10.26439/advocatus2023.n043.6420

Aspectos legales de la tecnología *Blockchain*

Alejandro Rafael Morales Cáceres

Abogado por la Universidad de Lima.
Máster en Derecho de las TIC, Redes Sociales y Propiedad Intelectual (IT+IP) por ESADE Business School.
Profesor de Derecho Comercial y de Derecho y Tecnología en la Universidad de Lima.

SUMARIO:

RESUMEN:

La *Blockchain* ha irrumpido en años recientes como una tecnología que promete revolucionar la forma como llevan a cabo las transacciones a nivel global. En tal sentido, por medio del presente artículo el autor realiza una aproximación sobre lo que es la *Blockchain*, cómo esta es un medio que ha favorecido el auge de las criptomonedas —que no requieren de un banco intermediario para efectuar pagos a través de internet—, la aparición de los *smart contracts* que operan automáticamente para regular los negocios efectuados por medios virtuales, pasando por explicar en qué consiste la tokenización de activos —tangibles o intangibles— para su posterior comercialización empleando la *Blockchain*, así como reflexionando sobre la incorporación de estas innovaciones en el ordenamiento jurídico nacional.

Palabras clave: *Blockchain*, criptomonedas, tokenización de activos, *smart contracts*, *Decentralized Autonomous Organizations* — DAOs.

ABSTRACT:

The Blockchain has emerged in recent years as a technology that promises to revolutionize the way transactions are carried out globally, in this sense, through this article the author provides an approach about what the Blockchain is, how it is a means that has facilitated the rise of cryptocurrencies —which do not require an intermediary bank to make payments over the internet—, the advent of smart contracts that operate automatically to regulate business carried out through virtual means, going through explaining what is the tokenization of assets —tangible or intangible— for their subsequent commercialization using the Blockchain, as well as reflecting on the incorporation of these innovations into the national legal system..

Keywords: Blockchain, cryptocurrencies, asset tokenization, smart contracts, Decentralized Autonomous Organizations — DAOs.

"Blockchain es la tecnología. Bitcoin es simplemente la primera manifestación convencional de su potencial".

Marc Kenigsberg

I. INTRODUCCIÓN

La tecnología *blockchain* comienza a volverse famosa desde el año 2008, a partir de la publicación del *White Paper Bitcoin: A Peer-to-Peer Electronic Cash System*, publicado por una persona o un grupo de personas con el seudónimo Satoshi Nakamoto. Así, el origen de esta tecnología, sin duda, se encuentra vinculada a *Bitcoin*; sin embargo, el concepto de la tecnología *blockchain* puede remontarse a inicios de la década de 1990, cuando los científicos de investigación Stuart Haber y W. Scott Stornetta introdujeron una solución computacionalmente práctica para "sellar temporalmente" —"timestamping"— documentos digitales a fin de que no pudieran ser alterados o manipulados.

El Foro Económico Mundial afirma que para el año 2027 el 10% del Producto Bruto Global estará almacenado en *blockchains*[1] y según GARTNER será un mercado de servicios de un valor aproximado de 3.1 billones de dólares en 2030[2]. Para ponerlo en términos relativos, este monto equivale a 15 veces el PBI peruano. Es innegable que un desarrollo tecnológico tan importante no debe desarrollarse sin un marco jurídico apropiado que brinde seguridad jurídica a todos los agentes del mercado.

1. World Economic Forum, *Deep Shift: Technology Tipping Points and Social Impact*, (2015), acceso el 5 de mayo de 2020 en https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf y Thibault Schrepel, Libra: a concentrate of "Blockchain Antitrust", publicado en Michigan Law Review (online), Abril de 2020, disponible para descarga el 16/04/2020 en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3574684, p. 160.

2. Confr. Gartner, Inc., The real business of blockchain, escrito por David Furlonger y Christophe Uzureau, y publicado en 2019 por Harvard Business Review Press, p. 3, Recuperado de: https://www.gartner.com/en/publications/thereal- business-of-blockchain.

El principal potencial revolucionario y transformador de la tecnología *blockchain* radica en la capacidad de transferir valor. Con la creación de la red Bitcoin se hizo posible por primera vez el intercambio de valor directamente entre partes desconocidas —*peer-to- peer*—, sin intermediarios y de forma estrictamente digital. Hasta entonces, internet había hecho posible el intercambio digital de datos.

Sin embargo, este protocolo TCP/IP resultaba insuficiente para la transferencia de valor, que siempre había necesitado de un complejo entramado de terceros de confianza para tener lugar. Pensemos por ejemplo que, hasta la creación de la red Bitcoin, los pagos solo habían sido posibles gracias a un sistema en el que participan distintos intervinientes con el objeto de dar seguridad al intercambio. El protocolo Bitcoin creó una unidad de cuenta —el bitcoin— o moneda digital que podía ser intercambiada de forma prácticamente automática por las partes intervinientes en el sistema sin necesidad de bancos, sistemas de compensación y liquidación y otros terceros que dieran seguridad a esas transacciones.

En esta línea, así como el internet significó un cambio fundamental en relación con la accesibilidad y la forma en la que compartimos, la tecnología *blockchain* permite revolucionar y cambiar trascendentalmente la forma en la que se realizan transacciones entre individuos, empresas o incluso máquinas. No debemos perder de vista que uno de los grandes beneficios que trae consigo la tecnología *blockchain* es que permite disponer de un sistema que garantice la absoluta transparencia[3].

En este contexto, la tecnología *blockchain* aparece como una fuerza que empuja hacia la próxima generación de Internet, a la que algunos denominan "*Web3*". La *blockchain* reinventa la forma en la que los datos son almacenados y gestionados en Internet, proveyendo un único conjunto de datos —una capa de estado universal— que es colectivamente administrado por todos los nodos de la red. Esta capa de estado único, por primera vez, provee una capa nativa para intercambios de valor para la Internet que no requiere intermediarios. Permite genuinas transacciones entre pares —*peer-to-peer*—.

Teniendo en cuenta lo expuesto, el objetivo principal del artículo es aproximar al lector al concepto, funcionamiento y características de la tecnología *blockchain*, así como desarrollar los principales aspectos legales que los abogados debemos de considerar. Lamentablemente, es muy probable que aquí no se encontrarán todas las respuestas relacionadas a las dudas e inquietudes generadas por la disrupción de la tecnología *blockchain*. Es más, es altamente probable que se generen más preguntas en torno a este tema; sin embargo, es nuestra intención que este artículo pueda ser su "punto de partida" en esta aventura llamada *blockchain*.

II. APROXIMACIÓN AL CONCEPTO DE BLOCKCHAIN

La "*Blockchain*" o "*cadena de bloques*" es una base datos, o un libro de contabilidad público mundial distribuida en una red descentralizada, en el que se anotan todo tipo de operaciones utilizando la criptografía[4]. Una *blockchain* es una base de datos distribuida que registra bloques de información y los entrelaza para facilitar la recuperación de dicha información y la verificación de que esta no ha sufrido cambios. En otras palabras, la tecnología "*Blockchain*" funciona igual que un libro mayor de contabilidad, pero, en este caso, los apuntes son públicos y descentralizados. Asimismo, esta cadena

3. Alvarado, María del Carmen, y Daniela Supo. "Blockchain y propiedad intelectual: aplicando una tecnología innovadora en la gestión de derechos intangibles." Themis 79, (2021): 346. https://doi.org/10.18800/themis.202101.019

4. Carrascosa, Cristina. "¿Qué es Blockchain y por qué va a cambiar (casi) todo?" ECIJA. ECIJA, 27 de septiembre de 2016. https://ecija.com/blockchain-va-cambiar-todo/

de bloques está diseñada exclusivamente para evitar su alteración una vez que los datos han sido publicados.

Don Tapscott, escritor del libro denominado "La Revolución del Blockchain" la define como:

> *"Un libro mayor o una gran base de datos distribuida globalmente, que opera en millones de dispositivos y se encuentra abierta a cualquier persona, donde no sólo la información es almacenada y gestionada de forma segura y privada, sino cualquier cosa de valor como el dinero, los títulos, los actos, las identidades, incluso los votos podrán ser administradas de esta manera. La confianza se establece a través de la colaboración masiva y criptografía inteligente en lugar de utilizar intermediarios poderosos como los gobiernos y los bancos[5]".*

Ilustramos dicha operativa a través del símil que recoge Feliu Rey[6]:

> *"Imaginemos una mesa de reuniones alrededor de la cual se sienta un número significativo de personas. Cada una de estas personas —ordenadores o nodos conectados— tiene un libro de registro en blanco donde realiza anotaciones —sistema descentralizado—. La primera anotación, sigamos con el ejemplo, es que A tiene 50 acciones y se las quiere transmitir a B. Primero se verifica que A tiene 50 acciones que puede transmitir —bloque con información—, y se comprueba que todos los miembros de la mesa están de acuerdo con esta anotación inicial —sistema de verificación por consenso descentralizado—. Luego se transmite a B. Como todos tienen en su libro que A es el titular y las puede transmitir, proceden a anotar la transmisión a B. Si A quiere volver a transmitir esas acciones, no podría porque ya no consta en el registro como titular y los miembros de la mesa al verificar tal información rechazarían la anotación, por lo que no permitirían esa transacción. En ese sentido, sólo B podría transmitir las acciones ulteriormente. Intentar una alteración de los registros, aunque no es imposible, exigiría un consenso de todos los miembros de la mesa y una modificación en todos los nodos de cadenas de bloques que recogen un tracto sucesivo, lo que resultaría, sin duda, altamente improbable."*

La tecnología *blockchain* es el tipo de protocolo que hace posible mantener una base de datos única pero distribuida o simultáneamente copiada en los respectivos ordenadores de los participantes de una red —nodos— de manera fiable. Esto da a cada parte acceso directo a los registros de su interés, eliminando la necesidad de intermediarios. El mantenimiento o gestión de esa base de datos se desarrolla de forma descentralizada a través de mecanismos de consenso. Además, el uso de criptografía hace posible atribuir cada uno de los registros de esa base de datos a una de las partes intervinientes, ofreciendo, a la vez, garantía de integridad del contenido.

Blockchain es una tecnología que permite la transferencia de información de una forma completamente segura gracias a la criptografía asimétrica. Se suele comparar con un libro de contabilidad de una compañía en donde están registradas todas las entradas y salidas de dinero. En este caso, lo que se registran son todos los acontecimientos digitales. Lo revolucionario es que se reemplaza al intermediario, quien actúa como tercero de confianza, por una red distribuida de nodos independientes que registran y validan los datos de la transacción. Así, una vez que la información es introducida no podrá ser borrada, solo se podrán añadir nuevos registros. Además, no será legitimada a menos que

5. Tapscott, Alex, y Tapscott, Don. 2016. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World. 1ra ed. Editorial Penguin Random House.

6. Feliu, Jorge. "Smart Contract: Concepto, Ecosistema Y Principales Cuestiones De Derecho Privado." La Ley Mercantil 47, (2018): 11, 12.

la mayoría de ellos se pongan de acuerdo para hacerlo. Básicamente, la tecnología *blockchain*, elimina a los intermediarios, descentralizando toda la gestión.

En buena cuenta se trata de una innovación en el diseño de bases de datos digitales que hace posible llevar a cabo una contabilidad fiable de activos digitales. Como bien señaló DE LA MATA MUÑOZ, en el programa de *Blockchain Compliance* de *Blockchain Intelligence* de Madrid, el elemento innovador se encuentra en la visión inteligente de combinar distintas tecnologías ya conocidas desde hacía incluso décadas: 1) registros digitales —*databases*—, 2) redes distribuidas y 3) criptografía. Es la alquimia de esos tres elementos tecnológicos la que hace posible la magia de *blockchain*.

De esta manera, se consigue de forma distribuida eliminar al tercero de confianza quien era el encargado de llevar a cabo el registro de todas las transacciones. En buena cuenta, lo que se busca es que, en vez de confiar en una persona, confiemos en todas. A modo de ejemplo, supongamos que una nave alienígena aterriza en plena Plaza de Armas de Lima y de allí salen dos extraterrestres que saludan al público terrestre para luego regresarse a su planeta de origen. Una vez sucedido este impresionante acontecimiento, se coloca un detector de mentira al 100% de personas que fueron testigos de dicho suceso y se registra aquello que han visto. Todos cuentan la misma historia, con los mismos detalles, despejando así las dudas y comprobando, sin margen de error, que este evento sucedió. La tecnología *blockchain* pretende ser este "detector de mentiras" que compruebe la autenticidad de los hechos a través de diferentes "nodos" que cumplen el rol de estos testigos. Esta tecnología es una forma de verificación y validación de la información, amparándose en el principio de veracidad de la información, empleando la criptografía.

En ese sentido, la tecnología *blockchain* representa el siguiente paso en la economía *peer-to-peer*. Al combinar redes *peer-to-peer*, algoritmos criptográficos, almacenamiento de datos distribuidos y mecanismos de consenso descentralizados, proporciona una forma para que las personas se pongan de acuerdo sobre un determinado estado de cosas y registrar ese acuerdo de manera segura y verificable[7].

III. BLOCKCHAIN COMO ESPECIE DE LA TECNOLOGÍA DEL REGISTRO DISTRIBUIDO

Desde hace mucho tiempo atrás, las empresas e instituciones han utilizado libros para crear y mantener, mediante asientos y anotaciones, registros de transacciones o movimientos. Los titulares de esos libros —Administraciones públicas, bancos, empresas, etc.— concentran, así, información relevante y están en posición de consultarla. En consecuencia, pueden actuar como intermediaros cuando otros agentes interesados precisan de tal información para realizar transacciones, pero, por no ser pública o por necesitar ser validada, no pueden de otra forma conocer o utilizar[8].

Así las cosas, el titular o garante de la información se convierte en una *autoridad central*, en un intermediario en quien todos los usuarios confían, que tiene un control total sobre el sistema e interviene en todas las transacciones. No debemos equiparar esta *autoridad central* a una *autoridad pública* ni a una entidad de crédito u otro tipo de entidad regulada en particular. Se trata, simplemente, del término que se emplea en los trabajos sobre esta tecnología para identificar al poseedor de la información en el

7. Wright, Aaron y De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Social Science Research Network, (2015): 4, 5. https://doi.org/10.2139/ssrn.2580664

8. Boucher, Philip. "How Blockchain Technology Could Change Our Lives." European Parliament. European Parliament, 20 de febrero de 2017. https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

sistema tradicional basado en la confianza, el sistema centralizado[9].

Pues bien, tal como mencionamos anteriormente, la tecnología *blockchain* se presenta como una solución al problema de tener que depositar toda la confianza en una entidad central. Esta tecnología resuelve el problema mediante un protocolo informático de código abierto permite llevar el registro en una base de datos de forma descentralizada y distribuida, sin necesidad, así, de contar siempre y en todo caso con una autoridad central, que actúe como garante de su corrección y como intermediaria en las transacciones realizadas sobre su base.

Al respecto, debemos señalar que la tecnología *blockchain* es un tipo de *distributed ledger technology* o DLT —tecnología de red o registro distribuido—. Una DLT, en esencia, es una base de datos que gestionan varios participantes y no está centralizada. No existe una autoridad central que ejerza de árbitro y verificador. Lo que se busca con esta figura es que el registro, al ser distribuido, aumenta la transparencia, dificultando, así, cualquier tipo de fraude o manipulación. Por tanto, el sistema es más complicado de *hackear* o corromper.

La tecnología DLT permite a los usuarios grabar y almacenar permanente, simultánea y públicamente los datos introducidos en un programa que comparte un colectivo de personas en distintas máquinas telemáticas o servidores informáticos llamados nodos. Esa colectividad da nombre al sistema de almacenamiento, que se conoce como registro distribuido —*distributed ledger*— debido a la existencia y dispersión de los nodos, y, en ocasiones, como registro descentralizado en el sentido de que no existe una entidad registradora central[10].

En ese sentido, la DLT es una tecnología digital "*de registros*", porque, por una parte, quienes operan lo hacen en un espacio de internet que es registral en la medida en que en el se apuntan o anotan datos que, por el hecho de su constancia material, quedan grabados o registrados pudiéndose recuperar posteriormente; y, por otra parte, porque tales anotaciones podrían componer un registro en el sentido jurídico del término, es decir, un espacio donde las transacciones u operaciones que apuntan los sujetos se guardan con finalidades jurídicas de confrontación o cotejo, al tiempo que de archivo o custodia. Y, asimismo, de constitución o composición de relaciones jurídicas, y, adicionalmente, prueba posterior de tales relaciones o de los datos registrados con la eficacia legal que la Ley o las partes determinen, una vez los datos quedan anotados y se recuperan con dicha finalidad probatoria[11].

De otro lado, si bien la tecnología DLT proporciona un sistema de base de datos distribuida, ésta cuenta con una característica diferencial de las bases de datos distribuidas tradicionales: En una DLT no existe una relación de confianza entre los nodos. Para la introducción de nuevos datos en la base y su distribución entre los nodos, existe un mecanismo de verificación colectiva de las nuevas operaciones que se producen en el sistema, para lograr la validación de la transacción, se requiere el consenso de la mayoría de ellos.

En otras palabras, en una red DLT, pueden existir intereses absolutamente contrapuestos entre los nodos que conforman el sistema y para garantizar la coherencia del conjunto y evitar el fraude en las nuevas transacciones que se introducen al sistema y su distribución entre los nodos, necesariamente se implementa un mecanismo de verificación colectiva de cada nueva operación susceptible de registrarse en

9. Porxas, Nuria, y María Conejero. "Tecnología Blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados." Actualidad Jurídica Uría Menéndez 48, (2018): 24-36. https://www.uria.com/documentos/publicaciones/5799/documento/art02.pdf?id=7875

10. Ibáñez, Javier. 2018. Blockchain: primeras cuestiones en el ordenamiento español. 1ra ed. Editorial Dykinson, 15.

11. Ibáñez, *Blockchain: primeras cuestiones en el ordenamiento español*, 16.

el sistema. Es decir, debe lograrse el consenso de la mayoría de los nodos que conforman el sistema, para que se introduzcan nuevos datos en la base de datos. Logrado este consenso sobre una nueva operación, el registro distribuido que comparten todos los nodos, se actualizará y guardará en cada uno de ellos, en cada uno de los ordenadores de estos nodos. Es decir, en cada nodo —computadora— de la red se guardará y se almacenará una copia idéntica del registro que conforma la base de datos.

En consecuencia, la tecnología DLT puede definirse como un conjunto de medios técnicos que posibilitan la implementación práctica de una base de datos digital, de naturaleza distribuida, fundamentada en el necesario mantenimiento de un consenso de los nodos del sistema sobre el estado y evolución de los datos compartidos. Asimismo, es importante señalar que la tecnología DLT emplea de forma combinada tres conocidas tecnologías:

a) Redes *Peer-to-Peer* — p2p: En un sistema DLT, los datos se distribuyen a través de redes p2p, también conocida como redes entre iguales. La tecnología p2p, que se plasma en redes dinámicas de ordenadores interconectados y que posibilitan el intercambio directo de información entre los ordenadores conectados a través de la *Word Wide Web*, sin necesidad de un servidor centralizado que redistribuya los datos, ni clientes fijos. Para dicho intercambio de información, no es necesaria la existencia de un servidor centralizado que redistribuya los datos, ni es necesaria la existencia de clientes fijos, simplemente se transmite de usuarios a usuarios. En un sistema de tecnología de registros distribuidos, los datos se distribuyen a través de dichas redes p2p.

b) Criptografía asimétrica: Es un método de criptografía que permite una conexión segura entre dos partes a través de la aplicación de un algoritmo de cifrado digital con el objetivo de autentificarse y cifrar y descifrar la información que quieren transmitirse de forma confidencial. Este sistema consiste en la utilización de una fórmula matemática muy compleja para crear un par de claves. Esta primera clave es la clave privada. La clave privada es de uso exclusivo para el creador del par de claves, y sirve para cifrar y descifrar mensajes de forma completamente segura. La segunda clave es la llamada clave pública. Esta es una clave que el creador puede entregar a terceras personas. La clave pública se crea a partir de la clave privada, pero el proceso inverso es imposible. De esta forma, el creador de las claves puede compartir esta clave pública con terceras personas, y gracias a ella estas personas puedan enviarle información cifrada que solo será accesible usando la clave privada del creador.

c) Algoritmos de consenso: El algoritmo de consenso, el cual consistente en un complejo algoritmo matemático, es el sistema de organización de una determinada red DLT para que sus nodos logren el consenso distribuido. Existen diferentes tipos de algoritmos de consenso, siendo el más popular el denominado *Proof of Work — PoW*. Cabe recordar que, la piedra angular de la tecnología de registros distribuidos es el consenso distribuido, que es la capacidad de una red de nodos de garantizar el estado común del registro, garantizando que dicho registro está integrado por transacciones válidas, que si bien se encuentran interconectados entre ellos no existe relación de confianza alguna.

Tal como se puede apreciar, la tecnología *blockchain* es un tipo de tecnología DLT. Puede señalarse entonces, que los registros en la *blockchain* se guardan en una consecución de bloques —por eso se llama "cadena de bloques"—. Las operaciones que suceden en la red se organizan en bloques de información vinculados entre sí mediante métodos criptográficos formando cadenas de dichos bloques, sin posibilidad de ser modificados con posterioridad —inalterables—. Un sistema DLT no necesariamente se estructurará en cadenas de bloques ni utilizará este tipo de estructura para garantizar un estado común fiable del registro y un consenso distribuido válido de los nodos.

IV. CÓMO FUNCIONA BLOCKCHAIN

La tecnología *blockchain* es una gran base de datos digital que se encuentra descentralizada en una red *peer-to-peer*. Desde un punto de vista funcional, el sistema permite que partes que no confían unas en otras puedan mantener consenso sobre la existencia, estado y evolución de una serie de factores compartidos. De otro lado, desde un punto de vista técnico, es una red global de ordenadores que gestionan una gigantesca base de datos abierta al público sin la necesidad de que haya ninguna entidad central.

A modo de ejemplo, podemos graficar el funcionamiento de una *blockchain* de la siguiente manera: Pensemos en una hoja Excel con dos columnas donde en una columna colocamos un identificador —ejemplo "abc"— y en la otra un número —ejemplo "22"—. Es decir "abc" le corresponden "22". Ahora imaginemos que esa hoja Excel pudiera estar duplicado en miles de ordenadores, con la seguridad de que nadie lo puede alterar maliciosamente pero cuando legítimamente se deba modificar algo, en cuestión de segundos, todos se sincronizan para registrar el cambio. Aunque uno de los miles de ordenadores desapareciese de la red no pasaría nada. Esto es lo que consigue la tecnología *blockchain* y aunque su "magia" es mucho más compleja y compuesta de más piezas como la criptografía, en esencia eso es lo que busca: un registro distribuido resistente y seguro en donde los miles de usuarios que participen en la red reemplacen a una autoridad central, quien validaba las transacciones.

Gartner[12] define a la *blockchain* como un mecanismo digital para crear un libro de registros digital y distribuido, en el cual dos o más participantes integrantes de una red *peer-to-peer* pueden intercambiar información y activos de manera directa, sin intermediarios. La *blockchain* autentica a los participantes, valida que éstos tengan los activos sobre los que quieren tranzar, y registra los intercambios en dicho libro de registros digital, del cual todos los partícipes tienen una copia actualizada y cuyos asientos o registros, que no son modificables, son cronológicamente organizados y empaquetados en bloques, encriptados, y vinculados unos a otros.

Para efectos del presente artículo, resulta importante desarrollar en forma general algunos conceptos técnicos de la tecnología *blockchain* a efectos de entender su funcionamiento. Para ello es necesario entender cuáles son los pasos que se deben tomar para realizar una transacción en una *blockchain*. En general, la secuencia de pasos en la *blockchain* de Bitcoin es la siguiente[13]:

a) Una persona desea realizar una transacción. Para ello requiere de una *wallet* y a su vez necesita conocer la clave pública de la otra persona con la que quiere realizar la operación en la *blockchain*.

b) Esta transacción se envía a una red *peer-to-peer* compuesto por todas las computadoras que participan en la red de la *blockchain* específica. A estas computadoras son las que se conocen como nodos.

c) La red de nodos verifica que la transacción esté firmada y a su vez el usuario disponga de recursos necesarios para poder realizarla. Dependiendo de los parámetros de la red, la transacción se verifica instantáneamente o se transcribe en un registro seguro y se ubica en una fila de transacciones pendientes. En este caso, los nodos determinan si la transacción es válida basándose en un conjunto de reglas que la red ha acorda-

12. Confr. Gartner, Inc., The real business of blockchain, escrito por David Furlonger y Christophe Uzureau, y publicado en 2019 por Harvard Business Review Press, p.10.

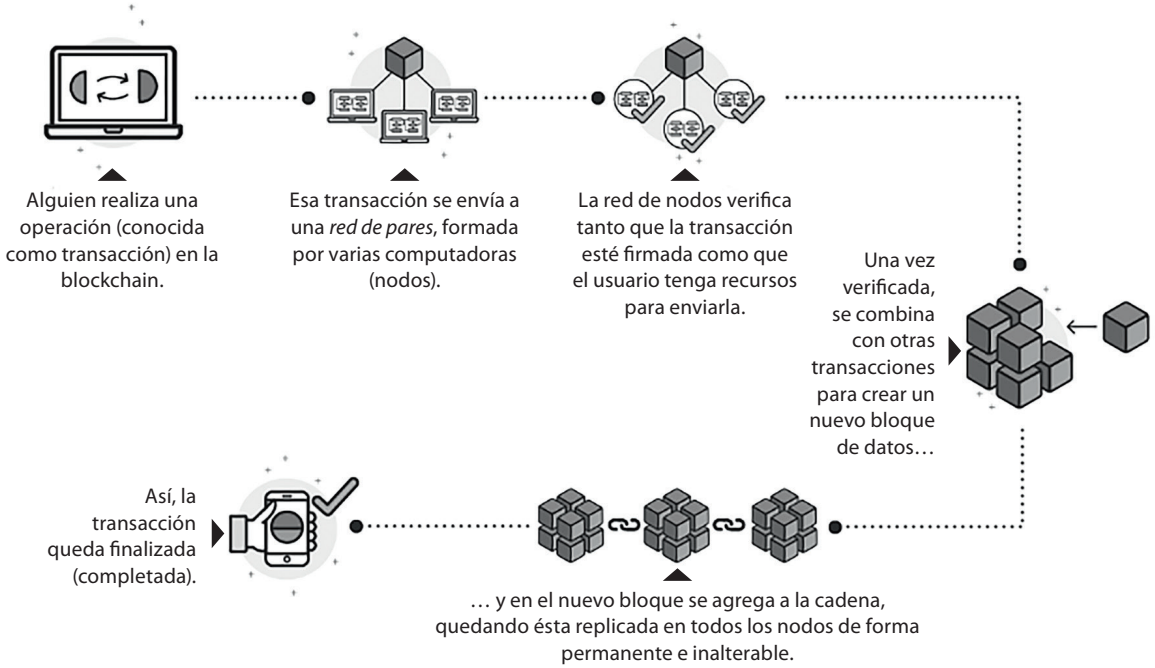
13. Es importante mencionar que la secuencia de pasos de una transacción va a cambiar dependiendo de la blockchain. Esta secuencia varía si es que hablamos de un token, ya que en ese caso no se requiere de la dirección del destinatario, sino la dirección del *smart contract*.

do. En otras palabras, los nodos verifican la transacción tomando en consideración algunas reglas de validación establecidas por los creadores de la *blockchain* específica.

d) Las transacciones validadas se almacenan en un bloque y se sellan digitalmente con un hash. Cabe señalar que cada bloque está identificado por un *hash* creado mediante un algoritmo acordado por la red. Un bloque contiene un encabezado, una referencia al hash del bloque anterior y un grupo de transacciones. La secuencia de *hash* vinculados crea una cadena segura e interdependiente.

e) Los bloques deben ser validados primero para ser añadidos a la cadena de bloques. La forma de validación más aceptada para las cadenas de bloques de código abierto es a través de un protocolo de consenso denominado "*Proof of Work*", que, en términos simples, es dar solución a un rompecabezas matemático derivado del encabezado del bloque. Los mineros intentan "resolver" el bloque haciendo cambios que incrementan en una variable hasta que la solución satisface el objetivo de toda la red.

f) Cuando un bloque es validado, los mineros que resolvieron el rompecabezas son recompensados y el bloque se distribuye a través de la red. Cada nodo añade a su registro el bloque a la cadena mayoritaria, volviéndose inmutable y auditable. Ahora la transacción forma parte de la cadena de bloques y no puede ser alterada de ninguna manera.



Fuente: Imagen recuperada del Sitio Web de Blockchain Federal Argentina

Para comprender esta secuencia en una transacción en *blockchain* es indispensable comprender los siguientes conceptos:

1. Wallet.

Las transacciones se realizan desde las *wallets*. Una *wallet* es una interfaz que permite conectarte con tu "cuenta" en *blockchain*. En otras palabras, una *wallet* es una herramienta que uno utiliza para interactuar con una red *blockchain*, a través de las cuales los usuarios almacenan y gestionan sus criptomonedas. Una *wallet*, al igual que la billetera que tenemos en nuestros bolsillos, se utiliza principalmente para tener acceso a los criptoactivos. Sin embargo, a di-

ferencia de su homólogo tradicional, también permite realizar transacciones, como una aplicación de banca por internet. En ese sentido, se denomina *wallet* porque al igual que sucede con el dinero, la moneda es con lo que pagas y la cartera es donde las guardas.

A efectos de graficar mejor una *wallet*, realizaremos el símil con un banco y su aplicación. Cuando uno decide abrir una cuenta bancaria, si no cuenta con una aplicación no podrá visualizar su saldo en tiempo real. Es por ello que el usuario descarga la *app*, inicia sesión con su número de usuario, contraseña y demás credenciales a fin de ver con cuánto dinero dispone. En buena cuenta, la aplicación es una interfaz que permite visualizar el saldo que uno tiene en su cuenta bancaria. En la tecnología *blockchain*, ocurre algo similar. Si uno desea realizar transacciones necesita crearse una cuenta; sin embargo, para poder leer de forma simplificada lo que se encuentra en una *blockchain*, se requiere de una wallet en donde uno podrá consultar el saldo de sus criptoactivos, permitiendo que el usuario pueda consultar su saldo, realizar transacciones entre distintas redes y firmar sus propias transacciones, evitando así la participación de intermediarios, como ocurre en el sistema financiero tradicional.

Las *wallets* utilizan mecanismos criptográficos de seguridad para firmar, acceder y cifrar las transacciones, los bloques y su encadenado. Esto permite que se puedan efectuar movimientos de valor entre usuarios sin que intervengan terceros en el proceso. Es decir, descentraliza la gestión y ofrece a sus participantes un libro de registro que permanece en el tiempo de manera segura y fiable: la *blockchain*.

Contrario a lo que se cree, las *wallets* no almacenan realmente activos digitales. En cambio, proporcionan las herramientas necesarias para interactuar con una *blockchain*, ya que están conformadas por una clave pública y una clave privada[14]. La clave pública está compuesta por una dirección de números y letras. Como su nombre indica es pública por lo cual puede ser compartida con otros usuarios. Asimismo, es de suma importancia la clave privada, la cual está integrada por una serie de números generados criptográficamente. Lo que permite confirmar las transacciones de salida y movilizar los fondos exclusivamente por el propietario. En conclusión, en la *wallet* ambas claves están relacionadas, ya que la pública se genera siempre a partir de la privada.

En buena cuenta, una clave pública será como entregar el número de cuenta de un banco, mientras que la clave privada es el pin y contraseña que el titular de la cuenta utiliza para acceder y gestionar su cuenta. Es en este punto donde radica la importancia del cuidado de las claves privadas, ya que quien tenga acceso a la *wallet* tendrá el control absoluto de la cuenta. Por lo tanto, si alguien obtiene acceso a las claves privadas, tendrá acceso a las criptomonedas que se encuentran en la *blockchain* y podrá disponer de ellas. Como bien señaló Andreas M. Antonopoulos, autor del libro Mastering Bitcoin: Unlocking Digital Cryptocurrencies:

"La clave privada debe permanecer secreta en todo momento porque revelarla a terceros equivale a darles control sobre los bitcoins asegurados por esa clave. También se debe hacer una copia de seguridad de la clave privada y protegerla de pérdidas accidentales, porque si se pierde no se puede recuperar y los fondos asegurados por ella también se pierden para siempre".

En resumen, tal como lo comenta Heredia Querro, es importante entender que una *wallet* no

14. Para entender mejor el concepto de claves públicas y privadas, utilizaremos el siguiente ejemplo. Pensemos en un buzón de correo que se utiliza para recibir cartas físicas. Para que alguien pueda enviar una carta al buzón de correo, tiene que saber la dirección y número del dueño del buzón. Y el dueño, a su vez, debe de tener una llave para abrir el buzón y recoger sus pertenencias. Del mismo modo, al igual que cualquier persona puede saber cuál es la dirección de la casa al que le están enviando las cartas, cualquier persona puede conocer cuál es la clave pública para enviar criptoactivos. Y para acceder a esos criptoactivos, el titular de la cuenta necesitará su clave privada.

funciona como una billetera en el sentido tradicional y *off-chain*. En efecto, la *wallet* per se no contiene criptomonedas; sólo contiene la/s llave/s pública/s y privada/s de una persona. Cuando una persona envía a otra bitcoins o cualquier otra criptomoneda, lo que en realidad hace es (i) firmar una transferencia "dominial" de dichas monedas a favor de la dirección –llave pública– de una *wallet* de otra persona, y (ii) quien las recibe, para poder gastarlas –i.e., transferirlas nuevamente– debe a su turno ingresar –i.e. firmar– con su llave privada, que está criptográficamente asociada a su llave pública contenida en la *wallet*, la que también le permite ver el saldo de todas sus tenencias.

Por otro lado, es importante mencionar que existen distintos tipos de *wallets*:

a) *Exchange Wallets*: Este tipo de *wallets* son bastante sencillas y fáciles de configurar, es por ello que son las más populares. Estas *wallets* se hospedan directamente en las plataformas como Binance, Kraken o Coinbase, en donde uno compra sus criptomonedas. En este tipo de *wallet*, son los *Exchanges* quienes suelen custodiar las claves privadas. Una de las ventajas de los *Exchanges* frente a las *cold wallets* es que, en estas últimas, si un usuario pierde la clave privada de su *wallet*, no podrá recuperar el dinero, dado que no existe la posibilidad de reestablecer la clave. En cambio, en un *Exchange*, sí existe la posibilidad de reestablecer la contraseña, sin ningún tipo de problema, y el dinero permanece intacto. Por otro lado, una de las desventajas es que, en un *Exchange*, el usuario no tiene posesión sobre las criptomonedas, ya que el *Exchange* retiene y administra los fondos en nuestro nombre.

b) *Hot Wallets*: Una *hot wallet* o billetera caliente es cualquier *wallet* que está conectada a Internet. Generalmente, es un software de descarga gratuita para el ordenador o smartphone. En el caso de las *hot wallets* para teléfonos celulares, éstas resultan muy cómodas, puesto que tienen la opción de recibir y enviar criptomonedas mediante el escaneo de cogidos QR. Entre las hot wallets más populares encontramos a *Metamask* y a *Trust Wallet*.

c) *Cold Wallets*: Una *cold wallet* o billetera fría es aquella que no cuenta con conexión a Internet. En su lugar, utilizan un medio físico parecido a un *pen drive* o memoria USB para almacenar las claves fuera del entorno digital, lo que las hace resistentes a los intentos de ciberataques. Este tipo de *wallet* ofrece una enorme ventaja sobre las demás, ya que hacen el rol de una cuenta bancaria de ahorros. Cabe señalar que son las más empleadas por los usuarios para depositar y resguardar grandes cantidades de criptomonedas y, ofrecen un nivel de seguridad insuperable. En ese sentido, es especialmente idóneo para inversores a largo plazo o "*Hodlers*".

Finalmente, desde un punto de vista más antropológico y social, Gary Vaynerchuck sostiene que las *wallets* van a ser parte de nuestra identidad social. Así como actualmente subimos fotos a Instagram, videos a TikTok, opiniones en Twitter, el siguiente paso será coleccionar NFTs en nuestras *wallets*[15].

2. Nodos.

Un nodo de red es un punto en el que se puede crear, recibir o transmitir un mensaje. Los nodos son la base fundamental de la tecnología *blockchain*. Gracias a estos podemos crear una enorme red de computadores interconectadas que comparten información de forma segura, rápida y descentralizada, además de permitirnos disfrutar de todas las bondades que la tecnología *blockchain* puede ofrecernos.

En otras palabras, un nodo es, en general, un punto de conexión físico o virtual donde se puede crear, enviar y recibir toda clase de datos e información. Así, desde el punto de vista de

15. Recuperado de: https://podclips.com/ct/zScaIR

la tecnología *blockchain*, los nodos se constituyen por todos aquellos ordenadores que están interconectados a la red de un criptoactivo, ejecutando el software que se encarga de todo su funcionamiento. En tal sentido, un nodo es simplemente un ordenador o servidor que está conectado a una red. Cuando un nodo se conecta a la red por primera vez, descarga una copia completa de la base de datos *blockchain*. Es gracias a esta esencial pieza dentro de la red, que es posible crear transacciones, compartirlas, minarlas, crear y compartir los beneficios de la tecnología *blockchain* a quienes participen de una.

Al sumergirse en el mundo de la tecnología *blockchain*, que están diseñados como sistemas distribuidos, la red de nodos informáticos es lo que hace posible que Bitcoin, por ejemplo, se utilice como una moneda digital descentralizada de igual a igual —*P2P*— que es resistente a la censura por diseño, y no requiere que un intermediario sea tramitado de un usuario a otro —sin importar cuán distantes estén en el mundo—.

Si bien Bitcoin fue la primera criptomoneda en utilizar una red de nodos para operar de forma descentralizada y autónoma a través de la *blockchain*, ésta no fue la primera en crear o introducir el concepto de nodo de una red *P2P*, ya que Napster fue la empresa que popularizó este concepto de red distribuida de forma masiva entre los usuarios.

Cabe señalar que cualquier persona que desee unirse y contribuir con la red del sistema Bitcoin, puede hacerlo libremente con tan sólo descargar e instalar el software de Bitcoin Core en su computadora. En el momento en que varios equipos de cómputo comienzan a ejecutar el software de Bitcoin Core del sistema Bitcoin empieza a formarse la red P2P. Cuando un nodo se conecta a la red por primera vez, descarga una copia completa de la base de datos registrada en la blockchain. A medida que más nodos se conecten, la base de datos se sincronizará entre ellos. Este proceso se repite con cada nuevo nodo agregado a la red, intercambiando información para que todos funcionen de forma coordinada. Así la *blockchain* de Bitcoin opera como un sistema descentralizado. Esto por lo que los nodos deben compartirse y distribuirse la responsabilidad de crear, almacenar y transmitir la información dentro de la red. No existen niveles ni jerarquías, en la *blockchain* de Bitcoin todos los nodos operan por igual. Una vez conectados, los nodos pueden realizar distintas funciones. Como por ejemplo la retransmisión o almacenamiento de dato o servicio de envío o recepción de operaciones[16].

Al respecto, debemos manifestar que existen distintos tipos de nodos en la red Bitcoin:

a) **Nodos Completos:** Son aquellos equipos de computación u ordenadores que implementa el cliente de Bitcoin, siendo el más común Bitcoin Core, y almacenan una copia exacta, completa y actualizada, de la *blockchain* de Bitcoin. Los nodos completos son los que hacen cumplir todas las reglas del protocolo Bitcoin y, por tanto, son los que verdaderamente le brindan robustez, seguridad y estabilidad a la red.

b) **Supernodos:** Un supernodo es un nodo completo que es públicamente visible. Se comunica y proporciona información a cualquier otro nodo que decida establecer una conexión con él. Por lo tanto, un supernodo es básicamente un punto de redistribución que puede actuar como fuente de datos y como puente de comunicación. Un supernodo, generalmente, se ejecuta las 24 horas del día, los 7 días de la semana y tiene varias conexiones establecidas, transmitiendo el historial de la *blockchain* y los datos de las transacciones a múltiples nodos en todo el mundo. Por esa razón, un súper nodo probablemente requerirá más poder de cómputo y una mejor conexión a Internet en comparación con un nodo completo que está oculto.

16. Bit2me Academy. Recuperado de: https://academy.bit2me.com/que-es-un-nodo/

c) Nodos de minería: Son aquellos nodos completos que, además de almacenar una copia completa de la *blockchain*, también ejecutan un software de minería.

3. Minería.

La minería es el proceso mediante el cual las transacciones de criptomonedas entre usuarios son verificadas y agregadas a la *blockchain*. Como mencionamos anteriormente, la minería básicamente es el proceso de resolución de un problema matemático mediante recursos computacionales intensivos. La minería de criptomonedas designa el proceso de verificación y validación de transacciones de una *blockchain*. Este es uno de los elementos clave que permite a la *blockchain* funcionar como un libro de registros distribuido, ya que son quienes realizan este trabajo los que verifican y validan las transacciones sin la necesidad de una autoridad central.

Por lo general, quienes diseñan una *blockchain* deben incentivar a aquellos usuarios que van a validar las transacciones a fin de reemplazar al tercero de confianza o autoridad central. Para ello se les otorga un incentivo económico. Como bien señala Javier Ibáñez Jimenez[17]:

> *"Cualquier miembro de la red puede enviar datos para registrarlos si se cumplen las reglas de introducción o validación prefijadas, y cualquier nodo que esté autorizado al efecto puede recuperar datos. Para introducir datos, como se ha avanzado, es ineludible que se sigan las reglas de un protocolo o procedimiento de "minado", que en esencia consiste en la composición correcta de los pasos necesarios para obtener la encriptación o cifrado de los datos que se persigue introducir en la red. Tal seguimiento, necesariamente, exige un esfuerzo consistente en el uso de aquella capacidad computacional —con el consiguiente gasto eléctrico que comportan, y el coste humano del control de las operaciones, así como la amortización del equipo informático empleado—, y, por esto, para hacer este uso racional y eficiente, se suele recibir un premio o incentivo económico, que igualmente es fijado y recibido por el "minero" conforme a reglas prefijadas —por ejemplo, recibiendo una moneda virtual a la que la red atribuya por convenio un valor económico—.*
>
> *Además de incurrir en los costes que acarrea la computación necesaria para encriptar datos, quienes desean realizar transacciones han de resolver un problema matemático, igualmente según las reglas fijadas por los creadores del sistema. Especialmente en redes abiertas, públicas o sin restricciones de uso, es habitual que muchos nodos estén realizando un esfuerzo computacional simultáneo para resolverlo, pero solo algunos lo van consiguiendo. A mayor esfuerzo —y capacidad de computación—, mayor probabilidad hay de encontrar la solución y así cerrar una transacción, esto es, introducir datos en la blockchain".*

Un ejemplo que grafica cómo es que funciona la minería es el siguiente: Imaginemos que el acertijo *hash* establece que quien antes descubra el número del 0 al 1000, se lleva el premio. Los mineros irán lanzando números, hasta encontrar el número que coincida con el acertijo. Durante el proceso se irá preguntando si el número es correcto o no. Quien llegue antes al número correcto, gana el premio o lo que es lo mismo, se lleva la recompensa del bloque[18]. Cabe señalar que para resolver el *puzzle* se deben tomar en consideración los protocolos de consenso que detallaremos más adelante. Esto debido a que se necesita el acuerdo de las normas por todos los participantes. Actualmente, los protocolos de consenso más utilizados con el *Proof-of-Work* —POW— y el *Proof-of-Stake*.

Resulta preciso mencionar que la recompensa se genera cada vez que se agrega un nuevo bloque a la cadena. Esta recompensa se con-

17. Ibáñez, *Blockchain: primeras cuestiones en el ordenamiento español*, 16-17.

18. Bit2me Academy. Recuperado de: https://academy.bit2me.com/que-es-minar-criptomonedas/

forma de dos partes: Las comisiones que pagan los usuarios participantes de las transacciones que conforman el nuevo bloque añadido y las nuevas criptomonedas puestas en circulación. De allí que resulta tan atractivo para los mineros realizar grandes inversiones en sistemas computacionales con el fin de minar criptomonedas. Actualmente cada minero de Bitcoin recibe 6.25 bitcoins por cada bloque completado. En resumen, la minería hace posible que la blockchain *"esté encendida"* procesando datos sin tener que depender de un servidor central auspiciado por un intermediario.

4. Bloques.

En relación con ello, un elemento esencial en la *blockchain* son los propios bloques que conforman la cadena y permiten su funcionamiento. Al respecto debemos señalar que cada bloque tiene en su conformación lo siguiente:

a) Datos de las transacciones del bloque: Las operaciones que se realizan para agregar información a una blockchain son denominadas transacciones. Una transacción se da cuando dos partes, "A" y "B" deciden intercambiar una unidad de valor —criptomoneda o token—. Cada transacción es enviada a la red a través de un nodo, y se combina con otras transacciones para conformar un bloque. Cuando ese bloque se agrega a la cadena, la transacción queda incorporada definitivamente y se considera como "*completada*". En un concepto básico, una transacción es un envío o transferencia de un valor entre dos partes.

Tal como su nombre lo señala, una parte elemental de la *blockchain* son los propios bloques, los cuales son esenciales en la construcción de la cadena y permiten su funcionamiento. Cada bloque contiene información acerca de eventos que han ocurrido recientemente. Esta información puede ser de la más variada índole, desde la compra de productos, transferencias de propiedad, registros de propiedad, o cobros de regalías por cualquier concepto.

En otros términos, en una *blockchain* todas y cada una de las transacciones se agrupan en bloques, que no son más que «*paquetes*» con la información sobre las últimas transacciones realizadas en un determinado periodo de tiempo. Estos bloques se van añadiendo de forma sucesiva al registro en la red a medida que se van formando. Cuando un bloque de información se incorpora a la blockchain, queda irreversiblemente vinculado al bloque aprobado anteriormente, de modo que se encadenan entre ellos, y de ahí que esta tecnología se denomine «cadena de bloques». Esta vinculación entre los bloques es posible gracias a un robusto sistema criptográfico, que convierte las redes blockchain en registros prácticamente inalterables.

b) Hash: El "*hashing*" alude al proceso de generar un output de extensión fija, a partir de un input de extensión variable. Esto se logra mediante el uso de unas fórmulas matemáticas denominadas funciones *hash* —y que se implementan como algoritmos *hashing*—[19]. En ese sentido, un hash es la expresión alfanumérica del empleo digital de determinadas funciones criptográficas de enlace o engarce de datos, aplicadas conforme a las reglas concretas de minado o creación de transacciones propias o específicas de cada *blockchain*. Los hashes, por otra parte, se caracterizan por su necesaria y exclusiva generación automática, desde los nodos de la red, por parte los mineros o autorizadores —a veces llamados validadores— de transacciones[20].

Un *hash* es el resultado de una función *hash*, la cual es una operación criptográ-

19. Binance Academy. Recuperado de: https://academy.binance.com/es/articles/what-is-hashing

20. Ibáñez, *Blockchain: primeras cuestiones en el ordenamiento español*, 19.

fica que genera identificadores únicos e irrepetibles a partir de una información dada. Los *hashes* son una pieza clave en la tecnología *blockchain* y tiene una amplia utilidad. Estas funciones tienen como objetivo primordial codificar datos para formar una cadena de caracteres única. Todo ello sin importar la cantidad de datos introducidos inicialmente en la función. Estas funciones sirven para asegurar la autenticidad de datos, almacenar de forma segura contraseñas, y la firma de documento electrónicos.

Un *hash*, en términos prácticos, es la huella digital del contenido que estamos empaquetando. Un *hash* es inalterable porque si cambiamos el contenido, el hash de forma automática cambia. Esto significa que un *input* con contenido distinto producirá un *output* diferente. Para graficarlo, procesaremos las palabras "*Binance*" y "*binance*" mediante el algoritmo *hashing* SHA-256 —que es el utilizado por Bitcoin—.

SHA-256	
Input	Output
Binance	f1624fcc63b615ac0e95daf9ab78434ec2e8ffe402144dc631b055f711225191
binance	59bba357145ca539dcd1ac957abc1ec5833319ddcae7f5e8b5da0c36624784b2

Tal como se puede apreciar, un cambio menor —la mayúscula de la primera letra— produce como resultado un valor de *hash* radicalmente distinto. Pero dado que estamos empleando el SHA-256, los outputs tendrán siempre una extensión fija de 256 bits —o 64 caracteres—, independientemente del tamaño del *input*. Asimismo, no importará la cantidad de veces que se procesen las dos palabras a través del algoritmo, los dos outputs se mantendrán inalterables.

En ese sentido, el *hashing* resulta útil cuando es necesario lidiar con cantidades enormes de información. Por ejemplo, es posible procesar un archivo grande o un conjunto de datos a través de una función hash, y a continuación utilizar su output para rápidamente verificar la exactitud e integridad de los datos. Esto es posible debido a la naturaleza determinística de las funciones hash: el input producirá siempre un output simplificado y condensado —hash—. Dicha técnica elimina la necesidad de almacenar y recordar grandes cantidades de datos. Asimismo, un hash se utiliza para asegurar la integridad de la información, ya que las alteraciones de los valores son fácilmente detectables.

Por tanto, entre las principales características de las funciones hash, se pueden mencionar las siguientes[21]:

i. Son fáciles de calcular. Los algoritmos de *hash* son muy eficientes y no requieren de grandes potencias de cálculo para ejecutarse.
ii. Es compresible. Esto quiere decir que, sin importar el tamaño de la entrada de datos, el resultado siempre será una cadena de longitud fija. En el caso de SHA-256, la cadena tendrá una longitud de 64 caracteres.
iii. Funcionamiento tipo avalancha. Cualquier mínimo cambio en la entrada de datos, origina un hash distinto a la entrada de datos original.
iv. Resistencia débil y fuerte a colisiones. Hace referencia a que es imposible calcular un *hash*, que permita encontrar otro hash igual. Mejores conocidos como preimagen y segunda preima-

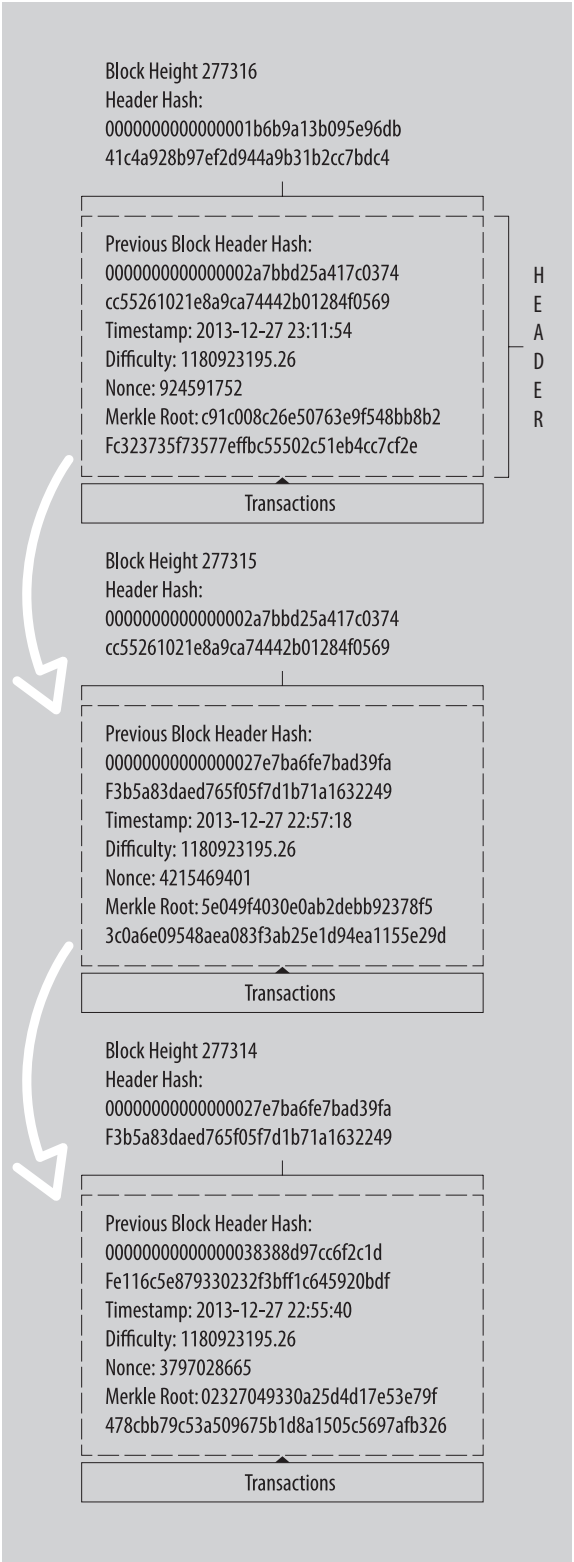
21. Bit2me Academy. Recuperado de: https://academy.bit2me.com/que-es-hash/

gen, es el concepto base de la seguridad de los hashes.

v. Son irreversibles. Tomar un *hash* y obtener los datos que dieron origen al mismo, en la práctica no puede ser posible. Esto es uno de los principios que hacen a los hashes seguros.

En lo que respecta a la conformación de un bloque, debemos señalar que se contempla tanto el *hash* del bloque y el *hash* del bloque anterior. Cada bloque hace referencia a un bloque anterior, conocido como el bloque padre, a través del campo «*hash de bloque anterior*» en la cabecera del bloque. La secuencia de los *hashes* que unen cada bloque a su padre crea una cadena que se remonta hasta el primer bloque jamás creado, conocido como el «*bloque génesis*».

Al tener el *hash de bloque anterior* dentro de la cabecera del bloque, el *hash del bloque anterior* afecta al *hash del bloque actual*. La identidad propia del hijo cambia si la identidad de los padres cambia. Cuando el padre se modifica de alguna manera, los cambios de *hash* de los padres también cambian. Cuando el *hash* del padre cambia requiere un cambio en el puntero *hash de bloque anterior* del hijo. Esto a su vez hace que el *hash* del hijo cambie, lo que requiere un cambio en el puntero del nieto, que a su vez cambia el nieto, y así sucesivamente. Este "*efecto cascada*" asegura que, una vez que un bloque tiene muchas generaciones siguientes, no puede ser cambiado sin forzar un nuevo cálculo de todos los bloques siguientes. Debido a que un nuevo cálculo requeriría una computación enorme, la existencia de una larga cadena de bloques hace que la historia profunda de la cadena de bloques sea inmutable, que es una característica clave de la seguridad de la tecnología *blockchain*[22].



22. Recuperado de: https://aprendeblockchain.wordpress.com/fundamentos-tecnicos-de-blockchain/la-cadena-de-bloques/

c) Timestamp: El *timestamp* o marca de tiempo es un pequeño dato almacenado en cada bloque a modo de serial único y que tienen como principal función determinar el momento exacto en el que el bloque ha sido minado y validado por la red *blockchain*. Cabe señalar que, estos sellos de tiempo ayudan a la red a determinar cuánto tiempo se lleva en extraer los bloques de un determinado período y de allí se ajusta el parámetro de dificultad de la minería.

d) Nonce: Significa "*number that can be only used once*" o "*número de un solo uso*". En tal sentido, es un número aleatorio único que identifica a cada bloque. La existencia de los números aleatorios o *nonce*, nos resulta de vital en criptografía. Esto se debe a que la generación y utilización de números aleatorios garantiza la seguridad de las funciones criptográficas. Por lo que dicha generación debe ser realmente aleatoria. Es decir, no debe seguir ningún patrón reconocible. Porque en caso contrario, resultaría muy sencillo romper los sistemas criptográficos que mantiene la seguridad de nuestras vidas digitales en la actualidad. En Bitcoin, el *nonce* es usado para generar un *Block ID* o *hash* de bloque en Bitcoin.

En resumen, podemos señalar que cada bloque de información está *hasheado*, lo que significa que está criptográficamente vinculado al anterior y encriptado. Asimismo, cada bloque contiene una referencia al bloque anterior, una lista de las transacciones incluidas en él, una estampa temporal, y una prueba criptográfica que garantiza la veracidad de la información.

V. CARACTERÍSTICAS DE UNA BLOCKCHAIN

A la vista de lo anteriormente expuesto, consideramos que existen seis características de la tecnología *blockchain* son especialmente relevantes en el planteamiento de las cuestiones jurídicas que suscitan las aplicaciones de esta tecnología. Estas características son las siguientes:

a) Inmutabilidad

La inmutabilidad es una de las características clave de la tecnología *blockchain*. La inmutabilidad significa que algo no puede ser cambiado o alterado. Esta es una de las características de la *blockchain* que ayuda a garantizar que la tecnología se mantenga como está: en una red permanente e inalterable[23].

La inmutabilidad se refiere a la capacidad de las blockchains para prevenir la alteración de transacciones que hayan sido ya confirmadas. A pesar de que estas transacciones remiten a menudo a la transferencia de criptomonedas, pueden referirse también al registro de otros tipos de datos digitales no monetarios[24].

Como consecuencia del encadenamiento sucesivo de los bloques basado en la criptografía —*los hash*—, el contenido de la cadena de bloques es inmutable. Si un nodo decide cambiar el contenido de la cadena de bloques alterando una transacción ya realizada e incluida en un bloque, provocará que el contenido de su versión del libro registro varíe, un cambio que será fácilmente identificable por el resto de los nodos. Por lo tanto, a la hora de someter a aprobación una nueva transacción, estos no aceptarán su versión del registro, puesto que el contenido será distinto.

En ese sentido, resulta extremadamente difícil cambiar las transacciones en una *blockchain*, porque cada bloque está vinculado al bloque anterior al incluir el *hash* del bloque anterior. Por consiguiente, cualquier mero intento de alterar la información de un bloque, se detecta fácilmente. Los intentos de manipulación se detectan rápidamente por el resto de nodos y

23. Rodríguez, Nelson. 6 características clave de la tecnología *blockchain* que debes conocer. Recuperado de: https://101blockchains.com/es/caracteristicas-tecnologia-blockchain/

24. Binance Academy. Recuperado de: https://academy.binance.com/es/articles/what-makes-a-blockchain-secure

se rechaza la cadena o el bloque con la información alterada. De este punto se deriva que sea resistente a la censura.

b) Consenso

Para cada *blockchain* existen una serie de normas que todos los miembros de la red deben cumplir. Estas reglas establecen el funcionamiento de la red y el mecanismo de validación de las transacciones y el proceso de generación de los bloques. Los protocolos de consenso garantizan la consistencia entre las distintas copias de un registro que se guardan en cada uno de los nodos de la red. Se consigue consenso cuando el protocolo puede asegurar que todos los nodos añaden los mismos nuevos bloques —con el mismo contenido— en su versión local de la *blockchain*. El hecho de que todos los participantes respeten las normas definidas en el protocolo para decidir cómo actualizar la base de datos, es la fuente de confianza en el sistema[25].

En un esquema centralizado, una entidad única tiene poder sobre todo el sistema. En la mayoría de casos, podrá realizar los cambios que quiera –no existe ningún sistema de gobernanza complejo para alcanzar consenso entre muchos administradores. Pero en un esquema descentralizado, la historia cambia por completo. Digamos que estamos trabajando con una base de datos distribuida — "*¿cómo nos ponemos de acuerdo respecto a qué entradas añadir?*"—. Superar dicho desafío en un entorno en el que extraños no confían entre sí fue, quizás, el desarrollo más importante que allanó el camino a las *blockchains*[26].

En tal sentido, podemos afirmar que el consenso es parte fundamental del funcionamiento de la tecnología *blockchain* y las criptomonedas. Ello se debe a que es el pilar que garantiza la seguridad de la cadena de bloques, ya que controla el hecho de que todos los que participen en la red acepten de forma unánime la información que dicha cadena contiene. El consenso busca responder la siguiente pregunta: "*¿Cómo nos aseguramos de que estamos de acuerdo con la validación del bloque?*" La respuesta es: mediante un acuerdo entre los nodos de la red. Esto permite una especie de "auditoría" que impide que alguien pueda mandar información manipulada a la *blockchain*. Para evitar que se añadan bloques erróneos en la cadena de bloques, cada uno de esos bloques necesita una revisión y una confirmación[27].

Cada *blockchain* define su mecanismo de consenso. En la actualidad existen múltiples protocolos, entre los que destacan los siguientes:

i. ***Proof of Work — PoW*:** El *PoW* o *Prueba de Trabajo* es el protocolo de consenso pionero de la tecnología *blockchain*, el cual fue implementado por primera vez por la *blockchain* de *Bitcoin*. Usando el protocolo de *Proof of Work*, con cada nuevo bloque creado se deberá resolver un acertijo matemático que solo puede ser resuelto mediante prueba y error. Estos acertijos son resueltos por los mineros, haciendo millones de intentos. Resolver el acertijo dará como resultado la creación del bloque, la confirmación de las transacciones involucradas en ese bloque y la generación de nuevos bitcoins que recibirá el minero como recompensa junto a las comisiones implícitas en cada una de las transacciones.

El *Proof of Work* funciona de la siguiente manera[28]:

25. Finck, Michele. 2018. Blockchain Regulation and Governance in Europe. Cambridge University Press, 20.

26. Binance Academy. Recuperado de: https://academy.binance.com/es/articles/what-is-a-blockchain-consensus-algorithm

27. Bit2me Academy. Recuperado de: https://academy.bit2me.com/consenso-criptomonedas/

28. Bit2me Academy. Recuperado de: https://academy.bit2me.com/que-es-proof-of-work-pow/#:~:text=El%20protocolo%20de%20Prueba%20de,los%20recursos%20de%20dicha%20red

"Etapa #1: El cliente o nodo establece una conexión con la red. En este punto, la red le asigna una tarea computacionalmente costosa. Esta tarea debe ser resuelta a los fines de recibir un incentivo económico.

Etapa #2: Comienza la resolución del acertijo. Esto conlleva el uso de mucha potencia de computación hasta resolver el enigma entregado. Este proceso es el que recibe el nombre de minería.

Etapa #3: Una vez resuelta la tarea computacional, el cliente comparte esta con la red para su verificación. En este punto, se verifica rápidamente que la tarea cumpla con los requisitos exigidos. Si lo hace, se brinda acceso a los recursos de la red. En caso contrario, se rechaza el acceso y la solución presentada del problema. Es en este punto, donde se realizan las verificaciones de protección contra el doble gasto. Una protección que evita, que se presente más de una vez, una tarea ya asignada y verificada por la red.

Etapa #4: Con la confirmación que la tarea ha sido cumplida, el cliente accede a los recursos de la red. Gracias a esto, recibe una ganancia por el trabajo computacional realizado".

La Prueba de Trabajo garantiza grandes niveles de seguridad, si la red está formada por miles de mineros. De hecho, mientras más mineros más segura es la red. Esto lo hace ideal para su uso en la formación de enormes redes distribuidas. Sin embargo, este método es cuestionado por su impacto en el medio ambiente, dado que el intensivo trabajo computacional de PoW necesita de grandes cantidades de energía eléctrica.

ii. ***Proof of Stake — PoS*:** El *Proof of Stake* es un protocolo de consenso creado para reemplazar al conocido *Proof of Work*. El objetivo de este algoritmo, al igual que en *PoW*, es crear consenso entre todas las partes que integran la red. El protocolo *PoS* utiliza un proceso de elección pseudoaleatorio para seleccionar un nodo para que sea el validador del siguiente bloque, basado en una combinación de factores que podrían incluir la edad de la moneda, la aleatorización y la riqueza del nodo. En *PoS*, no presentas un recurso externo como, por ejemplo, el consumo eléctrico o el hardware que inviertes para el proceso de minado; sino que se necesita de un recurso interno como la criptomoneda.

Los usuarios que quieran participar en el proceso de validación deben bloquear una cierta cantidad de sus criptomonedas en la red. Aquellos que tengan mayores reservas tendrán mayores posibilidades de ser seleccionado como el siguiente validador para forjar el siguiente bloque. Sin embargo, para que el proceso no favorezca solo a los nodos más ricos de la red, se agregan métodos más únicos al proceso de selección. Los dos métodos más utilizados son "*Selección aleatoria de bloques*" y "*Selección de la edad de la moneda*".

Cabe señalar que el PoS es una tecnología más respetuosa con el medio ambiente. Esto es gracias a que no necesita de potentes máquinas para actividades de minería. Lo que significa que su consumo energético es reducido.

c) Trazabilidad

La tecnología *blockchain* permite recorrer cada bloque y, por tanto, trazar todas las operaciones que se han realizado sobre una determinada dirección o retroceder en el tiempo y revisar las transacciones que se hicieron en una fecha determinada explorando todos los bloques generados en la fecha indicada. Esta caracteriza permite que la cadena de bloques pueda ser auditada y permite visualizar cualquier transacción.

En ese sentido, para distintas industrias, la tecnología *blockchain* representa un nuevo horizonte de oportunidades para el monitoreo de actividades, movimiento de activos y productos, ya que permite rastrear las distintas operaciones de una cadena de suministro, logística y

administrativa de un producto o servicio, generando un historial detallado.

d) Transparencia

Una red *blockchain* no solo puede rastrear pedidos, pagos o procesos de producción, por ejemplo, sino que todas las personas que forman parte de ese proceso pueden conocer todos los detalles de la transacción de principio a fin, lo que aporta confianza en toda una cadena de valor.

Partiendo de la base de que todos los usuarios de las redes *blockchain* tienen acceso al libro registro, ello implica que todos tienen la información sobre las transacciones que se efectúan por el grupo. Es más, en determinadas redes —no en todas—, los usuarios que no forman parte de la red también pueden consultar el contenido de la cadena de bloques. Así ocurre, por ejemplo, en las redes Bitcoin o Ethereum. A esto se añade, además, que se trata de protocolos informáticos de código abierto, por lo que el acceso al diseño de la programación es también libre.

Esta transparencia, sin embargo, no significa que podamos conocer al autor de las transacciones en todo caso. En algunos tipos de redes los usuarios no necesitan identificarse de forma personal para acceder y operar en la correspondiente red *blockchain*. Las transacciones son visibles, pero vinculadas a un código. Esta característica ha ocasionado que se hayan vinculado algunas de estas redes a actividades ilícitas por el carácter anónimo en la actuación que permiten en ciertos casos[29].

e) Autenticación

Otro elemento importante en el uso de *blockchain* para el intercambio de valor es la posibilidad de vincular transacciones con usuarios. De esa manera podremos saber quién ha transferido un activo digital a quién. La criptografía asimétrica hace posible esta función de autenticación. El sistema genera pares de claves vinculadas: una pública —puede ser conocida por todos— y otra privada —sólo conocida por una parte—. Lo que cifra una solo lo puede descifrar la otra. Si el dueño de una clave privada envía un mensaje, cualquier persona con la clave pública vinculada podrá descifrar el mensaje. Esta acción es lo que se considera la firma electrónica y permite comprobar el origen fidedigno de un mensaje o transacción. La efectividad de los algoritmos asimétricos depende de funciones matemáticas de un solo sentido, que requieren relativamente poca potencia de cálculo para ejecutarse, pero muchísima potencia para calcular la inversa.

Para enviar un mensaje seguro a una persona, éste se codifica con la clave pública del destinatario. El sistema garantiza que el mensaje resultante sólo puede ser descodificado con la clave privada del destinatario. Dado que se tiene la certeza de la identidad de dicho destinatario gracias a su clave pública, aseguramos que el mensaje llega al destinatario correcto. De este modo se consigue autenticación garantizando confidencialidad.

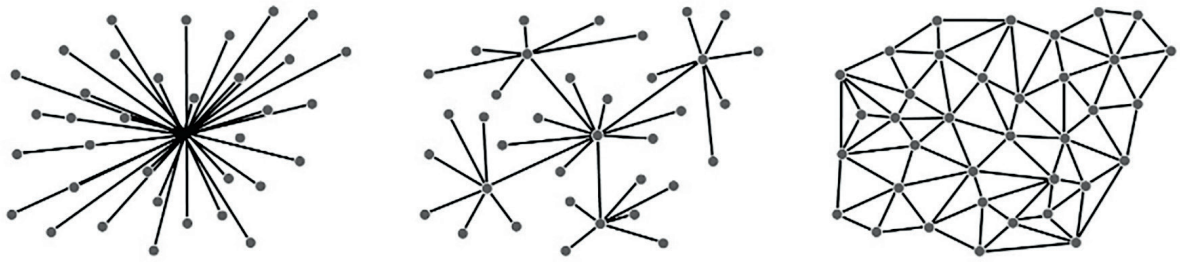
f) Confianza Distribuida y Descentralizada

Tal como se ha podido apreciar, la confianza se sustenta en las características desarrolladas anteriormente. A partir de lo afirmado por Vitalik Buterin, cofundador de Ethereum, podemos precisar[30]:

"Distribuido significa que no todo el procesamiento de las transacciones se hace en el mismo lugar", mientras que descentralizado significa que no hay una única entidad que tenga control sobre todo el procesamiento".

29. Porxas, Nuria, y Conejero, María, *Tecnología Blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados*, 28.

30. Buterin, Vitalik. The Meaning of Decentralization. Recuperado de: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274



Para hacer posible el intercambio de valor entre partes que no se conocen y/o no confían entre sí, la sociedad ha ido habilitando sistemas y procesos que otorgan a las partes la suficiente garantía de que la transacción se produce de forma segura en el tiempo definido, por el valor deseado y entre las partes intervinientes. Dichos sistemas se fundamentan en la existencia de intermediarios o terceros de confianza en los que depositamos la responsabilidad de ejecutar las transacciones con las características acordadas. A su vez, dichos intermediarios son "controlados" por estructuras jurídicas, regulación e instituciones de supervisión que garantizan su buen funcionamiento. Todo ello implica, por un lado, un elevado coste social acumulado y, por otro, la confianza de las partes en la estructura de gobierno de una sociedad. En ese sentido, el nodo central que es controlado por una persona natural o jurídica es quien controla la interacción con los servicios —propios o ajenos— distribuidos en distintas localizaciones y/o entidades. Este es el caso de servicios tradicionales como los bancos, aerolíneas, redes sociales, compañías de almacenamiento en nube, entre otras.

La gran revolución que supone *blockchain* es lograr la confianza en la autenticidad de las transacciones sin necesidad de esos intermediarios a través de protocolos informáticos. Las redes de registro distribuido serían "artefactos" tecnológicos que reemplazan la confianza organizativa. Es decir, se sustituye la confianza en estructuras humanas o instituciones por confianza en tecnología. Así, Satoshi Nakamoto en el *whitepaper* de *Bitcoin* alude a la naturaleza descentralizada de la confianza: "*un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, que permite a dos partes dispuestas realizar transacciones directamente entre sí sin la necesidad de un tercero de confianza*".

La firma auditora PWC resume tres razones por las que la tecnología *blockchain* genera confianza en los usuarios[31]:

i. "Utiliza una función criptográfica que en esencia es un algoritmo matemático para almacenar los datos y metadatos de una transacción, que no solo resulta compleja, sino que además es única. Es decir, un conjunto de datos tendrá un único código criptográfico o "hash", si un dato se altera se cambia ese código en consecuencia.

ii. El concepto de cadena: cada nueva transacción añade un nuevo bloque que se une a la cadena y éste además de su propia información, contiene información del bloque anterior. Esto permite que, si un usuario altera la información de un bloque, altere todos los bloques siguientes, invalidando la cadena. Corregir algo así requeriría un gran poder de cómputo por lo que se vuelve costoso.

31. Recuperado de: https://www.pwc.com/ia/es/publicaciones/perspectivas-pwc/Blockchain-brindando-confianza-y-transparencia.html#:~:text=Blockchain%20o%20Cadena%20de%20Bloques,Su%20funci%C3%B3n%20es%20crear%20confianza

iii. Aunque parezca paradójico, el hecho de que sea un modelo sin un control central, lejos de ser un punto en contra, es lo que más fortalece la confianza, ya que esto permite dos cosas fundamentales:

a. La Transparencia, la misma información se distribuye entre todos los usuarios y la autenticidad se logra por consenso, es decir, todos validan la cadena de bloques y
b. La Disponibilidad, si un punto de la red se inhabilita la red sigue funcionando porque todos tienen la misma información, cosa que no sucede en una red centralizada".

VI. TIPOS DE BLOCKCHAIN

Existen varias formas de construir una red blockchain. Pueden ser públicas, privada o permisionadas.

1. Blockchains públicas:

Las *blockchains* públicas, como Bitcoin, son accesibles para cualquier usuario que cuente con un dispositivo con conexión a internet. Es decir, son aquellas cuya participación es abierta y libre. El protocolo está basado en código abierto y cualquier persona puede descargarlo en su ordenador y participar en la cadena. Este tipo de cadena de bloques únicamente requiere la descarga de la aplicación correspondiente y la conexión con un número determinado de participantes o nodos. El protocolo está basado en código abierto y cualquier persona puede descargarlo en su ordenador y participar en la cadena. Esta naturaleza hace necesario que los mecanismos de consenso incluyan incentivos económicos para que algunos participantes en la red se decidan a realizar el trabajo de validación, ya sea a través del PoW, PoS u otro protocolo de consenso. Es a través de estos protocolos que el sistema funciona sin controles y de forma descentralizada Las cadenas de bloques públicas se caracterizan por su descentralización, inmutabilidad y seguridad.

Como hemos visto, el funcionamiento de estas redes se basa en la combinación de criptografía e incentivos basados en teoría de juegos, dando lugar a lo que se ha dado en llamar "criptoeconomía"[32] y permitiendo el desarrollo de sistemas descentralizados en los que el mantenimiento del registro se realiza entre los participantes, sin entidad central de control responsable y de forma pseudónima.

2. *Blockchains* privadas.

Las *blockchains* privadas son aquellas en las que la participación se define entre los miembros o los originadores de forma privada. Las partes intervinientes definirán los requisitos para formar parte de la red y la gobernanza de la misma. Entre otros elementos se deberán definir los mecanismos de adaptación del protocolo en caso de necesidad o conveniencia tecnológica, número mínimo de nodos, mecanismos de consenso, previsión en caso de desaparición de la red, responsabilidad de los intervinientes, nivel de identificación de los participantes, etc.

Las *blockchains* privados, a diferencia de las *blockchains* públicas, requieren de una invitación para acceder a ellos. Estas cadenas de bloques dependen de una entidad central que controla todas las acciones dentro de la misma. Las blockchain privadas, por lo general, se construyen para usos corporativos. En una *blockchain* privada, el acceso a la red está restringido y determinado a elementos que solo pueden ser autorizados por la unidad central de control.

3. Blockchains híbridas:

Este tipo de *blockchain* es una fusión entre las *blockchain* públicas y las privadas. Es un intento de aprovechar lo mejor de ambos mundos.

32. Vitalik Buterin define criptoeconomía como "*any descentralised criptographic protocol that uses economic incentives to ensure that it keeps going and doesn't go back in time or incur any glitch*", V. Buterin, Visions, Part I, The value of blockchain technology, 50.

En estas *blockchain*, la participación en la red es privada. Es decir, el acceso a los recursos de la red es controlado por una o varias entidades. Sin embargo, el "*ledger*" es accesible de forma pública. Esto significa que cualquier persona puede explorar bloque a bloque todo lo que sucede en dicha *blockchain*.

VII. CRIPTOMONEDAS

Con carácter general, la utilización de la tecnología *blockchain* aporta valor añadido, teóricamente, a aquellas actividades que cumplan con las siguientes condiciones: (i) requieran almacenar datos; (ii) precisen que el acceso a estos datos sea compartido entre diferentes partes; y, (iii) estas partes no se conozcan entre ellas o no exista confianza mutua por otro motivo. Si bien son muchas las actividades que se desarrollan o pueden desarrollarse bajo los anteriores parámetros; son las criptomonedas las que se han servido de esta tecnología. Éstas surgen como una alternativa a las formas de pago convencionales, con el fin de hacer menos costosas las transacciones y de simplificar la transferencia de dinero de un usuario a otro, en cualquier momento y en cualquier lugar, sin depender de instituciones financieras ni bancos centrales.

La primera vez que el mundo escuchó hablar de criptomonedas fue con el *bitcoin* en el año 2008. El *bitcoin* surgió en respuesta a la crisis financiera y tenía por objeto ser un sistema de pagos electrónicos que permite que dos usuarios realicen de manera directa una transacción sin la intervención de un tercero. Casi una década después el bitcoin cada vez es más popular. A la fecha de la redacción del presente artículo un bitcoin vale US$40,000.00, habiendo llegado US$69,000 en noviembre del 2021.

No cabe duda de que estamos experimentando un auge y crecimiento exponencial en el mercado de criptomonedas, siendo el *bitcoin, ether, bnb, ada, xrp* y *sol* las más populares. A pesar de ello apenas existen términos regulatorios claros en la actualidad, provocando inseguridad jurídica y falta de confianza en la estabilidad del sector. Un primer reto consiste en determinar la naturaleza jurídica de las criptomonedas, dado que esto impacta en las normas de mercado de valores, financieras, tributarias, mercantiles y normas de lavado de activos y financiamiento al terrorismo.

Al respecto, cabe preguntarse qué es una criptomoneda. El diccionario de Oxford define el concepto de criptomoneda como "*una moneda digital en la que se utilizan técnicas de encriptación para regular la generación de unidades de moneda y verificar la transferencia de fondos, operando independientemente de un banco central*[33]". A su vez, el diccionario de la Universidad de Cambridge lo define como *"una moneda digital producida por una red pública, en lugar de cualquier gobierno, que utiliza criptografía para asegurarse de que los pagos se envíen y reciban de forma segura"*[34].

Por su parte, La Directiva —UE— 2015/849, de 20 de mayo de 2015, relativa a la prevención *de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo* define las monedas virtuales como "*representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos*[35]".

33. Definición traducida de: https://dictionary.cambridge.org/es-LA/dictionary/english/cryptocurrency

34. Definición traducida de: https://dictionary.cambridge.org/es/diccionario/ingles/cryptocurrency

35. Artículo 3 apartado 18) de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) no 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (DOUE de 5 de junio).

En el mismo sentido, el Parlamento Europeo, en su Resolución sobre monedas virtuales de 2016, afirma que "*si bien aún no se ha establecido una definición de aplicación universal, a veces se hace referencia a las monedas virtuales como efectivo digital, la Autoridad Bancaria Europea —ABE— entiende las monedas virtuales como una representación digital de valor no emitida por un banco central ni por una autoridad pública, ni necesariamente asociada a una moneda fiduciaria, pero aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos*[36]". Como vemos, la definición es casi idéntica a la aportada en la Directiva —UE— 2015/849, de 20 de mayo de 2015 comentada anteriormente.

De acuerdo con el Grupo de Acción Financiera — GAFI, una moneda virtual es una representación digital de valor que puede ser comercializada digitalmente, y, que, debido al consenso de la comunidad de usuarios, funciona como lo siguiente: (i) un medio de cambio, (ii) una unidad de cuenta, y (iii) un depósito de valor. Sin embargo, ninguna jurisdicción emite o garantiza a las monedas virtuales[37]. A su vez, una criptomoneda es una moneda virtual fundamentada matemáticamente y que está protegida por criptografía —ciencia de escribir mensajes en forma cifrada o en código—. Las criptomonedas se basan en llaves públicas y privadas para transferir el valor de una persona —individuo o entidad— a otra, y debe ser criptográficamente firmado cada vez que se transfiere.

Cabe resaltar que el *White Paper* con las bases conceptuales de *bitcoin*, la más popular y extendida de las criptomonedas, sigue siendo un excelente punto de partida para definir todas las criptomonedas en el área de las ciencias sociales y económicas. Para Satoshi Nakamoto, el *Bitcoin* es un sistema de efectivo electrónico basado en prueba criptográfica que permite a las partes transar directamente entre sí sin necesidad de un tercero, que es reemplazado por una red *p2p* descentralizada que guarda registro cronológico de las transacciones y evita el problema del doble pago.

En nuestra opinión, una criptomoneda es aquella moneda virtual, que se encuentra representada en archivos digitales – *bits* – y es aceptada en una sociedad como unidad de cuenta, medida de valor y medio de pago, utilizando técnicas de criptografía para asegurarse de que los pagos se envíen y reciban de forma segura a través de la tecnología *blockchain*.

Ahora bien, la segunda cuestión es determinar cuál es su naturaleza jurídica. Antes de iniciar con el análisis, quisiera señalar que no comparto la posición de algunos colegas que sostienen que las criptomonedas al ser tecnología no tienen naturaleza jurídica. El hecho que lo que debe ser regulado son las actividades que giran en torno a esta tecnología y no la tecnología *per se*, no significa que ésta como tal no tenga una trascendencia en el Derecho. Es de suma importancia establecer cuál es su naturaleza jurídica, es decir, poder determinar qué es jurídicamente aquello que es objeto de análisis a fin de ver cuáles son las reglas aplicables. En ese sentido, cabe preguntarse si una criptomoneda es dinero o un *commodity* o una divisa o un activo financiero o un valor mobiliario.

La naturaleza jurídica de las criptomonedas no ha sido expresamente determinada por la legislación peruana y tampoco existe alguna propuesta de definición. No obstante, a continuación, se analiza si es posible incluir a las criptomonedas bajo algún concepto jurídico previsto normativamente en el Perú:

a) ¿Pueden las criptomonedas considerarse dinero? Etimológicamente, la palabra dinero proviene del latín "*denarius*" que sig-

36. Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre monedas virtuales disponible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0228+0+DOC+XML+V0//ES

37. Grupo de Acción Financiera (GAFI), "Informe del GAFI. Monedas Virtuales: Definiciones claves y riesgos potenciales de LA/FT", Recuperado de: https://www.uaf.cl/asuntos/descargar.aspx?arid=961

nifica moneda corriente. Inicialmente, el dinero se creó para reemplazar al trueque, dado que es un medio que facilita el intercambio. El dinero constituye un medio de pago que es aceptado por un determinado grupo de personas y existe una mejor asignación del valor de cada bien que se desea intercambiar. Por tanto, es un instrumento que permite reducir los costos de transacción. En la actualidad, el dinero comúnmente se compone de monedas y billetes, los cuales poseen las siguientes características[38]:

i. Portabilidad.- El dinero debe ser fácilmente transportable.
ii. Durabilidad.- El dinero que no sea durable pierde su valor como moneda —los soldados romanos recibían su pago en sal, por ello se habla de salario.
iii. Divisibilidad.- El dinero debe ser fácilmente divisible en partes iguales para permitir la compra de unidades más pequeñas.
iv. Uniformidad.- Para ser útil, el dinero debe ser estandarizado. Sus unidades deben ser de igual calidad y sin que existan diferencias físicas entre sí.
v. Reconocimiento.- El dinero debe ser fácilmente identificable.

Si bien la mayoría de las criptomonedas cumplen con estas características, esto no significa que puedan ser considerado como dinero, desde una perspectiva jurídica. Esto es debido a que el dinero debe tener curso legal, lo que significa que los billetes y monedas que el Banco Central de Reservas pone en circulación son de aceptación forzosa para el pago de toda obligación, pública o privada. En el Perú, el Sol —S/— es desde el 15 de diciembre de 2015, la unidad monetaria de curso legal y el artículo 42 de la Ley Orgánica del Banco Central de Reserva —en adelante, "BCR" — establece que la emisión de billetes y monedas es facultad exclusiva del Estado, quien la ejerce por intermedio del BCR. Las criptomonedas, por su parte, no son de aceptación forzosa.

Asimismo, las criptomonedas, por su parte, se sustentan en un conjunto de protocolos tecnológicos descentralizados que garantizan la seguridad de las operaciones y mantenimiento de la plataforma, siendo la tecnología más relevante para su funcionamiento, el sistema de registro único de operaciones —*blockchain*—; a diferencia de una divisa común y corriente, su generación y administración no dependen de ningún gobierno o banco central, sino del propio software y de los usuarios que componen la cadena, por lo que podemos desde ya concluir que no constituye una moneda de curso legal —dinero *fiat*—, cuya característica principal es la de ser emitido por un banco central[39]. En el Perú, la emisión de billetes y monedas, dentro del territorio peruano, es facultad exclusiva del Estado Peruano, de acuerdo con el artículo 83 de la Constitución Política de 1993. Esta facultad es ejercida por intermedio del Banco Central de Reserva del Perú —en adelante, "BCRP" —. Por consiguiente, las criptomonedas no califican como dinero.

b) ¿Pueden las criptomonedas considerarse dinero electrónico? Las criptomonedas tampoco califican como dinero electrónico, dado que no cumplen con las características previstas en el artículo 2 de la Ley 29985 — Ley que regula las características básicas del dinero electrónico como instrumento de inclusión financiera en el Perú.

De acuerdo con el referido artículo, el dinero electrónico es un valor monetario

38. Barchi, Luciano, "Código Civil Comentado, Tomo VI", Editorial Gaceta Jurídica, 1ra ed. Lima, Mayo 2004, 517.

39. Amprimo, Stefano. Algunas aproximaciones a la naturaleza jurídica del Bitcoin en el Perú. Recuperado de: https://ius360.com/algunas-aproximaciones-a-la-naturaleza-juridica-del-bitcoin-en-el-peru-stefano-amprimo/

representado por un crédito exigible a su emisor, el cual tiene las siguientes características:

i. Es almacenado en un soporte electrónico.
ii. Es aceptado como medio de pago por entidades o personas distintas al emisor y tiene efecto cancelatorio.
iii. Es emitido por un valor igual a los fondos recibidos.
iv. Es convertible a dinero en efectivo según el valor monetario del que disponga el titular, al valor nominal.
v. No constituye depósito y no genera intereses.

Como bien sabemos, las criptomonedas no tienen un valor nominal *per se*, y dependen netamente de su valor de cotización de mercado, el cual es sumamente volátil. Además, las criptomonedas no representan créditos exigibles a ningún emisor, puesto que no son emitidos por una entidad sino en virtud del proceso de minado.

Asimismo, según el artículo 3 de esta ley, sólo pueden emitir dinero electrónico las empresas que operan bajo el ámbito de supervisión de la Superintendencia de Banco, Seguros y AFP —en adelante, "SBS"—. En cambio, las criptomonedas pueden ser creadas por cualquiera que tenga un software especializado en este proceso descentralizado llamado "minería".

Coincidiendo con esta opinión, el GAFI señala que, en efecto, "*la moneda virtual es diferente del dinero electrónico puesto que éste es una representación digital del dinero fiduciario —de curso legal— usado electrónicamente para transferir el valor denominado en dinero fiduciario*". Agrega que "*el dinero electrónico funciona como el dinero fiduciario, es decir, se transfiere electrónicamente un valor que tiene la condición de moneda de curso legal*[40] ".

c) ¿Pueden las criptomonedas considerarse como *commodities*? Existe una corriente que califica a las criptomonedas como *commodities* que pertenecen al mundo digital – de los átomos a los bits -, dadas las similitudes con metales como el oro y la plata debida a la alta volatilidad de su cotización. Mientras que en Estados Unidos la *Commodity Futures Trading Commission —CFTC—* ha determinado que el *bitcoin* encajaría bajo la definición de *commodity*[41], la regulación peruana no goza de la generalidad del concepto americano, ni ha dado señales de inclinarse por esa línea interpretativa; por el contrario, contiene una definición bastante restrictiva del concepto de *commodity*.

En efecto, la Ley 26702 – Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros contempla a los *commodities* estrictamente como "*mercancías primarias o*

40. Grupo de Acción Financiera (GAFI). Op. Cit.

41. En el año 2018, la CFTC determinó que el Bitcoin y otros activos digitales califican como *commodities* bajo la definición del *Commodities Exchange Act* (7 U.S. Code § 1a): "*The term "commodity" means wheat, cotton, rice, corn, oats, barley, rye, flaxseed, grain sorghums, mill feeds, butter, eggs, Solanum tuberosum (Irish potatoes), wool, wool tops, fats and oils (including lard , tallow, cottonseed oil, peanut oil, soybean oil, and all other fats and oils), cottonseed meal, cottonseed, peanuts, soybeans, soybean meal, livestock, livestock products, and frozen concentrated orange juice, and all other goods and articles, except onions (as provided by section 13–1 of this title) and motion picture box office receipts (or any index, measure, value, or data related to such receipts), and all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in*." (Énfasis nuestro). Asimismo, en setiembre de 2020, un grupo de congresistas de la Cámara de Diputados de E.E.U.U., liderado por el congresista K. Michael Conaway, han introducido un proyecto de ley denominado "*Digital Commodity Exchange Act of 2020*" destinado a llenar los vacíos regulatorios que existen entre las potestades de la CFTC y la *Securities Exchange Commission (SEC)* de cara a la regulación y supervisión del uso de activos digitales y monedas virtuales.

básicas consistentes en productos físicos, que pueden ser intercambiados en un mercado secundario, incluyendo metales preciosos pero excluyendo oro, que es tratado como una divisa" —énfasis nuestro—, excluyendo así cualquier línea interpretativa que comprenda a los activos digitales o virtuales en la categoría de los *commodities*[42].

En tal sentido, teniendo en cuenta que las monedas virtuales solo se encuentran representadas digitalmente, y no de manera física, no califican como *commodities*.

d) ¿Pueden las criptomonedas considerarse como un instrumento de pago? De acuerdo con la Ley de los Sistemas de Pagos y de Liquidación de Valores, aprobada por la Ley 29440, los instrumentos de pago tienen por objeto efectuar un pago —como las transferencias de créditos— o requerirlo —como los cheques, débitos directos, letras de cambio, cuotas de crédito—.

Ahora bien, los instrumentos de pago indicados en la Ley 29440 son aquellos utilizados en el marco de un sistema de pagos o de liquidación de valores, los cuales se encuentran reconocidos de manera expresa por la referida ley o son declarados como tales por el BCRP o la Superintendencia del Mercado de Valores — SMV, respectivamente.

Teniendo en consideración que las criptomonedas a la fecha no han sido reconocidas por la legislación peruana o declarado por el BCRP, órgano rector de los sistemas de pagos, como un sistema de pagos, las criptomonedas tampoco constituyen instrumentos de pago bajo la Ley 29440.

Por otra parte, a través la Ley 28194 — Ley para la Lucha contra la Evasión y para la Formalización de la Economía, se establecen los supuestos en los cuales obligatoriamente se utilizarán los medios de pago con la finalidad de evitar la evasión y promover la formalización de la economía en el Perú, con lo cual, se entiende por medios de pagos los utilizados a través de empresas del Sistema Financiero, tales como: depósitos en cuenta, giros, transferencias de fondos, órdenes de pago, tarjetas de débito y crédito expedidas en el país, cheques, remesas y cartas de crédito.

Sin perjuicio de lo anteriormente mencionado, las criptomonedas pueden ser utilizadas como medios de pago o mecanismos de pago de forma consuetudinaria en efecto, en los establecimientos que las aceptan, estas criptomonedas gozan de efecto cancelatorio respecto de los bienes y servicios prestados. Dicho efecto cancelatorio es concedido de manera voluntaria por las partes involucradas en cada transacción, lo cual se asemejaría a una permuta o dación en pago.

e) ¿Pueden las criptomonedas considerarse como una divisa? De acuerdo con el glosario del BCRP, el término divisa se refiere a "*dinero de aceptación internacional, básicamente oro monetario y ciertas monedas extranjeras. En el caso peruano, la más aceptada es el dólar de los Estados Unidos de Norteamérica*[43]". Las divisas tienen además varias funciones: ser medio de pago, servir como instrumento de ahorro para ser recuperado en el futuro y servir como unidad de medida del valor de los precios de los bienes y servicios.

Al respecto, la NIC 21 define a la divisa como aquel concepto usado para referirse a toda moneda extranjera distinta de la moneda funcional. En ese sentido, para determinar a una moneda como divisa, en primer lugar, se le debe dar un reconoci-

42. Amprimo, Stefano. Op.Cit.

43. Recuperado de: https://www.bcrp.gob.pe/docs/Publicaciones/Glosario/Glosario-BCRP.pdf

miento como moneda funcional[44] de curso legal en su país de origen.

En lo que concierne a las criptomonedas, a excepción de *bitcoin*, ningún país las ha respaldado alguna abiertamente como una moneda funcional en curso legal, a pesar de ser reconocidas como un medio de pago alternativo. Sin embargo, ¿qué ocurre con *bitcoin*? ¿puede considerarse divisa al haber sido aceptada como moneda de curso legal en El Salvador y la República Centroafricana?

Al respecto, la Constitución Política del Perú establece que el Estado garantiza la libre tenencia y disposición de moneda extranjera. Asimismo, el Decreto Legislativo 668, en su artículo quinto complementa lo dicho por la Constitución señalando que el Estado garantiza la libre tenencia, uso y disposición interna moneda extranjera, por las personas naturales y jurídicas residentes en el país; así como la libre convertibilidad de la moneda nacional a un tipo de cambio único. El tipo de cambio para las operaciones de moneda extranjera será fijado por la oferta y la demanda conforme a lo señalado en el artículo 2 del Decreto Supremo Nº 068-91-EF y artículo 1 de la Resolución Cambiaria N° 007-91-EF-90.

Por su parte, la Ley Bitcoin de El Salvador tiene como objeto la regulación del *bitcoin* como moneda de curso legal, irrestricto con poder liberatorio, ilimitado en cualquier transacción y a cualquier título que las personas naturales o jurídicas, públicas o privadas requieran realizar. Asimismo, todo precio podrá ser expresado en bitcoin y todas las contribuciones tributarias podrán ser pagadas en bitcoin. Dicha norma establece que los intercambios en *bitcoin* no estarán sujetos a impuestos sobre las ganancias de capital al igual que cualquier moneda de curso legal. Finalmente, es una moneda de aceptación forzosa, ya que dispone que todo agente económico deberá aceptar *bitcoin*, como forma de pago cuando así le sea ofrecido por quien adquiere un bien o servicio.

¿El hecho que el *bitcoin* sea reconocido como una moneda de curso legal en un país lo convierte en moneda extranjera? Creemos que no. El *bitcoin* es una moneda nativa del internet y que un país la acoja no significa que sea su "moneda" ya que no es emitida ni controlada por un Banco Central. En el caso peruano, el BCRP ha señalado en el Oficio N° 0022-2022-BCRP que las criptomonedas no constituyen moneda de curso legal y no cumplen plenamente las funciones del dinero como medio de cambio, unidad de cuenta y reserva de valor. Asimismo, señala que pertenecen al ámbito privado de sus usuarios y no tienen un respaldo institucional del poder público. Por consiguiente, las criptomonedas no son consideradas divisas en nuestro ordenamiento jurídico.

Finalmente, para el caso de las monedas digitales de bancos centrales —CBDC – *Central Bank Digital Currency* – por sus siglas en inglés—, estas sí serían consideradas divisas porque a diferencia del resto de criptomonedas, las CBDC no son emitidas por entidades privadas o por organizaciones descentralizadas, sino por los propios bancos centrales.

44. NIC 23: "*El entorno económico principal en el que opera la entidad es, normalmente, aquél en el que ésta genera y emplea el efectivo. Para determinar su moneda funcional, la entidad considerará los siguientes factores:*
(a) La moneda: (i) que influya fundamentalmente en los precios de venta de los bienes y servicios (con frecuencia será la moneda en la cual se denominen y liquiden los precios de venta de sus bienes y servicios); y (ii) del país cuyas fuerzas competitivas y regulaciones determinen fundamentalmente los precios de venta de sus bienes y servicios.
(b) La moneda que influya fundamentalmente en los costos de la mano de obra, de los materiales y de otros costos de producir los bienes o suministrar los servicios (con frecuencia será la moneda en la cual se denominen y liquiden tales costos)".

f) ¿Pueden las criptomonedas considerarse como títulos valores o valores mobiliarios? Tomando en consideración que los títulos valores deben estar expresamente reconocidos por la ley, y ello no ocurre con las criptomonedas, podemos llegar a la conclusión que no son títulos valores, de acuerdo con nuestra legislación actual. Por esta misma razón, las criptomonedas tampoco califican como valores mobiliarios.

g) ¿Pueden las criptomonedas considerarse como un instrumento o activo financiero? De acuerdo con la NIC 32, un instrumento financiero es cualquier contrato que dé lugar a un activo financiero en una entidad y a un pasivo financiero o a un instrumento de patrimonio en otra entidad.

   Por su parte, un activo financiero es cualquier activo que sea: (a) efectivo; (b) un instrumento de patrimonio de otra entidad; (c) un derecho contractual: (i) a recibir efectivo u otro activo financiero de otra entidad; o (ii) a intercambiar activos financieros o pasivos financieros con otra entidad, en condiciones que sean potencialmente favorables para la entidad; o (d) un contrato que será o podrá ser liquidado utilizando instrumentos de patrimonio propio de la entidad, y sea: (i) un instrumento no derivado, según el cual la entidad está o puede estar obligada a recibir una cantidad variable de sus instrumentos de patrimonio propios; o (ii) un instrumento derivado que será o podrá ser liquidado mediante una forma distinta al intercambio de un importe fijo de efectivo, o de otro activo financiero, por una cantidad fija de los instrumentos de patrimonio propio de la entidad.

   Al respecto, en Estados Unidos existe lo que se denomina "*Prueba de Howey*", que es una prueba creada por la Corte Suprema para determinar si ciertas transacciones califican como «contratos de inversión». Si es así, entonces bajo la Ley de Valores de 1933 y la Ley de Bolsa de Valores de 1934, esas transacciones se consideran instrumentos financieros y, por lo tanto, están sujetas a ciertos requisitos de divulgación y registro. Cabe señalar que, en junio del año 2019, Jay Clayton, entonces Presidente de la SEC, aclaró que el Bitcoin, como tal, no constituye un contrato de inversión bajo la Prueba de Howey y, en consecuencia, no califica como un instrumento financiero a criterio de la SEC, indicando que "*las criptomonedas [como el Bitcoin] son reemplazos de las monedas soberanas … [ellas] reemplazan el yen, el dólar, el euro con bitcoin. Ese tipo de [cripto]moneda no es un valor*"[45].

   De otro lado, en nuestro ordenamiento jurídico, el artículo 2 de la Ley de Promoción del Mercado de Valores, Ley 30050, dispone que toda publicidad o aviso sobre activos financieros que se encuentre bajo competencia de la SMV o de la SBS, respectivamente, que se efectúe con el fin de obtener dinero del público a cambio de un retorno financiero, un derecho crediticio, patrimonial o de participación en el capital, o en las utilidades del receptor de los fondos, bajo cualquier modalidad, y que se realice en territorio nacional, empleando medios masivos de comunicación, como diarios, revistas, radio, televisión, correo, reuniones, redes sociales, servidores de internet ubicados en territorio nacional o en territorio extranjero u otros medios o plataformas, solo puede realizarse por sujetos autorizados o supervisados por la SMV o por la SBS. Para dicho fin, la norma autoriza a la SMV y la SBS a aplicar el principio de "primacía de la realidad", de manera que, con prescindencia de la denominación del activo financiero, pueden ejecutar las acciones que resulten aplicables frente al incumplimiento de lo dispuesto en el citado artículo 2.

45. Recuperado de: https://www.investopedia.com/news/sec-chair-says-bitcoin-not-security/

Al respecto, debemos señalar que una criptomoneda es un concepto distinto a un criptoactivo, que puede ser entendido como aquel activo que puede ser generado a través de la criptografía, como, por ejemplo, un token. La relación es de género a especie, siendo la criptomoneda un tipo de criptoactivo. Bajo esa lógica, somos de la opinión que algunos criptoactivos, como un *security token*, sí podría encajar en el principio de primacía de la realidad, mientras que, teóricamente, las criptomonedas no podrían ser consideradas instrumentos financieros, en tanto su adquisición no genera una obligación a cargo de alguien[46].

h) ¿Pueden las criptomonedas considerarse como bienes muebles? El artículo 886 inciso décimo del Código Civil establece que son considerados bienes muebles todos aquellos bienes no comprendidos en el artículo que corresponde al listado de bienes inmuebles —artículo 885—. En otros términos, todos los bienes que no son inmuebles son muebles.

Al respecto, podemos definir al bien como la cosa que está dentro del patrimonio de una persona y que es susceptible de valoración económica. Bajo esa misma línea, un bien mueble es aquél que puede trasladarse de un lugar a otro y pueden ser materiales o inmateriales. En tal sentido, podemos señalar con certeza que las criptomonedas son bienes muebles dado que son susceptibles de ser parte del patrimonio de una persona, son susceptibles de valoración económica y pueden ser trasladados por el ciberespacio de un lugar a otro.

Asimismo, las criptomonedas son bienes intangibles ya que no cuentan con una presencia física ni pueden ser percibidas por los sentidos; sin embargo, sí son susceptibles de valoración económica. Este bien intangible puede formar parte del activo de una empresa o puede ser empleado como un bien de cambio, dependiendo de la actividad a la que se dedica la empresa y la finalidad con la que se adquieren las criptomonedas. Cabe señalar que las criptomonedas sólo existen en el mundo digital.

Adicionalmente, es fungible[47] puesto que una criptomoneda puede ser recíprocamente sustituido por otro —a diferencia de los *NFTs*— y no consumible porque se puede usar sin que éste sea agotado.

En conclusión, en nuestro ordenamiento jurídico, las criptomonedas son bienes muebles, intangibles, fungibles y no consumibles.

De otro lado, cabe preguntarse cuál es la regulación de las criptomonedas en el Perú y la respuesta es que no existe normativa específica que regule este fenómeno. Por lo tanto, se enmarcan en la regla general de "*sujeción negativa al ordenamiento jurídico*" que aplica a los privados: se puede hacer todo aquello que la ley no prohíba. Sin embargo, como bien señala Castro[48], dicha regla general tiene como excepción

46. Cabe señalar que el BCRP, en el marco del trámite en el Congreso de la República del proyecto de "Ley Marco de Comercialización de Criptoactivos", ha emitido un Oficio[4] en el que menciona que las criptomonedas no constituyen activos financieros a través de los cuales se transmite la política monetaria y se da cumplimiento a las funciones del BCRP. Además, el BCRP menciona que las criptomonedas y los criptoactivos pertenecen al ámbito privado de los usuarios y no tienen respaldo institucional del poder público.

47. Hay quienes sostienen que el Bitcoin no es 100% fungible porque éstos pueden ser rastreados en la red y se encuentran determinados en la cadena de bloque. Sin embargo, para efectos del pago, los bitcoins tendrán el mismo valor en el mercado.

48. Álvaro, Castro, y Lucía Suárez. "Oferta de servicios de criptoactivos por parte de entidades del sistema financiero: análisis comparativo entre Perú y la Unión Europea." Ita Ius Esto 16, (2022): 19. https://www.itaiusesto.com/index.php/inicio/article/view/24

el caso de privados cuya actividad está sujeta a una licencia y regulación especiales. Por ejemplo, empresas del sistema financiero —bancos, financieras, emisores de dinero electrónico— o de seguros autorizados a operar como tales por la SBS y cuyas actividades permitidas son definidas en la licencia correspondiente, en el marco de la Ley General de Bancos y sus normas reglamentarias.

Los autores[49] agregan que, el Perú, en la línea de muchos otros países del mundo, creó en 2021 un programa de "pruebas piloto" para servicios financieros —*sandbox* regulatorio—, que permite a las empresas testear modelos de negocio innovadores bajo la mirada del regulador y un esquema regulatorio ligero. Así, mediante Decreto de Urgencia 013-2020 —Decreto de Urgencia que promueve el financiamiento de la Mipyme, Emprendimientos y Startups, el Gobierno peruano facultó a la SMV y a la SBS a reglamentar e implementar *sandbox* regulatorios en el ámbito de sus funciones de supervisión.

En el caso específico de la SBS, la Quinta Disposición Complementaria Modificatoria del Decreto de Urgencia 013-2020 incorpora a la Ley General de Bancos una disposición que le permite al regulador autorizar la realización temporal de cualquier operación o actividad a través de modelos novedosos, pudiendo otorgar excepciones a la regulación que les resulte aplicable a las personas naturales o jurídicas que realicen tales operaciones o actividades, así como respecto a las demás disposiciones necesarias para su desarrollo.

En agosto de 2021, mediante Resolución SBS N° 2429-2021 —el "Reglamento"—, la SBS reglamentó su *sandbox* regulatorio, estableciendo dos —2— regímenes:

a) Régimen de flexibilización, en que las pruebas se enfocan en actividades asociadas a modelos contemplados en el marco normativo actual, pero que requiere cierta flexibilización temporal; y,

b) Régimen extraordinario, en que las pruebas de actividades están asociadas a modelos no regulados, pero bajo la competencia de la SBS. Cabe precisar que, a diferencia de otras jurisdicciones —e.g., México—, solo pueden formar parte del *sandbox* de la SBS empresas con licencia de organización o funcionamiento otorgada por aquella —e.g., bancos, financieros, empresas fiduciarias, empresas emisoras de dinero electrónico, etc.—.

En tal sentido, una empresa que quisiera aprovechar el *sandbox* de la SBS para testear la provisión de un servicio asociado a criptomonedas —custodia, intercambio, etc. —, tendría que acogerse al régimen extraordinario. Reforzando ese entendimiento, el artículo 8 del Reglamento establece que, en el caso del régimen extraordinario, la empresa que solicita autorización para el programa piloto debe justificar que el modelo novedoso no cuenta con un marco normativo aplicable y que, por su naturaleza, se encuentra relacionado a actividades bajo competencia de la SBS.

Ahora bien, conforme al numeral 44 del artículo 221 de la Ley General de Bancos, en tanto se tratarían de servicios no previstos expresamente en dicha norma, se requeriría previamente la opinión favorable del BCRP para que la SBS pueda regular y autorizar su prestación por parte de empresas del sistema financiero. En el caso de las criptomonedas, el involucramiento del BCRP parecería sensato dada la preocupación que muchos bancos centrales del mundo han expresado respecto del potencial impacto de dichos activos digitales en la estabilidad monetaria y de los sistemas financieros. Sin embargo, si el BCRP no emite una opinión favorable estaríamos frente a un resultado paradójico en materia regulatoria: empresas supervisadas —que cumplen obligaciones en materia de solvencia

49. Álvaro, Castro, y Lucía Suárez, *Oferta de servicios de criptoactivos por parte de entidades del sistema financiero: análisis comparativo entre Perú y la Unión Europea*, 21-22.

patrimonial, gestión de riesgos, ciberseguridad, *conduct of business*, etc.—, que no pueden brindar servicios relacionados a criptomonedas y; por otra parte, empresas no supervisadas que -a falta de una normativa expresa que lo restrinja o prohíba- están facultadas a brindar tales servicios. Es por ello que urge una regulación ligera y flexible que permita a las empresas del sistema financiero prestar servicios vinculados a las criptomonedas.

Finalmente, es importante mencionar que, a la fecha, existe el Proyecto de Ley N° 1042/2021-CR — Ley Marco de Comercialización de Criptoactivos. Esta iniciativa responde a la urgencia de establecer un marco normativo y regulatorio que defina los lineamientos para la operación y funcionamiento de las empresas de servicio de intercambio de criptoactivos a través de plataformas tecnológicas, basándose en los principios de libre mercado y de libre competencia. Este proyecto señala que las entidades bancarias y no bancarias que presten el servicio de venta e intercambio de criptoactivos deberán registrarse en el Registro Único de Plataformas de Intercambio de Criptomonedas — RUPIC. Asimismo, estas empresas deberán cumplir con una serie de obligaciones tales como: (i) Constituirse como persona jurídica domiciliada en el Perú o como una sucursal de una sociedad extranjera; (ii) Estar debidamente inscrito en la Superintendencia de Banca y Seguros; (iii) Incorporar en la minuta de constitución como objeto social exclusivo la realización de actividades calificadas como "Servicios de Intercambio de Criptoactivos"; (iv) Contar con sistemas de ciberseguridad que aseguren la confidencialidad, disponibilidad e integridad de la información; (v) Adoptar medidas preventivas contra el lavado de activos y la financiación al terrorismo; (vi) Reportar operaciones sospechosas a la Unidad de Inteligencia Financiera; (vii) Dar cumplimiento a la normativa de protección de datos personales; (viii) Informar al usuario, en idioma español, de todos los riesgos asociados con sus servicios y con los criptoactivos.

VIII. SMART CONTRACTS

El éxito de Bitcoin demostró al mundo que era posible crear y transferir una moneda virtual utilizando la tecnología *blockchain* sin tener que depender de un banco u otra institución financiera. No obstante, no pasó mucho tiempo para que los expertos en la materia se comenzarán a cuestionar si es que esta tecnología podía ser utilizada para el desarrollo de otras aplicaciones.

Es en este contexto en donde aparece Vitalik Buterin, quien es el cofundador de la *blockchain Ethereum*. Su historia es bastante peculiar porque fue un cambio en los parámetros del juego *World of Warcraft* lo que lo inspiró a que se inmiscuya en la tecnología *blockchain* para luego crear *Ethereum*. El mismo Vitalik cuenta que debido a una actualización hecha por la compañía Blizzard —dueños del juego—, eliminaron el hechizo *Siphon Life* que afectaba a uno de sus personajes. Esta experiencia le sirvió para ver el lado más negativo de los sistemas de desarrollo de software centralizados, ya que no podía comprender cómo es que una empresa podía unilateralmente arrebatarle algo que le había costado tanto esfuerzo de conseguir.

A medida que conocía más sobre esta nueva tecnología, Vitalik Buterin comenzaba a darse cuenta de que una *blockchain* podía ser más que un libro contable descentralizado y que podía aportar más valor que solamente ser un sistema de transmisión de monedas virtuales sin intermediarios. En el *White Paper* de *Ethereum* se habla de nuevas funcionalidades y se proponía que la red *blockchain* no fuera solo una entidad para almacenar y validar transacciones, sino que también, de forma automática y consensuada, pudiera actuar de intermediario con ejecución de contratos. De ahí nació el concepto de "*smart contract*" en una *blockchain*, una forma de añadir cierta inteligencia y aprovechar el procesamiento en la ejecución de actividades sobre todas las transferencias o eventos que pudieran procesar dentro de la red. El *White Paper* de *Ethereum* comienza de la siguiente forma:

> *"La publicación de Bitcoin en 2009 por parte de Satoshi Nakamoto a menudo se ha aclamado como un avance radical en el ámbito del dinero y las divisas, siendo el primer ejem-*

plo de un activo digital que a la vez no tiene respaldo o valor intrínseco ni un emisor o mando centralizado. Sin embargo, otra parte, quizás más importante, del experimento de Bitcoin es la tecnología subyacente de blockchain como una herramienta de consenso distribuido, aspecto del Bitcoin sobre el cual se está empezando rápidamente a centrar la atención. Las aplicaciones alternativas que se citan comúnmente de la tecnología de blockchain incluyen el uso de los activos digitales blockchain para representar divisas a medida e instrumentos financieros —monedas coloreadas—, la propiedad de un artefacto físico subyacente —propiedad inteligente—, activos no fungibles como nombres de dominio —Namecoin—, así como aplicaciones más complejas que involucran activos digitales controlados directamente por un fragmento de código que implementa reglas arbitrarias —contratos inteligentes— o incluso organizaciones autónomas descentralizadas basadas en blockchain —DAO—. Lo que Ethereum pretende es proporcionar una blockchain con un lenguaje integrado Turing completo y plenamente desarrollado que se puede usar para crear "contratos" que, a su vez, se pueden utilizar para codificar funciones arbitrarias de transición de estados, permitiendo a los usuarios crear cualquiera de los sistemas descritos anteriormente, así como otros que todavía no hemos imaginado, tan solo escribiendo la lógica en unas pocas líneas de código".

En tal sentido, una de las grandes diferencias entre la *blockchain* de *Bitcoin* y la de Ethereum radica en lo que se conoce como la "*Ethereum Virtual Machine*" o EVM. La EVM es una de las piezas claves en el funcionamiento de la *blockchain* de *Ethereum*. Su función es la de permitir la ejecución de programas o *smart contracts* con la finalidad de desplegar sobre dicha *blockchain* una serie de funcionalidades añadidas para que los usuarios puedan disfrutar de las mismas. La EVM permite el diseño y la ejecución de *smart contract* y se utiliza un lenguaje de programación denominado *solidity*.

Ahora bien, la idea de los contratos inteligentes es más antigua de lo que podría pensarse. En la década de los 90, el jurista, informático y criptógrafo Nick Szabo trató ampliamente la tesis de los contratos inteligentes definiéndolos como un protocolo de transacción computarizado que ejecuta los términos de un contrato, que sirviera para dar lugar a unas relaciones contractuales donde el incumplimiento contractual fuera costoso para quien lo incumpliera. Se observa cómo la idea básica que reside detrás de esta tesis es la de aportar seguridad al cumplimiento de un contrato, evitando así conflictos y, consecuentemente, la necesidad de acudir a los tribunales; ello permite concluir que los *smart contracts* cumplen una especie de autoayuda —*self-help*—.

Cabe preguntarse por qué en los años 90s esta idea no tuvo tanta repercusión. La razón de ello es que, desde su concepción, existieron una serie de problemas que impedían llevar a la práctica su implementación, tales como la imposibilidad del código informático de poder controlar los activos a efectos de hacer cumplir los acuerdos, así como la dificultad de encontrar un código informático sobre el que recaiga la confianza de las partes contratantes, en tanto ejecute lo acordado por ellas y que no pueda ser manipulado. Si bien no es necesaria la tecnología *blockchain* para codificar y automatizar un contrato, lo cierto es que esta tecnología resuelve el primer problema en mención ya que permite controlar el activo a través de un código o clave escrita en lenguaje criptográfico asociado a ese activo. Asimismo, lo que permite esta tecnología es masificar y globalizar el uso de los *smart contracts* debido a sus características de inmutabilidad, trazabilidad, descentralización y seguridad.

En este orden de ideas, un *smart contract* o contrato inteligente es un programa informático que se almacena en la *blockchain*, cuyas líneas de código reemplazan los términos y condiciones que se encuentran en un contrato tradicional que sigue un "*script*" —secuencia de comando— a fin de ejecutarse de forma automática sin que medie un tercero entre las partes. Es decir, mediante el uso del código informático se verifica y ejecuta un acuerdo entre partes

sin intervención de estas. Esta tecnología permite la ejecución automática e independiente de aquellos términos de un contrato que sean objetivables mediante la siguiente fórmula matemática: "*If* + *Then*", esto es, "*Si ocurre esto…entonces sucederá lo siguiente…*". Esto permite que las cláusulas contractuales sean vinculantes y automáticas, dado que pueden autoejecutarse a través de la información que reciben. Además, permiten garantizar la ejecución de un contrato de forma neutral y ser más eficientes en la distribución de bienes y servicios. Por lo que para que el contrato pueda ser verificado y ejecutado de manera automática, necesitamos que dichas cláusulas o condiciones sean objetivas u objetivables, ya que los *smart contracts* utilizan la lógica booleana.

En efecto, como bien señala Abel Revoredo, los *smart contracts* son acuerdos, escritos en código de programación, que ejecutan automáticamente funciones programadas cuando se cumplen ciertas condiciones preestablecidas. En otras palabras, cuando la condición "A" se cumple, genera que la acción "B" se realice. Esta es la idea simplificada detrás de los *smart contracts*[50]. El funcionamiento de los contratos inteligentes parte de un acuerdo entre las partes contractuales, las cuales deciden valerse de las características de un *smart contract* para ejecutar los términos del acuerdo una vez se verifiquen las condiciones preestablecidas en dicho acuerdo. Especial relevancia tiene el hecho de que el acuerdo, de forma total o parcial, se codifica y se almacena en una cadena de bloques, dotándole de inmutabilidad y seguridad.

En el Ted Talk denominado "*How Smart Contracts Will Change the World*", Olga Mack señala que un *smart contract* es una suerte de "máquina expendedora —*vending machine*— con esterioides". De hecho, Nick Szabo también hace el símil. Este *speaker* sostiene que los *smart contracts* cumplen tres funciones esenciales: (i) Guardan reglas; (ii) Verifican el cumplimiento de las reglas; (iii) Autoejecutan el comando una vez verificado el cumplimiento de la regla. Esto también ocurre con una máquina expendedora de *snacks*. En primer lugar, la máquina tiene guardada la regla de que una vez insertadas las monedas equivalentes al precio del producto, el consumidor obtendrá el producto elegido. En segundo lugar, una vez insertada la moneda, verifica el valor de la misma y el producto de elección. Finalmente, luego de culminar el proceso de verificación, la máquina ejecuta la orden y el consumidor obtiene el snack que eligió. ¿Por qué se dice que es una *vending machine* con esteroides? Porque la complejidad en la automatización del contrato depende de la complejidad del contrato. Por ejemplo, en un contrato inteligente de compraventa de una acción, cuando el comprador le hace el pago del dinero al vendedor, el *smart contract* comunica inmediatamente a la sociedad, quien a su vez registra al nuevo titular de la acción y expide un certificado digital de acciones.

A lo largo del presente artículo, hemos podido apreciar cómo los *smart contracts* se sirven de la tecnología *blockchain* para ejecutar automáticamente un contrato al darse la verificación de las condiciones preestablecidas en el mismo; lo cual permite que sea un proceso especialmente rápido y eficiente. Por otro lado, el uso de los contratos inteligentes no necesita de terceras partes ni intermediarios, lo cual, además de permitir mayor rapidez, repercute positivamente en la reducción de costes y en que la confianza se traslada al código, difícilmente manipulable una vez almacenado en la cadena de bloques. Sin embargo, ¿cómo podemos beneficiarnos de los *smart contracts*?

Literalmente, existen cientos de ejemplos:

a) En el sector de seguros, una persona podrá someterse a una operación y ni bien salga de ella podrá ver en su cuenta el reembolso del pago sin tener que estar peleándose con la aseguradora.
b) En el sector de transportes, si un avión

50. Revoredo, Abel. Blockchain y Smart Contracts: ¿Hay futuro para los abogados? Recuperado de: https://gestion.pe/blog/cyberlaw/2018/03/blockchain-y-smart-contracts-hay-futuro-para-los-abogados.html/?ref=gesr

o tren se demora, automáticamente se transferirá el precio del ticket más una indemnización por los daños y perjuicios ocasionados.

c) En el sector de apuestas, quien gane la apuesta no tendrá que estar persiguiendo al perdedor para que le pague.

d) En el sector financiero, los bancos podrán ejecutar hipotecas o garantías cuando el deudor deje de pagar.

En tal sentido, los contratos inteligentes aportan transparencia, previsibilidad, control y facilidad de cumplimiento a las relaciones contractuales a la vez que mitigan los riesgos asociados con la participación humana, ya que buscan reducir los costos transaccionales, eliminar a los intermediarios y simplificar la ejecución de los contratos. Esto sin duda repercute en el ordenamiento jurídico, dado que la actividad comercial que se ejecuta vía un *smart contract* no puede separarse del Derecho Contractual. Entonces, ¿cuál es la naturaleza jurídica de los *smart contracts*? Al hilo de lo indicado anteriormente, los *smart contracts* pueden ser vistos desde dos perspectivas distintas: por un lado, desde una perspectiva informática que los concibe como un código informático, y, por otro lado, desde una perspectiva jurídica que concibe al código informático como una herramienta al servicio de un acuerdo que se redacta total o parcialmente en código para servirse de la autoejecución con la verificación de condiciones estipuladas en un acuerdo que posee relevancia jurídica[51].

Con base a lo anterior, ¿un *smart contract* puede ser considerado como un contrato para el Derecho Civil peruano? Desde el punto de vista formal, el hecho de que los contratos legales inteligentes se redacten, en todo o en parte, en forma de código informático no supone ningún obstáculo para reconocerles la consideración de un contrato dado que el Código Civil peruano consagra en su artículo 143 el principio de libertad de forma, esto es, que las personas pueden manifestar su voluntad de la forma que estimen conveniente, salvo que se exija una formalidad determinada para ciertos actos jurídicos. Es decir, ante el silencio de la ley, las partes son libres de escoger cualquiera modalidad de exteriorización del querer. Por tanto, observamos que la libertad de forma que prevé la legislación peruana significa que las partes pueden elegir plasmar un contrato en la forma de *smart contract*, sin perjuicio de requisitos formales que puedan establecerse.

Recordemos que nuestro Código Civil permite explícitamente la utilización de medios electrónicos para manifestar la voluntad al momento de celebrar un acto jurídico debido a una reforma llevada a cabo en junio del año 2000, a través de la promulgación de la Ley 27291, la cual modificaba los artículos 141 y 1374 del Código Civil, así como, agregaba el nuevo artículo 141-A a dicho cuerpo normativo. En ese sentido, los *smart contracts* se caracterizan por su naturaleza electrónica y no son más que una variante de los contratos electrónicos, entendidos como aquel acuerdo de dos o más personas que se obligan entre sí o respecto de otra u otras, para crear, modificar o extinguir una relación jurídica de carácter patrimonial —como puede ser dar alguna cosa o prestar algún servicio—, con la particularidad de que el consentimiento de las partes que se presta por medios electrónicos, es permitido en nuestro ordenamiento jurídico.

Los contratos electrónicos, al igual que cualquier otro tipo de contrato, deberán reunir los requisitos esenciales para la validez de todo contrato; esto es, que los agentes capaces hayan manifestado su consentimiento, el objeto contractual sea física y jurídicamente posible, que cuente con un fin lícito y que siga la formalidad exigida por ley. Los contratos electrónicos se perfeccionan cuando el remitente obtiene un acuse de recibo de conformidad con el artículo 1374 del Código Civil.

51. Fetsyak, Ihor. "Contratos Inteligentes: Análisis jurídico desde el marco legal español." Revista Electrónica de Derecho de la Universidad de La Rioja, REDUR 18, (2019): 197-236. https://dialnet.unirioja.es/servlet/articulo?codigo=7814692

Como bien señala, Agustina Pérez, es importante entender que en el caso de los *smart contracts* no nos encontramos ante un nuevo tipo de contracto, sino ante una nueva herramienta para contratar con medios electrónicos que permite aplicar de manera profunda el famoso principio de "*pacta sunt servanda*" —la eficacia o cumplimiento no puede dejarse al arbitrio de una de las partes—, de forma que la naturaleza de los contratos "tradicionales" es aplicable, sin necesidad de tener una norma expresa, siempre que el mismo sea "programado" con el consentimiento de ambas partes[52].

Al haber concluido que los contratos legales inteligentes pueden llegar a tener la consideración de contratos, resulta inevitable señalar que a la fecha existen más dudas que certezas en la aplicación de esta tecnología al mundo contractual.

1. ¿Qué ocurre con aquellos contratos que necesitan de una formalidad específica?

Tal como hemos mencionado anteriormente, en el ordenamiento jurídico peruano existe el principio de libertad de forma. Sin perjuicio de ello, una práctica recomendable es que igual se redacten los contratos de la forma "tradicional" y posteriormente los términos y condiciones del mismo se traduzcan a *solidity* u otro lenguaje de programación. De este modo, las partes tendrán el contrato por escrito e inclusive podrán cumplir con todas las formalidades exigidas por ley y a su vez tener un *smart contract* que sea una representación de dicho contrato. De esta forma, se puede conseguir cumplir con los requisitos de validez del acto jurídico y poder ejecutar automáticamente las prestaciones del contrato una vez que se cumplan determinadas condiciones. Esta buena práctica podría lograrse al exigir a las partes contratantes que acepten términos en lenguaje natural que confieren un efecto contractual vinculante sobre la transacción realizada por el código. El contrato inteligente sería entonces "lanzado" y autoejecutado con efecto legal de acuerdo con los términos codificados. En consecuencia, con las medidas adoptadas para garantizar que se cumplan las formalidades legales y los elementos constitutivos de un contrato, es muy probable que un contrato inteligente y el resultado de su autoejecución puedan considerarse jurídicamente vinculantes[53]. La versión en "*word*" o "*pdf*" del contrato podría ser *hasheada* para que quede registrada en la *blockchain*.

2. ¿Cómo se firma un smart contract?

En principio, quien tiene acceso a su *wallet* puede autenticarse y celebrar operaciones con otra *wallet*. Sin embargo, en el mundo "*off-chain*" quien celebra un contrato, en muchas ocasiones, debe tener poderes suficientes para poder llevar a cabo dicho acto jurídico. Es por ello que una forma para firmar electrónicamente un *smart contract* podría ser a través de una videofirma que cuente con varias formas de autenticación y luego esta firma electrónica se registre en la *blockchain* a través de un *hash*.

3. ¿Qué ocurre si el *smart contract* tiene ciertos vicios e irregularidades?

Con la perfección del contrato, éste deviene en obligatorio y vincula a las partes, las cuales deberán cumplir lo expresado en el mismo —artículo 1361 Código Civil— No obstante, el contrato puede tener ciertos vicios e irregularidades que impidan que el contrato sea válido y, por ende, vincule a las partes. Esta cuestión resulta de enorme calado a la hora de relacionarlo con los contratos inteligentes dado que la automatización característica de los mismos es ajena a la concurrencia de toda clase de vicisitudes porque el software seguirá ejecutando

52. Pérez, Agustina. Concepto y aspectos legales a considerar en la formación de un contrato inteligente. Recuperado de: https://montevideolegalhac.wixsite.com/website/post/concepto-y-aspectos-legales-a-considerar-en-la-formaci%C3%B3n-de-un-contrato-inteligente

53. Revoredo, Abel. *Blockchain y Smart Contracts: ¿Hay futuro para los abogados?*

los términos reflejados en el código, sean estos legales o no. Sin embargo, un *smart contract* debe respetar lo dicho por el ordenamiento jurídico. En ese sentido, a pesar de que las prestaciones se ejecuten de forma automática a pesar de tener algún vicio, esta ejecución genera una serie de efectos jurídicos que el Derecho no puede dejar al margen. Por tanto, en caso de que concurran causales de nulidad o de anulabilidad, las partes podrán solicitar la restitución de las prestaciones. En otras palabras, al igual que un contrato "tradicional" se anula, un *smart contract* también podrá ser anulado. Por consiguiente, es importante que las partes prevean este supuesto.

4. ¿Qué cláusulas se deberían considerar a la hora de programar el *smart contract*?

Como bien señala Agustina Perez, la etapa de preparación del contrato inteligente puede considerarse una de las etapas más importantes de todo su proceso, por eso es importante tener un asesoramiento adecuado y un armado de estructura meticuloso y conservador. Mas allá de que es claro que no pueden contemplarse todos los posibles desarrollos, es pertinente tener algunos aspectos contemplados de forma previa a su ejecución. En todo el procedimiento, siempre debemos tomar en cuenta la regulación prevista en nuestro derecho y respetarla de acuerdo al tipo de contrato que estemos programando.

Sin perjuicio de que se contrate a un programador para redactar el contrato inteligente o se utilice un modelo, las partes deben incluir cuando menos las siguientes cláusulas:

a) Identificación de las partes: La posibilidad de que no sea posible o sea muy complicado identificar a las partes y que el *smart contract* se almacene en una red blockchain supone un serio obstáculo de cara a determinar la ley aplicable al contrato legal inteligente y la jurisdicción competente para conocer de las posibles disputas que puedan derivar del mismo. Es por ello que para que el contrato se cumpla, evidentemente se requiere conocer la identidad de las partes. Esta identidad debe estar vinculada a las claves públicas que utilizarán.

b) Ley aplicable y jurisdicción competente: Uno de los principales retos de la tecnología *blockchain* y la aplicación de los contratos inteligentes es que son un fenómeno multijurisdiccional, es decir, las partes están situadas en distintos países y el activo sobre el que se está transaccionando puede ser algo virtual, sin una presencia física. Esto es muy importante porque la mayoría de las veces se aplica una norma u otra en función de dónde esté físicamente el activo o las partes. Es por ello que es imperativo que las partes fijen voluntaria y expresamente cuál es la ley que rige el contrato y cuál es la jurisdicción competente en caso exista alguna controversia.

c) Cláusula de resolución de conflictos: Resulta importante que las partes prevean *ex ante* cómo es que se van a resolver los conflictos que pudieran darse en el futuro. Nada impide a las partes acudir alternativamente a un árbitro, que podría ser una opción más interesante que la de acudir al juez ordinario dada la especialización de los árbitros. Dicha cláusula podría recogerse tanto "*off-chain*" como en el propio *smart contract*, pudiendo articularse asimismo un mecanismo mediante el que se suspendiera la ejecución del *smart contract* hasta que el árbitro resolviera.

d) Interpretación del contrato: Se debe establecer si la programación prevalece sobre el contrato escrito o viceversa.

e) Utilización de oráculos: La verificación de las condiciones preestablecidas en el *smart contract* requerirá normalmente de la concurrencia de los denominados "oráculos", encargados de conectar el código con el mundo exterior y comunicar al primero la concurrencia de las condiciones preestablecidas en el *smart contract*. Una limitación de los *smart contracts* es que se encuentran limitados a obtener información de la misma *blockchain* y para autoejecu-

tarse requiere de información "*off-chain*". Un oráculo tiene como principal función, ser un servicio mediante el cual un *smart contract* se nutre de información externa a la *blockchain* sobre la que se ejecuta. Este "*input*" puede desencadenar una acción específica dentro de la misma según una determinada programación. Es por ello que resulta trascendental que el oráculo sea fiable y seguro al fin de evitar una auto ejecución equívoca.

f) Auditoría técnica antes de la ejecución del *smart contract*: Una auditoría de seguridad técnica proporciona un análisis detallado de las vulnerabilidades de un *smart contract*. Por lo general, los auditores examinan el código de los contratos inteligentes, redactan un informe y lo proporcionan al proyecto para que este trabaje con él. Luego, se publica un informe final en el que se detallan los errores pendientes y el trabajo ya realizado para abordar problemas de rendimiento o seguridad.

g) Cláusula de escape: ¿Un contrato inteligente es reversible? Si no lo es, ¿qué ocurre si se ejecuta automáticamente una operación incorrecta ya sea por un error humano en la codificación o por una situación "gris"? Es claro que la inalterabilidad del contenido del contrato inteligente debido a la característica propiciada por el uso de la tecnología *blockchain* tiene muchos beneficios como la seguridad y transparencia del acuerdo. Sin embargo, la inmutabilidad también genera un "riesgo de actuación" en la ejecución contractual, ya que las partes no están en la capacidad de prever con exactitud todos los supuestos de hecho a los que se enfrentarán. No existe contrato perfecto. Por tanto, esta característica de la *blockchain* haría que las partes se vean obligadas a trazar en detalle y con mucha minuciosidad cada una de las facetas y vías por las que el contrato debe desenvolverse. Esto sin duda genera enormes costos de transacción por lo que es importante tener un mecanismo de escape. Para ello debería el contrato codificarse con un plan B alternativo si el plan A falla y no se puede llevar a cabo la operación inicialmente deseada por las partes. Por ejemplo, el código tiene una ruta alternativa ejecutable en caso de que concurran determinadas circunstancias.

h) Remedios para errores de codificación, bugs, oráculos erróneos u otros fallos tecnológicos: En aquellos supuestos donde la inejecución contractual no es imputable a las partes, ya sea por un error de programación o un "*bug*" en el *smart contract* o porque el oráculo fue hackeado y dio información falsa, se daría un resultado no deseado por las partes. Si bien, una vez ejecutado el *smart contract*, se generaría una pretensión de restitución de lo pagado por la configuración de un enriquecimiento indebido, además de existir una pretensión de cumplir con la prestación debida, bien mediante un segundo *smart contract* correctamente redactado o bien por un contrato tradicional, esto en la práctica supondría que las partes incurran en altos costos de transacción. Por consiguiente, se deben pactar "*off-chain*" los remedios ante estas situaciones y asignar el riesgo ante el malfuncionamiento del *smart contract*.

Los *smart contracts* surgieron con la idea de aportar seguridad al cumplimiento de lo estipulado en una relación contractual haciendo que el incumplimiento contractual fuera costoso para el que lo incumpliera, evitando así la necesidad de acudir a los tribunales. En este sentido, la ejecución automática de los *smart contracts* no requiere de la intervención de las partes contractuales, lo cual restringe de forma importante el incumplimiento. Sólo el tiempo dirá si la sociedad se adecuará a esta realidad. También debemos de observar cómo es que esta tecnología se potenciará con el *machine learning* conllevando a que ese código sea capaz de hacer valoraciones subjetivas por sí mismo, como determinar si una sociedad está válidamente constituida para después ejecutar sobre ella esas órdenes.

IX. CONCEPTO DE TOKENIZACIÓN DE ACTIVOS

Recuerdo que cuando era niño iba a jugar *Street Fighter* o *Pacman* en estas máquinas de *arcade* en Daytona o en Larcomar. Para ello uno debía insertar una ficha que se canjeaba por dinero en un cajero. Una ficha equivalía a una determinada cantidad de soles de acuerdo con lo que el local establecía. Algo muy similar ocurre con las fichas que uno canjea en los casinos. En ambos ejemplos, se puede apreciar que existe un consenso entre todos los participantes en el que se le atribuye un determinado valor a estas fichas para emplearlos para un determinado fin. Y, en esencia, esto es lo que ocurre con la tokenización de activos, que no es otra cosa que la representación de un activo o un derecho en un activo digital.

El proceso de tokenización no es nada nuevo para el ser humano y ha existido desde mucho antes que aparecieran las redes de *Blockchain*. Los tokens representan cualquier forma de valor económico o derecho. Por ejemplo, las "*gift cards*", los programas de lealtad como los "puntos bonus" o el programa de millas, las fichas que entregan en los guardarropas de las discotecas, las pulseras para entrar a conciertos, zonas vips u hoteles "*all inclusive*" son formas de representar algo. Son tokens en el mundo analógico. Inclusive, si uno analiza detenidamente, el número de DNI es un token que representa la identidad de una persona. Un asiento en una partida registral es un token que representa algún derecho o acto inscribible.

Ahora bien, cuando hablamos de la tokenización de activos nos referimos a la transformación y representación digital de activo(s) o de derecho(s) dentro de una *Blockchain*. Dicho proceso digital crea un bloque dentro de la *Blockchain* en donde se logran registrar las propiedades únicas del activo o del derecho que se está tokenizando. En otras palabras, en la Blockchain se almacena toda la información referente al objeto o derecho que se está tokenizando. Una vez creado el token, este puede intercambiarse, almacenarse y compartirse libremente. La tokenización es, en definitiva, la conversión de los derechos de propiedad de un activo o la transformación de los derechos de un título en un 'token' comercializable dentro del espacio *Blockchain*.

Tokenizar es representar un derecho —personal o real, o sobre un bien tangible o intangible— en un registro distribuido —*Blockchain*— privado a efectos legales —en el sentido de que no está respaldado por la Administración, como ocurre con el Registro Mercantil o con el Registro de la Propiedad, por ejemplo— y público o semipúblico a efectos tecnológicos, materializándose dicha representación en anotaciones contables unitarias llamadas tokens. Además, dichos tokens irán ligados siempre a una cuenta concreta —denominado, en la jerga *Blockchain*: *wallet* o monedero— que permitirá poseer y transferir los tokens. Por tanto, los tokens son, en esencia, transmisibles y, generalmente, su legítimo propietario es el propietario de la *wallet* que los almacena y controla[54].

Si acabas de leer los dos párrafos anteriores y te suenan a "chino mandarín" no te preocupes que hasta hace poco estaba en la misma situación. Es por ello que considero que es de suma importancia aterrizar en ejemplos cómo es que se puede utilizar la tokenización de activos en nuestra vida cotidiana.

Si eres fanático del deporte, como yo, este ejemplo te puede servir para entender lo que son los tokens. Imaginemos que tu club favorito de fútbol emite mil "*fan tokens*". Quien compra estos tokens tendrá derecho a descuentos en entradas y mercancía oficial del equipo. También da el derecho a reunirse de forma privada una vez cada 6 meses con los jugadores y adquirir pasajes en avión para acompañar al equipo en todos sus partidos de visitante, entre

54. Pascual, Javier. Tokenización de activos: Naturaleza jurídica del token y del activo. Recuperado de: https://www.legaltoday.com/legaltech/novedades-legaltech/tokenizacion-de-activos-naturaleza-juridica-del-token-y-del-activo-2019-11-20/

otras experiencias y recompensas. Seguramente te estás preguntando: *¿Para qué necesito un token si esto lo puedo hacer con una promoción común y corriente?*

La *Blockchain* permite garantizar la trazabilidad del token. Dicho de otro modo, esta tecnología permite crear una base de datos electrónica que refleje a tiempo real quiénes son los titulares de ese derecho en cada momento y en él se establecen las reglas para que dicha base de datos pueda modificarse cada vez que el derecho se transmita, determinando con ello quién es el nuevo titular. Esto nos lleva del "*Internet de la información*" al "*Internet de Valor*". Si pensamos en un archivo pdf como activo digital, una vez enviado se pierde el control del bien, dado que cualquiera lo puede enviar, reutilizar o eliminar. En cambio, con la tokenización, siempre se puede trazar en la Blockchain la titularidad del token. Esto permitiría, en el ejemplo anterior, que cuando un hincha, titular del token, se aburra de los beneficios de este lo pueda vender a otro hincha. El token se puede programar de tal manera que, ante cada transacción, el club pueda percibir un ingreso por esa venta, lo cual cambia las reglas de juego completamente.

Pongamos otro ejemplo. Imaginemos que tienes una banda de música y en vez de firmar un contrato con una disquera decides emitir tokens que representen el 20% de los derechos de autor por perpetuidad sobre la música que compongan. Los fans que confiaron en el grupo desde un inicio van a poder ganar el 20% de las regalías y cada vez que ellos decidan vender sus tokens a otros fans, la banda también podrá percibir un ingreso por esa venta. Si los tokens se adquirieron a US$2,000 cada uno y luego el grupo termina siendo el nuevo "Nirvana", los fanáticos podrían venderlos por cientos de miles de dólares. Sin duda alguna un "*game changer*".

No cabe duda de que la capacidad disruptiva de la tecnología *Blockchain* la encontramos en la tokenización. Tal como se señala en el libro "La Economía del Token" de Shermin Voshmgir: "*La posibilidad de desplegar tokens a un bajo costo y relativamente con poco esfuerzo en una infraestructura p2p puede cambiar las reglas del juego, porque hace económicamente posible representar muchas clases de activos y de derechos de acceso de una manera digital que en el pasado no era posible*". La tokenización de activos en Blockchain puede aplicarse prácticamente a cualquier cosa. La NBA puede tokenizar momentos legendarios y venderlos como coleccionables. Los desarrolladores de juegos van a crear videojuegos en donde sus jugadores puedan "jugar para ganar" —"*play to earn*"— los tokens del mismo juego para luego ser canjeados por dinero real o inclusive cambiarlo por otros tokens que sirvan para otros videojuegos. Las empresas podrán emitir deuda para financiarse a través de tokens. Asimismo, las acciones, los bonos y los inmuebles también podrán ser tokenizados. Inclusive las identidades de las personas podrán ser tokenizadas. Esta capacidad de tokenización abre las puertas a una transformación digital sin precedentes.

Lo que diferencia esta tokenización con otros procesos de representación virtual —como las millas, por ejemplo— es que el token cuenta con una lógica interna, que se encuentra sujeto a ciertas condiciones. Es aquí en donde el fenómeno de tokenización se junta con el fenómeno de los contratos inteligentes, que son el código responsable no sólo de crear a los tokens sino también de gestionar las transacciones que se realizan con los tokens. En términos sencillos, el *smart contract* actúa como el cajero en la tienda de arcade cambiando el dinero por fichas. Esa es la relación que existe entre un token y un *smart contract*. En términos jurídicos, el token es el objeto digital —bien materia del acto jurídico— sobre el que incide el código informático del *smart contract*.

En definitiva, el proceso de tokenización se refiere a la emisión de tokens que se introducen como bloque dentro de una *Blockchain* y pueden ser almacenados y transferidos en el mundo digital. Estos tokens existen en la *Blockchain*, actúan como una reserva de valor y otorgan a sus titulares los derechos de los activos que representan, mientras que los activos del mundo real respaldados por estos tokens continúan existiendo "*off-chain*". Desde un punto de vis-

ta jurídico, cuando hablamos de "tokenización" de activos estamos hablando de un negocio jurídico complejo, unilateral y recepticio integrado normalmente por el negocio jurídico de la emisión y el de representación digital propiamente dicho[55].

Después de entender que la *tokenización de activos* no es más que una forma extravagante de hablar de *titulización de activos y derechos a través de la Blockchain*, lo que corresponde cuestionarnos es cuál es la naturaleza jurídica de los tokens. Vale preguntarse si un token que represente un derecho a un descuento de un determinado producto o servicio tendrá la misma naturaleza que un token que represente un bien inmueble o un valor mobiliario.

Si se analiza al token de forma aislada podemos concluir que las características de un token son las siguientes:

a) Es susceptible de valoración económica y formará parte del patrimonio de una persona por lo que es considerado como un bien;
b) Al poder trasladarse de "*wallet*" a "*wallet*" y ser apropiado por la esfera jurídica de un sujeto, será considerado como bien mueble;
c) Algunos tokens son fungibles y otros no. Por ejemplo, el *bitcoin* o el *ether* y, en general, los tokens que siguen el estándar ERC-20 son bienes fungibles; es decir, que puede ser recíprocamente sustituido por otro. Sin embargo, también pueden existir tokens no fungibles, que siguen el estándar ERC-721. Estos últimos son los famosos "*NFTs*".
d) Se encuentra dentro del tráfico mercantil —salvo que represente un activo prohibido—.
e) Puede ser divisible o indivisible. Será divisible cuando se pueda dividir en fracciones más pequeñas como sucede con *bitcoin* y sus *satoshis*. Será indivisible cuando los tokens estén vinculados a la identidad, como los certificados y los títulos. No tendría sentido tener una fracción de un título o de una licencia de conducir.

Sin embargo, enunciar las características de los tokens no responden realmente si el token es el derecho subjetivo que está representando o si es la ficha digital sobre la que recae un derecho de propiedad. En mi opinión, me inclinaría más por la primera postura, dado que la naturaleza jurídica del token es muy similar a un título valor, ya que es un activo digital que contiene un derecho. El token será el título representativo del derecho subyacente que se encuentra registrado en la Blockchain. Debido a que nuestra legislación no contempla la figura de la tokenización de activos, se deberá analizar caso por caso si es que los derechos que se pretenden tokenizar son susceptibles de tal proceso.

Un tema que es de bastante importancia cuando se pretenda determinar la naturaleza jurídica del token es ver si existen elementos particulares de los activos o derechos que se pretendan tokenizar y ver si esto puede alterar el marco regulatorio aplicable a los mismos. Generalmente, esto sucede cuando el token se desenvuelve en el ámbito de sectores regulados o con grandes formalidades o restricciones para celebrar determinadas transacciones. Si bien no existe un consenso regulatorio internacional sobre las clases de tokens y su naturaleza jurídica, considero que se pueden clasificar en los siguientes tipos:

a) Tokens de pago o de intercambio: Son aquellos que son usados como un mecanismo de intercambio con la finalidad de adquirir bienes o servicios o utilizarlo como depósito de valor. En esta categoría entraría *bitcoin*, *ether*, *sol*, *doge*, así como los *stablecoins* o monedas estables como *tether*, que normalmente se encuentra res-

55. Ruiz-Gallardón y García de la Rasilla, Miguel. Tokenización de activos y blockchain. Aspectos Jurídicos. Recuperado de: https://www.elnotario.es/hemeroteca/revista-91-92/10107-tokenizacion-de-activos-y-blockchain-aspectos-juridicos

paldada por un activo a efectos de no verse afectado por la volatilidad del mercado.

b) *Security* Tokens o Tokens de Inversión: Aquellos tokens cuyo derecho subyacente otorga derechos sobre el capital de una sociedad, sus dividendos o emisión de deuda. Es transmisible y existe una expectativa por parte del adquirente de obtener un beneficio económico, mientras que por el lado del emisor busca un financiamiento. Si bien en el Perú, este tipo de tokens no encajan dentro de la definición de "valores mobiliarios", la Ley de Promoción del Mercado de valores autoriza a la Superintendencia de Mercado de valores a aplicar el principio de "primacía de la realidad" para definir cuándo estamos frente un activo financiero, cuya compra o suscripción es publicitada en forma masiva —por ejemplo, a través del internet o redes sociales— por personas o entidades no supervisadas. Es decir, bajo la legislación actual los reguladores podrían restringir la comercialización de este tipo de tokens si consideran que funcionan como activos financieros.

c) *Utility* Tokens o Tokens utilitarios: Es aquel token cuyo derecho subyacente representa un uso específico, normalmente de un bien o un servicio. Se trata de promociones, descuentos, accesos. Tiene por fin fidelizar a los titulares de los tokens. No es un instrumento financiero, a pesar de que por sus características técnicas sea esencialmente transmisible. Se rige por el derecho civil y mercantil.

Un reto legal al que se enfrentan los tokens es que, en ocasiones, las propias características de los tokens permiten su uso para más de una finalidad e inclusive se puede desviar de lo originalmente planeado, ya que finalmente las leyes de oferta y demanda por un determinado token pueden elevar su valor y, finalmente, ser comercializados en un mercado secundario. Los usuarios podrán, por tanto, especular con el precio de éste y ser tratados como activos financieros. Esto puede generar la interrogante si un *Utility Token* se puede convertir en un *Security Token*. Tomando como referencia la práctica española, resulta muy importante ver cuál es la intención inicial a efectos de determinar su naturaleza jurídica, sino todos los tokens podrían ser "destrozados" por la conducta de los usuarios y desviarse de su naturaleza original. Para ello, es importante que el emisor especifique en el *White Paper* cuál es la razón determinante de crear ese token. Asimismo, este documento deberá estar alineado con los términos y condiciones de uso, así como con todo el material publicitario. En buena cuenta, la coherencia en el deber de información determinará hasta cierto punto la naturaleza jurídica del token.

Otro aspecto legal que se debe tomar en consideración es el proceso de tokenización del activo o derecho. El mismo comienza con un estudio de factibilidad, en donde se realiza un análisis exhaustivo del activo o derecho que se pretende tokenizar. Es en este punto en donde se debe definir si es viable o no la tokenización. Un segundo paso es ver cuál es el tipo de token que vamos a emplear para el negocio o transacción que el cliente tiene en mente. Finalmente, se deben considerar determinadas cláusulas en el *Smart Contract* no sólo para la emisión del token, sino que también es importante definir con claridad las reglas para transferir los tokens y los derechos que éstos otorgan a sus titulares. Como bien menciona Agustina Pérez[56], es importante entender que no nos encontramos ante un nuevo tipo de contrato, sino ante una nueva herramienta para contratar con medios electrónicos que permite aplicar de manera profunda el famoso principio de "*pacta sunt servanda*" —la eficacia o cumplimiento no puede dejarse al arbitrio de una de las partes—.

Uno de los desafíos prácticos que actualmen-

56. Pérez, Agustina. Concepto y aspectos legales a considerar en la formación de un Contrato Inteligente. Recuperado de: https://montevideolegalhac.wixsite.com/website/post/concepto-y-aspectos-legales-a-considerar-en-la-formaci%C3%B3n-de-un-contrato-inteligente

te existe es el riesgo de doble tokenización. Es decir, resulta sumamente difícil saber si un activo tokenizado no ha sido tokenizado previa o posteriormente en otra red *Blockchain* de forma paralela. Si bien en el contrato se puede establecer una cláusula de resolución automática y una penalidad por los daños y perjuicios en caso se realice esto, lo cierto es que es un punto importante para considerar. Una posible solución es que para el caso de los activos que son registrables se podría inscribir en la partida registral un asiento en donde conste que dicho activo ha sido tokenizado a fin de saber cuándo y en qué red se tokenizó. Sin embargo, los bienes no registrables no podrían optar por esta solución. Para estos casos, la solución deberá ser propuesta por un privado, ya sea una empresa que certifique o registre de forma privada las tokenizaciones a efectos de brindar seguridad en el tráfico mercantil.

A modo de conclusión, la tokenización de los activos va a revolucionar el mundo, ya que se puede tokenizar prácticamente todo. Esto va a permitir que tanto los empresarios, consumidores e inversionistas vivan en un mundo más líquido, transparente y eficiente. De otro lado, nosotros, los abogados, nos enfrentamos a un sinnúmero de retos legales que probablemente aún no avizoramos. Actualmente existe un marco regulatorio que no ha sido diseñado o pensando en esta nueva realidad por lo que nuestra labor consistirá en navegar entre la implementación de nuevas tecnologías y un ordenamiento jurídico complejo. Por consiguiente, se debe analizar minuciosamente todos los elementos jurídicos relativos a toda clase de tokenización, la naturaleza jurídica del token y, sobre todo, el sector de actividad para que, tras dicho estudio, se pueda valorar si dicho proceso de tokenización aporta seguridad jurídica y, por tanto, supone una mejora real para todas las partes.

X. DECENTRALIZED AUTONOMOUS ORGANIZATIONS — DAOS

La aparición de las DAOs es una progresión natural del uso de la tecnología blockchain por parte de la sociedad. Pero ¿qué es una DAO? Las siglas "DAO" provienen del inglés Decentralized Autonomous Organization, que quiere decir Organización Autónoma Descentralizada. Una DAO es una organización cuyos estatutos y normas se encuentran codificadas en un smart contract y las reglas programadas se registran en una blockchain, lo que brinda transparencia, inmutabilidad, autonomía y seguridad. Una DAO es una forma innovadora de organizar y hacer funcionar a las empresas porque se automatiza a través de un smart contract las funciones de los órganos de administración. En otras palabras, una DAO utiliza la tecnología blockchain para gestionar una sociedad a través de reglas o protocolos autoaplicables.

¿Cómo opera una DAO? Imaginemos que una cafetería ha optado por organizase a través de una DAO. Todo el dinero que perciba por la venta de café será gestionado de forma automática. El stock del producto se reordena de acuerdo con las reglas consignadas en el contrato inteligente. Asimismo, también se programa la limpieza del local y el pago del alquiler. Además, a medida que el negocio evoluciona, los titulares de los tokens de gobernanza pueden ejercer su voz y voto para la toma de decisiones. Una vez tomada la decisión, el código lo ejecuta. En la DAO, no hay un órgano de administración, ya que todos estos procesos fueron prescritos y ejecutados por un código. Entre más complejo el negocio, más complejas serán las reglas que rijan el smart contract. Lo constante es que el código reemplaza a los administradores y son los titulares quienes deciden de forma democrática y participativa.

Como bien se puede apreciar del ejemplo anterior, a diferencia de las estructuras societarias tradicionales, una DAO no tiene un liderazgo o una gestión centralizada. La idea principal detrás de las DAO es que la gobernanza de una sociedad funcione plenamente sin una gestión jerárquica centralizada. Este modelo busca prescindir de los órganos de administración, ya que la DAO es gobernada y gestionada por contratos inteligentes en donde se automatizan las tomas de decisiones a través de procesos democráticos y participativos. En consecuencia, los miembros aceptan el uso de contratos inte-

ligentes para administrar, gobernar y, efectivamente, automatizar la organización.

Este tipo de organización pretende resolver el problema de agencia que existe entre los administradores y los accionistas. Los problemas de agencia se originan porque una persona u organización denominada "agente" tiene la capacidad de tomar decisiones y llevar a cabo acciones en nombre de otra denominado "principal", pudiendo el agente desatender los intereses del principal por maximizar su propio interés. Esto se debe principalmente por las siguientes razones[57]:

a) La conducta maximizadora de las partes la cual produce conflictos de intereses. Si asumimos que tanto el principal como el agente son sujetos maximizadores de su propio beneficio —individual—, es posible que se produzcan situaciones donde los intereses y objetivos perseguidos por ambas partes, no necesariamente coincidan y que cada uno vele por sus propios intereses.

b) La asimetría en la información que favorece al agente. Generalmente es el Agente quien tiene mayor conocimiento y experiencia acerca de la actividad que realiza y el valor de las funciones y actividades que desempeña, mientras que el Principal posee un menor grado de información o le es más costoso informarse.

c) El hecho que los agentes no asumen la totalidad de los costos y beneficios de sus acciones.

Las DAOs justamente buscan resolver el problema de agencia puesto que no permiten el abuso o los probables riesgos en la toma de decisiones, por parte de un individuo que actúe en su propio beneficio y olvide el interés general. El agente es reemplazado por el *smart contract*, que en buena cuenta ejecuta un conjunto de reglas preprogramadas y coordinadas a través de un protocolo de consenso distribuido. En esencia, las DAOs eliminan o minimizan los roles de los directores y gerentes en la organización, confiando, en cambio, en reglas transparentes que se aplican a todos los miembros y participantes.

La siguiente tabla demuestra las principales diferencias entre una DAO y las estructuras societarias tradicionales:

DAO	Organizaciones Tradicionales
Estructura plana y democratizada	Estructura jerárquica
Para implementar cualquier decisión en la organización los miembros deben votar	Dependiendo de la estructura societaria, las decisiones son tomadas por el directorio o la gerencia.
La toma de decisiones se encuentra tokenizada y depende del protocolo de consenso establecido.	Las decisiones son tomadas por el directorio o la gerencia.
La votación de los miembros es continua, digital y descentralizada —sin intermediarios—. La decisión de la mayoría se ejecuta automáticamente.	La votación se debe realizar en una junta general, que, por lo general está sometida a ciertas formalidades. La decisión es ejecutada por los órganos de administración.
Toda la actividad es transparente, accesible y totalmente pública al quedar registrada en la *blockchain*.	La actividad realizada por el directorio y la gerencia es privada y reservada.
Su gestión se basa en las reglas prestablecidas en los *smart contracts* o contratos inteligentes.	Su gestión se basa en la actividad realizada por el directorio y la gerencia.

57. Martínez, Juan José. "Apuntes Sobre El Rol Del Derecho Frente Al Problema De La Agencia En Las Organizaciones." Themis 46, (2003): 48. https://revistas.pucp.edu.pe/index.php/themis/article/view/9973

Cabe señalar que las DAOs cuentan con una serie de mecanismos que son los que garantizan su funcionamiento en todo momento:

a) **Smart Contract:** Como mencionamos anteriormente, la columna vertebral de una DAO es el *smart contract*, ya que en este se codifican las reglas que rigen la vida y funcionamiento de la organización. En ese sentido, para que una DAO se encuentre operativa, en primer lugar, debe definir el conjunto de normas que regirán el funcionamiento de la organización. Este primer paso está relacionado con la capacidad de programar acciones y hacer que se ejecuten automáticamente de acuerdo a unos determinados parámetros. Para ello, los desarrolladores deben comprender completamente el problema de gobernanza que están tratando de codificar para crear un contrato inteligente exitoso que sirva como base de DAO.

b) **Protocolo de Consenso:** Una vez establecidas las reglas, se debe definir cuál es el protocolo de consenso que se va a utilizar. Este mecanismo busca garantizar que las decisiones a las que se lleguen dentro de la DAO sean adoptadas por el consenso de sus partes y que ningún factor externo afecte la toma de decisiones. A modo de ejemplo en "*The DAO*"[58] el proceso de toma de decisiones es el siguiente[59]:

   i. Mediante la creación de un smart contract, se realiza una propuesta o proyecto para que sea acometido por la DAO. La persona que realiza la propuesta, denominado *contractor*, debe ser titular de tokens de la DAO, además de realizar un depósito en Ether.

   ii. Una vez diseñado el smart contract y subido a la red de Ethereum, los *tokens holders*, actuando como nodos de la red, alcanzarán un consenso, decidiendo de ese modo qué propuestas son aprobadas y qué proyectos acomete la DAO.

   iii. En caso de aprobarse la propuesta del *contractor*, se procede a cerrar el bloque y unirlo a la cadena, obteniéndose por el *contractor* una recompensa —ya sea en tokens de la DAO o en otra criptomoneda.

   Es necesario destacar que todo este proceso se hace de forma totalmente automática y descentralizada. Es decir, mediante un smart contract alojado en la propia *blockchain*, se produce la votación, y se ejecutan todos los automatismos necesarios, desde la obtención de la recompensa por el *contractor* hasta la implementación del proyecto mismo, si esto fuera posible.

   iv. Emisión y financiación a través de tokens de gobernanza: Es necesario que la DAO se financie a fin de que sea económicamente viable. Para ello, la DAO se financia a través de la emisión de tokens, los cuales permiten a sus titulares obtener derechos políticos y económicos dentro de la organización. Es decir, en una DAO los derechos de voto se obtienen mediante la adquisición del token de la DAO. Estos tokens son divisibles e intercambiables entre los distintos titulares. Por lo tanto, para la creación de una DAO es necesaria la formulación de un vehículo de inversión, ya sea en forma de *Initial Token Offering*, mediante el cual los inversores aporten un capital —normalmente mediante una criptomoneda como

58. Este proyecto creado en 2016 por Simon Jentzsch y Christoph Jentzsch fue lanzado con el objetivo de construir la DAO más importante de Ethereum.

59. Pastor, Pablo. La Tecnología Blockchain aplicada al Derecho de Sociedades. Universidad Internacional de Andalucía, 15.

ether— a cambio de los tokens creados por la DAO. Una vez financiada la DAO, ya existirían lo que serían los socios o accionistas de la organización, o más bien los denominados *tokens holders*.

Estos tokens también sirven como recompensa económica por establecer propuestas. Las DAOs emplean mecanismos económicos para alinear los intereses de la organización y los de sus miembros, normalmente, a través del uso de la teoría de juegos.

v. *Blockchain*: Finalmente, cuentan con un cuarto mecanismo cuya finalidad es grabar todo lo que sucede en la DAO. Esta tarea recae en la *blockchain*, donde toda la información es almacenada para ser accedida de forma pública y garantizar su seguridad. La tecnología *blockchain* representa una cadena de bloques que se configura como una base de datos distribuida, compartida y segura. Funciona como un documento público de transacciones, donde quedan registrados todos los movimientos mediante códigos. Aquí se almacena toda la información y las transacciones que se producen dentro de la organización descentralizada.

Una vez finalizado el período de financiación y desplegado una DAO, esta se convierte en un organismo totalmente autónomo y completamente independiente de sus creadores, así como de cualquier otra persona. Son de código abierto, lo que significa que su código puede ser visto por cualquiera. Además, todas las normas y transacciones financieras se registran en la cadena de bloques. Esto hace que las DAOs sean totalmente transparentes, inmutables e incorruptibles.

Luego de haber analizado, de forma resumida, qué es una DAO y cuáles son los mecanismos de funcionamiento habituales de este tipo de organización, es necesario abordar si es que esta figura encaja con el Derecho de Sociedades peruano y cuáles serían los inconvenientes y fricciones de incorporar esta figura a nuestro ordenamiento jurídico.

En primer lugar, las DAOs no encajan en ningún tipo de organización en nuestro ordenamiento jurídico. El artículo 2 de la Ley General de Sociedades establece que toda sociedad debe adoptar alguna de las formas previstas en dicha ley. En tal sentido, si un grupo de emprendedores decidiera organizarse como una DAO para llevar a cabo su emprendimiento, existirá incertidumbre jurídica respecto a los derechos y obligaciones derivadas del establecimiento de una DAO. Cabe señalar que en el Estado de Wyoming se aprobó una norma en donde se le otorga a las DAOs la categoría de sociedades de responsabilidad limitada — LLC.

En segundo lugar, el sistema que propone implementarse mediante las DAO colisiona con las estructuras de gobierno corporativo tradicionales que se encuentran consolidadas en nuestro ordenamiento jurídico. Nuestro marco normativo busca atribuir responsabilidad tanto al directorio como a la gerencia por las decisiones tomadas y ejecutadas por los acuerdos o actos que sean contrarios a la ley, al estatuto o por los realizados con dolo o aquellos que impliquen un abuso de sus facultades o por negligencia grave. En el caso de una DAO, al no tener administradores, cabe cuestionarse quiénes serían los responsables solidarios en caso la sociedad ocasione un daño a un tercero.

Otro aspecto que no encaja es que los acuerdos deben constar en actas, las cuales se encuentran sometidas a distintas formalidades. En cambio, en una DAO estas formalidades se obvian en post de la automatización que implica la elevación de propuestas a través de *smart contracts*, los cuales son autoejecutables una vez adoptado un determinado consenso.

Finalmente, no podemos olvidar que una DAO es tan buena como su *smart contract*. Cabe señalar que la autonomía completa de un *smart contract* puede ser una espada de doble filo y deben tomarse recaudos a nivel de arquitectura de software que permitan modificar los outputs de un contrato inteligente en función de

distintos inputs variables, o que permitan directamente eliminar el contrato de la *blockchain* mediante una función de "*autodestrucción*". De lo contrario, la DAO no podría ser modificada y es posible imaginar casos donde tokens sean retenidos *ad infinitum* por un error de programación. Un contrato inteligente que retenga lo que, por alguna razón, debe ser liberado, debe poder ser eliminado.

A modo de conclusión, las denominadas DAO no tienen actualmente asidero en nuestro ordenamiento jurídico, siendo que no es posible una organización íntegramente alojada en *blockchain*, descentralizada y automatizada en su integridad. Sin embargo, es importante analizar estas nuevas formas de organización que surgen con las nuevas tecnologías porque cuestionan el fundamento de las instituciones tradicionales y su incorporación puede ser beneficioso para la sociedad. Además, es altamente probable que en esta década exista una "explosión" de DAOs porque muchas personas decidirán llevar a cabo sus proyectos de esta forma, siendo consideradas "asociaciones de hecho" o "sociedades irregulares". Es por ello que es un asunto que amerita mucho estudio, así como mucho cuestionamiento sobre conceptos que creíamos que estaban escritos en piedra.

XI. REFLEXIONES FINALES

a) En el Perú no existe un marco jurídico específico que regule la tecnología *blockchain*. Las iniciativas y proyectos *blockchain* no esperan a nuevas regulaciones, simplemente avanzan y, por tanto, debemos aplicar nuestro ordenamiento jurídico actual a las materializaciones de esta tecnología. Este es uno de los desafíos más importantes porque no solo nos enfrentamos a la complejidad de los elementos tecnológicos de la *blockchain*, sino a la velocidad con la que surgen nuevos proyectos completamente innovadores, poniendo en tela de juicio instituciones jurídicas que llevamos años construyendo. Sin embargo, como abogados, debemos entender que este no es un fenómeno nuevo: El Derecho está diseñado para aplicarse a situaciones imprevisibles que no han ocurrido pero que ocurrirán. En ese sentido, es nuestro deber aprender a interpretar la norma, aplicarla a los fenómenos tecnológicos para luego desarrollar marcos normativos que promuevan e incentiven aquellas conductas que saquen el mejor provecho de esta tecnología y beneficie en última instancia a la sociedad.

b) La revolución de la tecnología *blockchain* es que permite intercambiar valor a todos sus usuarios sin la necesidad de contar con una entidad central o un intermediario de confianza. *Bitcoin* permite intercambiar criptomonedas sin la necesidad de una institución financiera. Un grupo musical podrá ser financiado directamente por sus propios fans a través de tokens, dejando de lado a las productoras y disqueras. Es en virtud de la descentralización, transparencia, inmutabilidad y confianza que los creadores de *tokens* puedan ser controlada por sus creadores y no se pierdan en el ciberespacio.

c) No existe una norma que regule a las criptomonedas; sin embargo, podemos señalar que las criptomonedas en nuestro ordenamiento jurídico son bienes muebles, intangibles, fungibles y no consumibles.

d) En relación a los *smart contracts*, es importante señalar que el hecho de que los contratos legales inteligentes se redacten, en todo o en parte, en forma de código informático no supone ningún obstáculo para reconocerles la consideración de un contrato dado que el Código Civil peruano consagra el principio de libertad de forma y son una expresión adicional del fenómeno de contratación electrónica. Por tanto, para su validez, al igual que cualquier otro tipo de contrato, deberán reunir los requisitos esenciales para la validez de todo contrato; esto es, que los agentes capaces hayan manifestado su consentimiento, el objeto contractual sea física y jurídicamente posible, que cuente con un fin lícito y que siga la formalidad exigida por ley.

e) El concepto de tokenización de activos se refiere a la transformación y representación digital de activos o de derechos dentro de una red *blockchain*. Un tema que es de bastante importancia cuando se pretenda determinar la naturaleza jurídica del token es ver si existen elementos particulares de los activos o derechos que se pretendan tokenizar y ver si esto puede alterar el marco regulatorio aplicable a los mismos. Esto es de suma importancia dado que habrá tokens que serán regulados por la normativa mercantil mientras que otros podrán ser regulados por normas especiales del mercado de valor o regulación financiera.

f) Las DAOs son incompatibles con la regulación de sociedades o de asociaciones en nuestro ordenamiento jurídico, puesto que lo que pretenden es prescindir de los órganos de administración cambiándolos por *smart contracts*. Resulta interesante que se busquen eliminar los problemas de agencia con esta figura; sin embargo, nuestro marco normativo está diseñado para que los administradores sean los responsables frente a la persona jurídica por las decisiones tomadas y ejecutadas por los acuerdos o actos que sean contrarios a la ley, al estatuto o por los realizados con dolo o aquellos que impliquen un abuso de sus facultades o por negligencia grave. En el caso de una DAO, al no tener administradores, cabe cuestionarse quiénes serían los responsables solidarios en caso la sociedad ocasione un daño a un tercero.