a su posible centralización.

8. Referencias

ARECHA, Martin (2019). *Las nuevas Tecnologías ante el Derecho Comercial*, 1ª ed., Didot, Ciudad Autónoma de Buenos Aires.

Blockchain Techhnologies (2023) [en línea] : https://ec.europa.eu/digital-single-market/en/blockchain-technologies

CAMACHO CLAVIJO, Sandra (2005). *Partes intervinientes, formación y prueba del contrato electrónico,* Editorial Reus, S.A., Madrid.

CANO MARTÍNEZ de VELASCO, José Ignacio (2011). *La decadencia del contrato, el derecho robot*, Editorial J.M. Bosch Editor: Barcelona.

FALBO, Santiago y DI CATELNUOVO, Franco (2019). *Nuevas tecnologías aplicadas a la función notarial, actuaciones notariales en soporte digital, firma digital*, 1 ed. revisada, Di Lalla ediciones: Ciudad de Buenos Aires.

FALIERO, Johana (2017). *Criptomonedas: La nueva frontera regulatoria del derecho informático*, 1 ed., AD-HOC, SRL, Buenos Aires.

GARCÍA MEXÍA, Pablo (2018). *Criptoderecho: La regulación de Blockchain*, Wolters Kluwer España, España.

HERNÁNDEZ, Luis Encinas, ARROYO GUARDEÑO, David y DÍAZ VICO, Jesús (2019). *¿Qué sabemos de? Blocchain,* Editorial CSIC Consejo Superior de Investigaciones Científicas.

IBÁÑEZ JIMÉNEZ, Javier Wenceslao (2018). *Blockchain: primeras cuestiones en el ordenamiento español*, Dykinson S.L., Madrid.

INSTITUTO CUATRECASAS (2019). *Economía de plataforma, Blockchain y su impacto en los*

recursos humanos y en el marco regulatorio de las relaciones laborales, Wolters Kluwer España, España.

La Historia de Blockchain (Cadena de bloques) (2018). [en línea]: https://www.binance.vision/es/blockchain/history-of-blockchain

NAKAMOTO, Satoshi (2008). *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a.-Usuario*, traducido al Español por Ángel León [en línea]: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

MARQUÉS-PASCUAL, Joaquín y SINTES-OLIVELLA, Marçal (2020). *Blockchain y periodismo: como la cadena de bloques cambiará los media*, Editorial UOC. .

MORA, Santiago J. y PALAZZI, Pablo A. (2019). *Fintech: Aspectos legales*, CDYT Colección Derecho y tecnología, Buenos Aires.

Panamá usará *Blockchain* en contrataciones públicas y fortalecerá transparencia (2019). *ANP agencia de Noticias* [en línea]: https://anpanama.com/8647-Panama-usara-Blockchain-en-contrataciones-publicas-y-fortalecera-transparencia.note.aspx

SANTIAGO, J. Mora y PALAZZI, Pablo A. (2019). *Fintech: Aspectos Legales*, Tomo II, 1ª ed.- , CDYT Colección Derecho y Tecnóloga, Ciudad Autónomo a de Buenos Aires.

***Signature: electronic transactions: blockchain technology, State of Arizona, House of Representative, Fifty Legislatura, Firs Regular Session, HB2417,* Introduced by Representative Jeff Weninger,** (2017). [en línea]: https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf