UNIVERSIDAD DE SAN ANDRES

DEPARTAMENTO DE DERECHO EMPRESARIO

MAESTRIA DE DERECHO EMPRESARIO

TRABAJO FINAL:

"BEWARE OF GEEKS WEARING FORMULAS"

UNA APROXIMACIÓN A LA CARACTERIZACIÓN DE BITCOIN COMO MONEDA EXTRANJERA

Autor: Franco J. Rodríguez Vázquez
DNI 27.119.220
Director de Tesis: Marina Bericua

Ciudad Autónoma de Buenos Aires 31.07.2019

CONSIDERACIONES PRELIMINARES

La crisis financiera del 2008 tuvo un profundo impacto negativo en calidad de vida de la sociedad mundial que contribuyó a generar mayor desconfianza de los consumidores hacia la manera en que las entidades financieras realizan sus negocios y la capacidad de los gobiernos y entidades públicas para supervisar y controlar a estas entidades.

De este estado de frustración y desconfianza nació Bitcoin, la primera critpomoneda o moneda virtual, creada por Satoshi Nakamoto. Bitcoin se basa en la tecnología de código abierto Blockchain para su creación, administración, validación, y registro distribuido a través de usuarios particulares diseminados en toda la red. La creación, administración, validación y registro no requiere intervención de ningún gobierno ni de ninguna entidad pública ni privada centralizada.

Bitcoin y Blockchain constituyen una tecnología disruptiva que está cambiando la forma de pensar el dinero y la forma en la cual opera el mercado financiero mundial. El impacto de Bitcoin y Blockchain es tan significativo, que otras personas, gobiernos y ahora los gigantes digitales Facebook, Ebay, MercadoPago, entre otros crearon o están prontos a lanzar nuevas monedas virtuales.

Hoy en día existen usuarios de Bitcoin en todos los países del mundo, y aunque las monedas virtuales no son utilizadas habitualmente como medio de pago, es indudable que van adquiriendo un mayor grado de aceptación y de uso.

Ante este escenario, resulta importante saber qué es Bitcoin para la ley argentina ¿es una moneda? Si así lo fuera, ¿Es una moneda de curso legal? ¿Es una moneda extranjera? Las respuestas a estas preguntas determinarán consecuencias desde el punto fiscal, como respecto de su capacidad cancelatoria y liberatoria como medio de pago, su exigibilidad, su transmisión, y su conservación.

OBJETIVO

Mediante este trabajo intentaré demostrar que, para la ley argentina, Bitcoin es asimilable a una moneda extranjera.

METODOLOGÍA

A los fines de alcanzar los objetivos de la presente investigación, analizaré normativa vigente sobre moneda extranjera, obligaciones en moneda extranjera, así como jurisprudencia y doctrina relacionada a Bitcoin. Para el análisis de qué es Bitcoin y cuáles son sus usos analizaré información en páginas web, seminarios, y una entrevista personal con un programador.

A efectos de exponer los resultados de esta investigación, explicaré como funciona Blockchain y Bitcoin, y cada uno de sus características esenciales, los motivos por los cuales Bitcoin no es una moneda de curso legal en la Argentina y porque Bitcoin debería ser para la ley argentina asimilada a moneda extranjera.

Indice Temático

"Ante todo partimos de que el universo es caos, y que el caos es anarquismo y descentralización, pero que existen condiciones naturales para que éste caos, dentro de su libertad, se alinee y que de por resultado construcción.[1]"
Rodolfo Andragnes

1. Introducción. Hipótesis.

William Batchelder Green fue un individualista, anarquista, y un pionero de la banca libre. Nacido en 1819, en Massachussets, Estados Unidos, que creó la idea de los bancos mutualistas, un sistema de bancos libres y gratuitos según el cual "moneda" podía ser cualquier cosa que pudiere ser vendida o permutada. Los bancos mutualistas podrían circular sus monedas libremente, las cuales se encontrarían respaldadas en propiedad de todo tipo y la competencia entre ellos haría que el precio del crédito baje, permitiendo que quien necesite dinero pueda tomarlo al costo.

El banco mutualista, organizado en forma de cooperativa y de propiedad de sus miembros proveería crédito barato y abundante para los pobres para poder organizarse y competir contra los monopolios.

El objetivo de Greene era disolver la intervención del estado en las relaciones económicas, con la expectativa de que la industria, la cooperación y el comercio harían que el estado quede obsoleto. De esa manera, Greene creía que un sistema descentralizado recompensaría a quienes trabajan más y distribuiría la riqueza una manera más equitativa.

Si bien la idea de Greene nunca alcanzó gran difusión, podríamos decir que constituye evidencia de que desde hace años ciertos sectores de la sociedad realizan esfuerzos para crear un sistema monetario privado, distinto y separado del sistema bancario tradicional y del control central del estado con el fin de evitar el pago de comisiones y controles que encarecen su circulación.

Al igual que la idea de bancos mutuales de Greene, Bitcoin también surgió como un movimiento anárquico, como una reacción a la crisis financiera mundial del año 2008, y en consecuencia, una reacción al sistema bancario y monetario formal y tradicional conformado por gobiernos y bancos. La idea de un sistema monetario descentralizado, privado, y anónimo, sin intervención del estado ni la intermediación de instituciones bancarias, donde cada uno de los miembros verifica la validez de cada transacción es la idea que a impulsado a todos los creadores de las monedas virtuales que se han montado en Blockchains descentralizadas.

A diferencia de las ideas de Greene, Bitcoin alcanzó un grado de difusión masivo y se estimaba sus usuarios en más de 40 millones a fines de julio de 2019.

A pesar del gran número de usuarios y la difusión que ha alcanzado Bitcoin, al día de la fecha no se ha podido determinar con exactitud cuál es la "naturaleza jurídica" para las legislaciones del mundo. Posiblemente, la razón de que al día de la fecha no se sepa cuál es la naturaleza jurídica de Bitcoin es justamente su origen anárquico y su creador (o creadores) nunca pensaron en su clasificación dentro en una categoría legal existente.

[1] Descentrología y Bitcoin, *Rodolfo Andragnes*, artículo publicado en https://www.cripto247.com/opinion/descentrologia-y-bitcoin-182765, del 5 de julio de 2019.

Sin embargo, y a pesar de lo que puedan creer los creadores, miembros y usuarios de Bitcoin, resulta importante determinar su "naturaleza jurídica" para poder determinar para que podrá usarse, quienes la van a poder usar, (si va ser algo masivo o para solo un determinado grupo de usuarios, o inversores sofisticados), y en resumen, que normativa debería aplicársele y si su exigibilidad nace de la ley, o solo de la voluntad de las partes.

Con este trabajo pretendo demostrar que el Bitcoin es asimilable a una moneda extranjera de acuerdo a lo establecido por la ley argentina, y, por lo tanto, debería tener ese mismo tratamiento jurídico.

2. Criptomonedas.

Me resultó difícil encontrar una definición única, simple y clara de criptomoneda. Durante esta investigación encontré casi tantas definiciones como documentos analizados. Sin embargo, todas las definiciones contienen, en más o en menos, los mismos elementos, esto es: sistema, descentralizado, anónimo, virtual, y encriptado.

De todas las definiciones que encontré, la que construyo a continuación parece ser la más clara y completa: *"una criptomoneda es una moneda digital que utiliza técnicas de encriptado para regular la generación de unidades y verificar su transferencia y pagos realizados*[2]*, que opera sin depender de un banco central y/o gobierno determinado, no tiene una forma física o material, y se compone de algoritmos de software de código abierto (open source) que operan de punto a punto*[3] *(peer to peer), es decir sin ningún intermediario entre quien entrega la criptomoneda y quien la recibe".*

Es decir, una criptomoneda es un "activo digital", un algoritmo, un software inviolable e inmodificable que tiene un valor medible en dinero, generalmente administrado por comunidades de usuarios, y que en algunos casos sirve como medio de pago o cambio, para adquirir bienes o servicios.

La primera criptomoneda que empezó a operar fue el Bitcoin en 2009[4] y, desde entonces, han aparecido muchas otras con diferentes características y protocolos. Algunas de las más conocidas son Litecoin, Ethereum, Ripple, Dogecoin[5]. De auerdo a *Coinlore*, la cantidad de criptomonedas existentes suma más de 2500[6].

Las criptomonedas parten de un principio de libertad; buscan crear un modelo económico que pretende eliminar intermediarios en operaciones financieras. Es, para muchos de sus creadores, un deseo de justicia económica, o al menos esa fue la justificación de los pioneros de las divisas digitales[7]. Ello, sumado al hecho de que el software de las criptomonedas sea de código abierto y gratuito, explica el motivo por el cual hoy en día existen más de dos mil criptomonedas, porque es de fácil acceso, gratuito y se encuentra disponible en la web para su descarga.

Al igual que cualquier divisa, las criptomonedas son un sistema contable que representa un valor determinado. A diferencia de los bancos centrales o privados, en estas nuevas divisas no existe un sistema centralizado de información. Es decir, es un sistema contable que se encuentra en

---

[2] Geva, Benjamin, Tories LLP, *Is cryptocurrency money and why does it matter?,* Tories LLP. https://www.torys.com/insights/publications/2018/06/is-cryptocurrency-money-and-why-does-it-matter (último acceso 29 de julio de 2019).

[3] Punto a punto se refiere a los sistemas que trabajan como una organización colectiva, permitiendo que cada individuo interactúe directamente con otros. En el caso de Bitcoin, la red se construye de tal manera que cada usuario está transmitiendo transacciones de otros usuarios. Y algo muy importante, ningún banco se requiere como intermediario. Bitcoin, https://bitcoin.org/es/vocabulario#monedero (último acceso 27 de julio de 2019).

[4] McDonnell, Patrick, *What Is The Difference Between Bitcoin, Forex, and Gold*. NewsBTC. Archived from the original on 16 September 2015. Retrieved 15 September 2015, https://www.newsbtc.com/2015/09/09/what-is-the-difference-between-bitcoin-forex-gold-a-tripod-theory-revised/ (ultimo acceso 27 de Julio de 2019)

[5] https://es.wikipedia.org/wiki/Criptomoneda

[6] https://www.coinlore.com/all_coins (último acceso 29 de julio de 2019)

[7] Christopher Cannucciari, *Banking on Bitcoin*, 2016, citado por Talavera, Jorge en " *Las criptomonedas y su desafío legal*", Revista del Mundo del Abogado, Edición 226, páginas 26 a https://issuu.com/elmundodelabogado_/docs/226_2018_febrero (último acceso 29 de julio de 2019)

miles de servidores a lo largo y ancho del mundo, que se encargan de validar las transacciones realizadas[8].

Uno de los rasgos esenciales de las criptomonedas es que no requieren intermediarios, es decir, bancos privados que permitan las transacciones entre los usuarios. Existen diversas plataformas gratuitas en las que los propietarios de las divisas digitales pueden realizar las transacciones entre pares en cualquier parte del mundo, siendo validadas por los usuarios de dichas divisas[9]. De esa forma, el intercambio de las criptomonedas se realiza a través de internet entre los usuarios.

El uso de criptomonedas proporciona un servicio único: **transacciones financieras que no requieren que los gobiernos emitan divisas ni de bancos para procesar los pagos**[10] ni para darles respaldo.

Otras características de las transacciones con criptomonedas **han caracterizado su anonimato, velocidad, bajo costo de transacción, y la dificultad en el seguimiento de las transacciones**[11].

Aunque las criptomonedas no son creadas por bancos centrales (se crean por emisión directa de su creador o por medio de la actividad de minería, tal como lo veremos más adelante) y no existen del modo en el que conocemos las monedas tradicionales, en billete o papel o moneda, ya que son caracteres digitales; sin embargo, pueden ser intercambiadas con las monedas tradicionales, conservadas digitalmente y hasta impresas[12]. Al igual que otros patrones de valor se prevé, al menos en el caso de Bitcoin, que las criptomonedas tengan un límite[13].

En resumen, las criptomonedas son una "representación digital de valor" que no es emitida por una autoridad central y que no necesariamente lleva su valor atado al de una moneda fiduciaria. Son emitidas por personas naturales o jurídicas como un medio de intercambio y son transferidas, guardadas o transadas de manera electrónica[14].

Para empezar a entender que es Bitcoin y la relevancia funcional que tiene su clasificación, es necesario hablar de Blockchain, que – como veremos en el capítulo siguiente - no es otra cosa que es el sistema operativo de código abierto que (con matices) sustenta todas las criptomonedas.

[8] *Ibíd.*
[9] *Ibíd*.
[10] Mansur, Axlberto, Wolff , Jack, y Robles, Natalia, *Lo que todo abogado debe saber sobre el bitcoin* . https://elmundodelabogado.com/revista/opinion/item/lo-que-todo-abogado-debe-saber-sobre-el-bitcoin, último acceso (27 de Julio de 2019).
[11] Faliero, Johanna C., *Criptomonedas: La nueva frontera regulatoria del derecho informático*,, Ed. Ad-Hoc, 2018 pág. 28.
[12] *Ibíd.*
[13] Talavera, Jorge, *supra* nota 7.
[14] Rivas Herazo, Andrés, *La inclusión del bitcoin en el marco de la soberanía monetaria y la supervisión por riesgos en Colombia*, Revista de Derecho Privado, Nro. 55, junio 2016, citando al EBA/Op/2014/08, DOI: http://dx.doi.org/10.15425/redepriv.55.2016.03 (último acceso 27 de julio de 2019).

3. Blockchain.

3.1 Blockchain Explicado.

Si bien Bitcoin y Blockchain en esencia son dos cosas distintas, no se puede explicar la una sin la otra.

En sentido amplio, Blockchain es la base de lo que se llama *"Internet de Valor"*[15], la cual se compone de un universo de criptomonedas y/o "activos digitales" que permiten a sus titulares adquirir bienes y servicios, intercambiarlos por otros activos digitales, o simplemente guardarlos como una reserva de valor o para hacer una operación de especulación financiera.

Técnicamente hablando, Blockchain es una combinación de tecnologías existentes aplicadas de una forma combinada, esto es: internet (una red de personas con un registro común), claves criptográficas, y un protocolo que gobierna el incentivo a mantener el registro y validar las transacciones en forma segura (*mining*).

Dicho de manera más técnica, Blockchain es una tecnología que permite la realización confiable y segura de cualquier tipo de transacción entre dos o más personas sin la necesidad de intermediarios, a través de Internet. Es una articulación de tecnologías estructuradas en un sistema naturalmente encriptado, lo que proporciona a los usuarios involucrados protección de sus identidades y de los datos de sus transacciones[16].

A través de Blockchain, los miembros de la red crean un libro de contabilidad digital donde se anotan todas las transacciones que suceden en la misma, agrupadas en bloques que continuamente son enlazados linealmente entre sí, esto es: el primer bloque con el segundo, el segundo con el tercero, y así sucesivamente[17].

Resumidamente, Blockchain es una base de datos de contabilidad pública compartida en la que se basa toda la red Bitcoin y que permite la transferencia de valor dentro de una red de computadoras[18].

En decir, Blockchain no es nada más ni nada menos que un registro público de computadora mantenido por muchos participantes, que lo actualizan cada vez que se le incorpora un nuevo bloque a la cadena[19].

Todas las transacciones confirmadas se incluyen en la cadena de bloques. De esta manera, los monederos Bitcoin pueden calcular su saldo gastable y las nuevas transacciones pueden ser verificadas, asegurando que el cobro se está haciendo al que realiza el pago. La integridad y el orden cronológico de la cadena de bloques se hacen cumplir con criptografía[20].

---

[15] Milton, Herán K., *Criptomonedas, Blockchain y Derecho*, Revista Acta Jurídica Peruana, 2018, 1(2), pág. 133.
[16] https://www.criptonoticias.com/informacion/que-es-tecnologia-contabilidad-distribuida-blockchain/ (último acceso 29 de julio de 2019)
[17] *Ibíd.*
[18] OECD (2016), *OECD Science, Technology and Innovation Outlook 2016*, OECD Publishing, Paris. *http://dx.doi.org/10.1787/sti_in_outlook-2016-en* (último acceso 29 de julio de 2019)
[19] Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*,,, https://Bitcoin.org/Bitcoin.pdf (último acceso 29 de julio de 2019)
[20] https://bitcoin.org/es/como-funciona (último acceso 29 de julio de 2019)

Cada bloque contiene datos no sólo sobre la transacción que se anota en él, sino sobre otros datos que lo "vinculan" al bloque o eslabón anterior de la cadena[21]. No solo se indica el origen y destino de las operaciones, así como su monto, sino que además se consigna el momento exacto en que dicha operación tuvo lugar[22], es decir, se le aplica un sello de tiempo.

De esa manera, las cadenas de bloques o Blockchain se usan como un *"inventario de existencia electrónico no modificable"* de todo el sistema de transacciones que es mantenido por varios partícipes en una red de computadoras[23].

Las primeras y más conocidas blockchains, hasta el momento, son mantenidas por muchos nodos alrededor de todo el mundo y ninguno tiene realmente el poder para controlarla y aprobar o desaprobar transacciones según su propio criterio, (descentralización): **el poder no está centrado en una sola parte**, sino distribuido entre muchas partes que deben llegar a un acuerdo[24] para validar o rechazar transacciones.

Otra de las características del Blockchain es que almacena de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión[25].

Esta tecnología apunta a ser confiable en si misma (sin necesidad de un banco central o institución bancaria que la blinde de confianza) mediante la prevención del "doble gasto", y manteniendo un registro constante de la propiedad de las criptomonedas y de las transacciones[26]. Por eso, Blockchain es el sistema base para la mayoría de las criptomonedas[27].

En resumen, las ventajas que aporta la tecnología de las cadenas de bloques son principalmente dos: en primer lugar, permiten validar y detectar fácilmente la modificación o la corrupción de la información y, en segundo lugar, que la totalidad de la información se encuentra replicada en cada uno de los nodos de la red, todo lo cual permite prescindir de los llamados *terceros de confianza*. **Efectivamente, en las cadenas de bloques públicas cualquier usuario puede, no solo consultar la información almacenada en ella, sino que también puede verificar su integridad y autenticidad, en el caso de Bitcoin mediante la comprobación de firmas y el recalculo de *hashes*, y, en el caso de que alguna de estas comprobaciones falle, se puede acudir a la copia de la información que se almacene en cualquier otro nodo, hasta obtener alguna que supere todas las comprobaciones y pueda ser considerada correcta**[28].

---

[21] Manzur, Wolff y Robles, *supra* nota 10.
[22] Chomczyk, Andrés, *Status LegalActual de los Bitcoin en la Argentina*, elDial DC1D79, 9/10/2014.
[23] https://www.cnv.gov.ar/SitioWeb/Prensa/Post/1204/1204-alerta-al-publico-inversor-sobre-ofertas-iniciales-de-monedas-virtuales-o-tokens (último acceso 29 de julio de 2019).
[24] https://www.criptonoticias.com/informacion/que-es-tecnologia-contabilidad-distribuida-blockchain/ (último acceso 29 de julio de 2019).
[25] Manzur, Wolff y Robles, *supra* nota 10.
[26] OECD (2016), *OECD Science, Technology and Innovation Outlook 2016*, OECD Publishing, Paris. *http://dx.doi.org/10.1787/sti_in_outlook-2016-en*
[27] Boar, Andrei, *Descubriendo el Bitcoin, Como Funciona, Como Comprar, Invertir, Desinvertir*, Editorial Profit, p. 13.
[28] Como explica Luis Antonio Gallego Fernández, IOTA utiliza un entramado que se llama *direct acyclic graph*, cuyo funcionamiento se encuentra fuera del alcance del objeto de este trabajo. Gallego Fernández, Luis Antonio, *Cadenas de Bloques y registros de derechos*, citado por Legerén Molina, *Antonio en Retos Jurídicos que plantea la tecnología de la cadena de bloques*, Revista de Derecho Civil, Vol VI (1), http://nreg.es/ojs/index.php/RDC/article/view/356 (último acceso 26 de julio de 2019).

3.2 Tipos de Blockchain.

a. **Blockchain Publica o Privada**. Basándose en el acceso a los datos almacenados, podemos encontrar blockchains **públicas o privadas**. En la primera, no hay ninguna restricción para la lectura de datos ni la realización de las operaciones por parte de los usuarios; en cambio, en la segunda, tanto la lectura como las operaciones se limitan a participantes determinados[29], cuyo acceso se obtiene por invitación, y está pensada para transacciones de alto volumen donde no interesa que terceros puedan tener acceso a las mismas[30].

b. **Blockchain de Consorcio.** También se puede hablar de Blockchain en forma de consorcio, que difiere en el mecanismo de validación de los bloques. En este caso, una serie de nodos preseleccionados son los encargados de validar las transacciones, y no cualquiera, como en el caso de la Blockchain pública. Se considera que es un sistema parcialmente descentralizado[31].

c. **Con o sin Permiso.** Basándose en la capacidad para generar bloques, se divide en aquellas **sin permisos (*permisionless*) y con permisos (*permissioned*)**. En la primera no hay restricciones para poder realizar transacciones y crear nuevos bloques, de modo que se ofrecen monedas o activos digitales nativos de la red como recompensa a los usuarios que quieran mantener la red[32]. Las segundas son desarrolladas por entidades generalmente privadas (como sería Libra de Facebook en un principio), en muchos casos para uso interno, y los usuarios de estas necesitan permisos por parte de los administradores de la red para interactuar con el protocolo. Este es el tipo de blockchain que están probando los bancos: son centralizadas, es decir, controladas por la entidad y no por los usuarios[33].

3.3 Claves de Blockchain (Pública y Privada).

Cada usuario del Blockchain tiene una **clave pública** (como si fuera una dirección de correo electrónico, que opera como un medio de identificar a un usuario) y una **clave privada** (opera como medio para prestar consentimiento); ambas claves en forma conjunta hacen las veces de una firma digital que asegura el contenido de su activo digital.

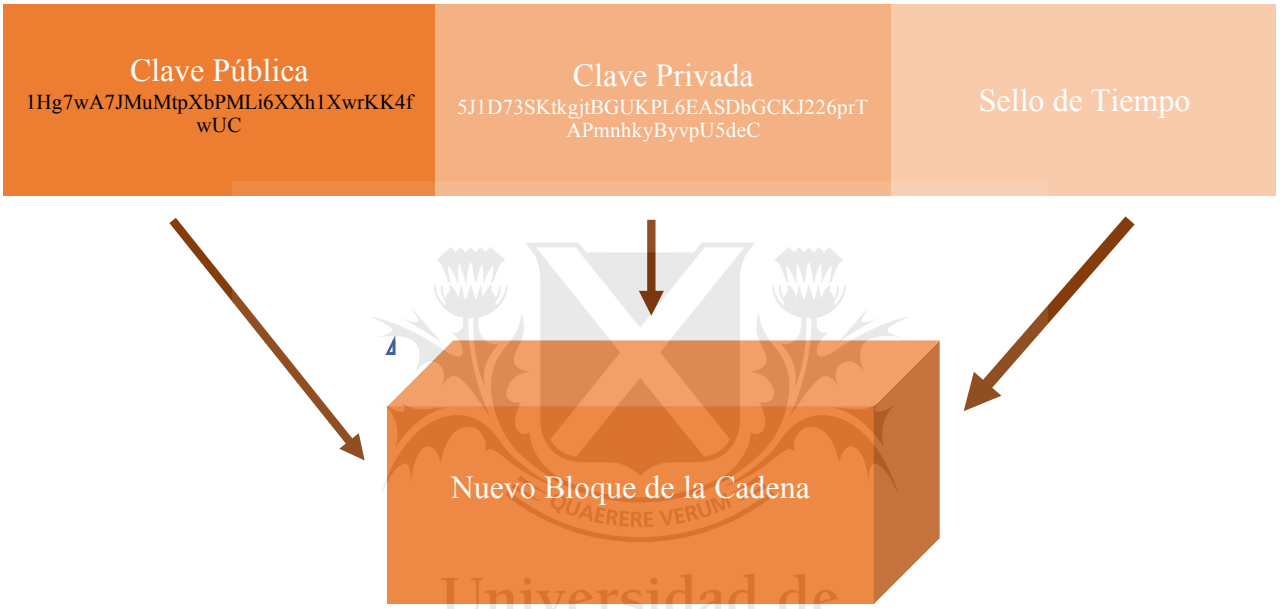
La **clave privada** es un código que funciona como una contraseña que permite al usuario firmar transacciones con bitcoins y transferirlos a otras direcciones. La utilización de las claves privadas permite probar la "titularidad" sobre los bitcoins. Cada clave pública, o dirección Bitcoin, deriva de una clave privada a través de un procedimiento matemático unidireccional[34].

En el caso del Bitcoin, **la posesión de un Bitcoin, equivale a conocer la clave privada que corresponde a la clave pública de esa dirección**. La clave privada, que es la contrapartida de

[29] *Supra* nota 16.
[30] Boar, *supra* nota 27..
[31] ,Boar, *supra* nota 27, p. 16.
[32] *Supra* nota 16.
[33] *Supra* nota 16.
[34] Ello significa que el procedimiento matemático utilizado para obtener una clave pública de una clave privada no puede ser utilizado a la inversa. En este sentido, es correcto afirmar que puede obtenerse una clave pública desde una clave privada, pero no puede obtenerse una clave privada desde una clave pública. Eraso Lomaquiz, Santiago E., *Las monedas virtuales en el Derecho argentino. Los Bitcoins*, AR/DOC/4070/2015.

la clave pública, da control sobre las transacciones de Bitcoins que se celebran desde una determinada dirección. Específicamente cualquier pago que implica una dirección de envío debe ser firmado con la clave privada correcta, para ser considerado válido[35].

Cada dirección Bitcoin está individualizada por una **identificación pública única**, que es un identificador alfanumérico que se corresponde a la clave pública de esa dirección[36]. La **clave pública** solo puede ser utilizada una vez, y esta queda inscrita en el registro público para el conocimiento de la comunidad Bitcoin[37].



Cuando los usuarios del Blockchain (o Bitcoin para el caso) quieren hacer una transferencia de ese activo digital, le envían al comprador su clave privada, que se asocia a la clave pública del comprador y se genera un sello de la hora en la que se llevó a cabo esa asociación. Las claves, la información transferida y el sello de tiempo forman un bloque. Varios bloques forman una cadena de transacciones, una atrás de la otra sin solución de continuidad.

3.4 Nodos.

Los nodos son ordenadores conectados que se encargan de almacenar y distribuir copias actualizadas de la Blockchain[38]. Es decir, los nodos son los usuarios y mineros[39] de Bitcoin.

Cada bloque se publica a los "nodos[40]" de la red, quienes operan el software Bitcoin.

---

[35] Faliero, *supra* nota 11, p. 73..
[36] *Ibíd*.
[37] Rivas Herazo, supra nota 14.
[38] Boar, *supra* nota 27,, p. 13.
[39] Explicaremos más adelante quienes son lo mineros y que función cumplen.
[40] En informática y en telecomunicación, de forma muy general, un nodo es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar. Ahora bien, dentro de la informática la palabra nodo puede referirse a conceptos diferentes según el ámbito en el que nos movamos: En redes de computadoras cada una de las máquinas es un nodo, y si la red es

Para que una transacción se confirme, los nodos deben validar los distintos componentes de la misma[41]. Cada nodo mantiene un registro y el historial de cada transacción en forma independiente, prestando conformidad o rechazando cada transacción (cada nuevo bloque de la cadena). Cuando la mayoría de los nodos valida una transacción, se le agrega un nuevo bloque a la cadena con el sello de tiempo correspondiente, de lo contrario se descarta. Ese sello registra el momento exacto en que un bitcoin se creó o envió de una persona a otra[42].

Una vez verificado todo ello, las transacciones se incorporan a los registros oficiales que se emiten con frecuencia y se denominan bloques. Como dije antes, el conjunto de bloques compone lo que se denomina Blockchain, es decir la cadena de bloques, registro, o libro mayor[43].

Al ser un registro público, pueden existir millones de copias y para modificarlo, tendrían que cambiarse los registros de todos los ordenadores que guardan una copia, cosa completamente inviable, al ser una base abierta y pública. El propio sistema operativo es su reaseguro, o al menos eso parecería ser el caso[44].

En Bitcoin existen distintos tipos de nodos o, dicho de otra forma, nodos que llevan a cabo diferentes funciones[45].

En primer lugar, **nodos que solo emiten transacciones** *(broadcast node):* Son aplicaciones monedero que únicamente permiten enviar o recibir monedas a través de la red Bitcoin. Las hay para todo tipo de dispositivos y también existen plataformas web que ofrecen este servicio[46].

Después están los nodos que propagan transacciones *(relay node):* Su función es, principalmente, recibir transacciones y retransmitirlas a otros nodos, aunque también comprueban que tienen el formato correcto, que las firmas criptográficas que contienen son válidas y también verifican, en la cadena de bloques, que el dinero que se transfiere existe en la cuenta de origen de la transacción[47].

Y, por último, **nodos que emiten, transmiten y minan transacciones** *(mining node):* Además de poder llevar a cabo las mismas tareas que los anteriores tipos, su principal cometido es validar y añadir las transacciones a la cadena de bloques[48].

Como contraprestación por esa tarea de verificación, los participantes de la cadena reciben una comisión en la criptomoneda soportada por esa cadena de bloques.

Internet, cada servidor constituye también un nodo. En estructuras de datos dinámicas un nodo es un registro que contiene un dato de interés y al menos un puntero para referenciar (apuntar) a otro nodo. Si la estructura tiene sólo un puntero, la única estructura que se puede construir con él es una lista, si el nodo tiene más de un puntero ya se pueden construir estructuras más complejas como árboles o grafos. https://es.wikipedia.org/wiki/Nodo_(inform%C3%A1tica) (último acceso 29 de julio de 2019)

[41] Cuando un usuario malintencionado intenta gastar sus bitcoins en dos destinatarios al mismo tiempo se denomina doble gasto. La minería de Bitcoin y la cadena de bloques permiten crear un consenso en la red acerca de cuál de las dos transacciones es considerada válida. https://bitcoin.org/es/vocabulario#firma (último acceso 29 de julio de 2019)

[42] Rivas Herazo, *supra* nota 14.

[43] Faliero, *supra* nota 11, p. 63.

[44] Barreira Delfino, *Acerca de la Criptomonedas*, Revista de Derecho Bancario y Financiero – Numero 43 – Noviembre de 2018, 28-11-2018 - IJ-DXLII-773.

[45] Gallego Fernández, supra nota 28.

[46] *Ibíd*.

[47] *Ibíd*.

[48] *Ibíd*.

El Blockchain genera una versión única del tracto sucesivo de cada moneda[49]. Como dije anteriormente, una vez agregado al Blockchain, el bloque no puede ser borrado ni alterado y nuevos bloques van siendo agregados constantemente después de cada bloque[50], y este es el rasgo esencial que le otorga a Blockchain su confiabilidad.

Como se puede ver, Blockchain constituye la piedra angular de Bitcoin y le otorga las notas características que hace a su esencia, como ser descentralización, criptografía, seguridad, y, anonimato, y determina, en última instancia la capacidad de crecimiento, desarrollo y circulación de los activos que componen la red.

[49] Manzur, Wolff y Robles, *supra* nota 10
[50] Manzur, Wolff y Robles, *supra* nota 10

4. Monederos y Billeteras.

Para comenzar a operar en la red Bitcoin (o cualquier criptomoneda) lo primero que debe hacerse es crear nuestro propio monedero en el que almacenar las monedas virtuales y que también nos permitirá realizar transacciones[51]. Precisamente, los bitcoins se pueden guardar en una computadora personal o en servicios suministrados por internet[52], que se llaman "monederos" o "billeteras". Los términos "billetera" y "monedero" se usan a modo de sinónimos y a los efectos de este trabajo significan lo mismo.

Esta "billetera" no es más que un "archivo" para transferir bitcoins[53], que funciona de modo similar a una cuenta de correo electrónico[54], por decirlo de una manera simplificada.

Existen numerosas páginas web que permiten crear estos monederos o bien se puede optar por la instalación en nuestro equipo de la correspondiente aplicación cliente. En este último caso también existe una gran variedad de programas entre los que elegir, para todo tipo de dispositivos (ordenadores personales, dispositivos móviles, etc.) o sistemas operativos e, incluso, es posible encontrar librerías para programar nuestro propio programa cliente[55].

Para lo que nos interesa, un monedero Bitcoin es aproximadamente equivalente a un monedero físico. El monedero realmente contiene su clave(s) privada que le permite gastar los bitcoins asignados a la clave en la cadena de bloques. Cada monedero Bitcoin puede mostrarle la cantidad de bitcoins que contiene y le permite pagar una cantidad específica a una persona específica, como un monedero de verdad[56].

Lo que se guarda en el monedero es una clave alfanumérica que nos permite acceder al sistema y escribir y consultar las transacciones en el libro mayor[57]. Es el equivalente a un CBU de una cuenta bancaria, y funciona de la misma manera, pero anónimo y secreto. Esa clave alfanumérica generalmente empieza con un número "1", y el destinatario de una transferencia de bitcoins deberá compartir esa clave a quien debe hacer la transferencia.

De esa forma, el Bitcoin en la forma de claves públicas se guarda en "billeteras" o monederos, en una computadora, a las cuales solo se puede acceder mediante una clave privada. Se puede incrementar la seguridad contra los "hackeos" mediante el uso de "depósitos fríos" off-line, y ese servicio lo proveen lo brokers de plataformas intermediarias[58]. Las billeteras conservadas con conexión de internet, o relacionadas (linked) a una aplicación de Smartphone, son muy similares al efectivo[59]. Las criptomonedas, pueden ser movidas de un depósito frío a billeteras móviles según sea necesario[60].

---

[51] Gallego Fernández, *supra* nota 28.
[52] Rivas Herazo, *supra* nota 14
[53] Farina, Sebastián, *Sobre el Bitcoin o moneda virtual,* 4/5/17 http://abogados.com.ar/sobre-el-bitcoin-o-moneda-virtual/19780 (último acceso 29 de julio de 2019).
[54] *Ibíd.*
[55] Gallego Fernández, *supra* nota 28.
[56] https://bitcoin.org/es/vocabulario#mineria (último acceso 29 de julio de 2019)
[57] Boar, *supra* nota 27, p. 31.
[58] Blundell-Wignall, A.,, *The Bitcoin Question: Currency versus Trust-less Transfer Technology*, *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jz2pwjd9t20-en. (último acceso 29 de julio de 2019).
[59] *Ibíd.*
[60] *Ibíd*.

Una vez instalados los monederos, los usuarios del Bitcoin descargan la totalidad de la cadena de bloques, convirtiéndose su dispositivo en un nodo más de la red Bitcoin, en el que se almacenará y, posteriormente, se actualizará una copia de la cadena de bloques[61].

Cabe destacar que en la actualidad la cadena de bloques completa ocupa, aproximadamente, unos 100 Gb. La primera vez que se ejecute el programa, el usuario tratará de descargar, construir índices y validar la totalidad de la cadena de bloques existente en ese momento lo que, debido a su volumen, podrá demorarse varios días dependiendo de la velocidad de nuestra conexión y de la capacidad de procesamiento de nuestro dispositivo. Una vez completado este proceso la copia de la cadena de bloques descargada se irá sincronizando automáticamente[62]. Igualmente, como veremos a continuación, a veces no será necesario descargar la totalidad de la cadena de bloques, ni constituirse en un nodo de la red.

En ese momento, se generará su primera dirección Bitcoin y se podrán crear más cuando lo necesite. A partir de ese instante, el usuario puede compartir a terceros para que estos le paguen o viceversa. De hecho, es similar a como funciona el correo electrónico, excepto que las direcciones Bitcoin solamente deberían ser usadas una única vez[63].

Los Bitcoin se guardan y son enviados a y desde "direcciones". Juntamente con cada dirección de bitcoin, la billetera guarda una clave privada para esa dirección, en esencia una clave usada por el tenedor del bitcoin para acceder a bitcoin con esas direcciones, y al historial de transacciones asociados a esa dirección[64].

Cabe destacar, que, si el usuario pierde la clave privada para acceder a la billetera, entonces perderá el bitcoin que se encontraba en esa billetera para siempre, como si hubiera extraviado un billete de 10 pesos que se le cayó del bolsillo.

Existen varios tipos de monederos, a saber:

a) **Escritorio:** consisten en programas informáticos, con mejor o peor interfaz gráfica, que nos permiten guardar bitcoins al almacenar las claves privadas en la computadora[65].

Existen dos tipos de clientes: i) *Full Client*, donde el usuario descarga la totalidad de la cadena de bloques, y se convierte en nodo del Bitcoin y de esa forma tiene toda la información actualizada de la red; y ii) *Light Weight Clients*, solamente guardan en la computadora la cadena de claves que les corresponde, pero no todo el nodo. Siempre se necesita de un tercero para poder acceder a la red Bitcoin en su totalidad. Algunos de los monederos de escritorio pueden ser hot que están conectados continuamente a la red y a los que podemos comprar con el efectivo que llevamos en la cartera en nuestro día a día, o cold que no está conectada a la red (puede ser en formato hardware o papel), nos puede servir como caja fuerte o reserva y no está conectada continuamente a la red ni se lleva encima en el móvil[66].

[61] Gallego Fernández, *supra* nota 28.
[62] Gallego Fernández, *supra* nota 28.
[63] https://bitcoin.org/es/como-funciona (último acceso 29 de julio de 2019)
[64] Conforme, Sec. Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2013 U.S. Dist. LEXIS 110018, at * 5 (E.D. Tex. Aug. 6, 2013) (holding that Bitcoin is a "currency or form of money").
[65] Boar, *supra* nota 27, p. 32.
[66] I*bíd*.

b) **Móvil o App:** Los monederos en formato móvil son aplicaciones que tenemos en nuestros dispositivos electrónicos que nos permiten tanto guardar nuestros bitcoins como realizar y controlar pagos a usuarios y comerciantes.

Estas aplicaciones son monederos SPV (*Simplified Payment Verification*). Son un intermedio entre los *full client* y los *lightweight client*. Descargan solo una parte de Blockchain, pero suficiente para poder comprobar en todo momento la validez de la transacción y hacer frente a posibles ataques externos. Esta aplicación nos permite realizar pagos a comercios[67].

c) **Web:** Las plataformas web son aquellas a las cuales podemos acceder desde el navegador de nuestra computadora. Funcionan de una manera parecida a las dos comentadas anteriormente. La gran desventaja de las plataformas web es que algunas usan sus propios servidores para guardar las claves de los bitcoins, lo que hace vulnerables a posibles ataques externos[68]. El caso más emblemático de vulnerabilidad fue el de Mt. Gox, que fue víctima de un ataque de hackers, y sufrió una pérdida de bitcoins equivalentes a cientos de millones de dólares.

d) **Hardware:** Los monederos físicos son totalmente diferentes a los descritos anteriormente. Son dispositivos que nos permiten guardar nuestras claves de bitcoin totalmente desconectados de la red en formato de disco duro externo o en USB. Para realizar cualquier transacción necesitamos conectar nuestro dispositivo a través del USB del ordenador o bien a través del cable OTG del móvil. Un software será el encargado de cargar, validar y permitir realizar las transacciones, pero nunca dispondrá en el sistema de nuestras claves, sino que estas se mantendrán en el dispositivo externo y solamente se compraban de forma las necesarias. Este sistema es inmune a los ataques de hackers, porque no está conectado a Internet y se pueden realizar copias de seguridad o bien añadir contraseñas de acceso para asegurarnos de que ningún otro usuario lo va a usar sin nuestro permiso. Por el contrario, si nos roban el dispositivo físico, perdemos los bitcoins[69].

e) **Monederos en Papel:** Los monederos de papel son otro método físico para guardar nuestros bitcoins, pero a la vez, pueden ser un método complementario a otro de los tipos anteriores para fortalecer la seguridad de nuestro capital. Lo más habitual es crear una *cold wallet* en formato papel que sea totalmente segura. Nuestra nueva cartera estará formada por dos claves escritas y facilitadas en código QR para su posterior lectura[70].

f) **Paper Wallet ATM:** Se trate de cajeros automáticos a disposición del público que te permiten comprar y vender bitcoins y, a la vez, generan los dos tipos de clave para tenerlos guardados en nuestro *cold wallet*[71].

[67] *Ibíd*.
[68] *Ibíd.*
[69] Boar, *supra* nota 27, p. 34.
[70] Boar, *supra* nota 27, p. 35.
[71] Boar, *supra* nota 27, p. 36.

5. Bitcoins.

Bitcoin fue la primera criptomoneda que se creó, y, por lo tanto, la precursora de todas las criptomonedas que existen hoy.

Esencialmente, los Bitcoins son unidades de cuenta compuestos de secuencias alfanuméricas únicas que constituyen unidades de moneda y que tienen valor sólo porque usuarios individuales están dispuestos a pagar por ellos[72] o aceptarlos como medio de pago, o de cambio y que se encuentran guardados en una red.

El sistema Bitcoin fue implementado por una persona identificada (o grupo de personas identificadas) con el seudónimo Satoshi Nakamoto[73], mediante la publicación de sus reglas de funcionamiento en un trabajo intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System"[74] a fines de 2008, y con la emisión del software correspondiente, a modo "código abierto" a comienzos del 2009. El Sistema Bitcoin constituye un sistema electrónico que tiene por objeto permitir a sus usuarios realizar pagos a través de Internet. Dicha circunstancia lo asimila en buena medida a los sistemas de tarjeta de crédito, y a los sistemas de dinero electrónico[75]. De todas formas, el Sistema Bitcoin tiene varias particularidades que lo distinguen terminantemente del resto de los sistemas mencionados[76].

Es decir, el esquema del Bitcoin conlleva los atributos de un sistema de pago, en el cual se ve facilitada la transferencia de valor entre las partes[77]. Como moneda, no tiene curso legal, y muchos economistas cuestionan su cumplimiento de los atributos estándar que tienen las monedas tradicionales[78], como ser reserva de valor, unidad de cuenta y medio de cambio.

Esta criptomoneda es una versión puramente electrónica de efectivo que utiliza la criptografía para controlar su creación y sus transacciones, en lugar de que lo haga un ente público centralizado, pues, a diferencia del dinero fiduciario, su valor no viene dado por una autoridad monetaria que además lo emita. Esta moneda digital puede usarse para el pago de bienes físicos y servicios en el mundo real, como pasa con las monedas físicas tradicionales[79]. En esencia es

---

[72] Cámara Federal de Apelaciones de San Martín, Sala I, "Rodríguez Córdova, Max y otros s/legajo de apelación", 27/11/2017, https://www.google.com/search?q=Rodr%C3%ADguez+C%C3%B3rdova%2C+Max+y+otros+s%2Flegajo+de+apelaci%C3%B3n&rlz=1C5CHFA_enAR775AR775&oq=Rodr%C3%ADguez+C%C3%B3rdova%2C+Max+y+otros+s%2Flegajo+de+apelaci%C3%B3n&aqs=chrome..69i57.144j0j8&sourceid=chrome&ie=UTF-8 (accedido el 29.07.2019)

[73] Se desconoce la identidad de Satoshi Nakamoto, ya que habría abandonado el proyecto a finales de 2010 sin revelar mucho sobre su persona. Se aclara no obstante que, dado que el protocolo bitcoin y su software se han publicado abiertamente, cualquier programador puede revisarlo o crear su propia versión, todo lo cual significa que el Sistema Bitcoin notiene propietarios, ni es relevante la identidad de su creador. Ver https://bitcoin.org/es/faq (accedido el 01.10.15).

[74] Publicación disponible en https://bitcoin.org/es/bitcoin-documento (accedido el 01.10.15). Allí se reconoce como antecedente de la idea a una publicación anterior, de 1998, efectuada por un criptógrafo llamado Wei Dai, e identificada como "b-money", la cual se encuentra disponible en http://weidai.com/bmoney.txt (accedido el 01.10.15).

[75] En la Unión Europea, ámbito en el cual el dinero electrónico ha sido más analizado, es regulado actualmente por laDirectiva 2009/110/CE, cuyo artículo 2° lo define como "todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico". Para una mayor descripción de este sistema, ver Mora, Santiago J., "El Dinero Electrónico en el DerechoArgentino".Mora, Santiago J.,*Monedas virtuales*. Una primera aproximación al Bitcoin, LA LEY 31/12/2015, 31/12/2015, 1, AR/DOC/3860/2015.

[76]Mora, Santiago J.,*Monedas virtuales. Una primera aproximación al Bitcoin*,LA LEY 31/12/2015, 31/12/2015, 1, AR/DOC/3860/2015.

[77] Faliero,*supra* nota 11. p. 65..

[78] *Ibíd*..

[79] León A. Martínez, *¿Qué es el bitcoin y como funciona?,* El Economista, 17/10/17.

un *token*[80], sin referencia a ninguna materia prima subyacente o moneda soberana, y no es un pasivo en un balance[81].

Su primera particularidad consiste en que utiliza unidades de valor, llamadas "bitcoins", que no están expresadas en una moneda fiduciaria convencional, ni representan bienes o acciones que alguien deba entregar o cumplir. No obstante, ello, los bitcoins pueden ser canjeados por bienes y servicios, o por monedas de curso legal, a un valor que varía constantemente según las reglas de la oferta y demanda[82].

Cada bitcoin se divide en cien millones de partes que no reciben el nombre de céntimos ni de peniques sino de *satoshis* (en honor al creador del sistema), siendo la transferencia mínima, que se puede realizar, de: 546 *satoshis* o 0,00000546 BTC[83].

El Bitcoin forma parte de las divisas virtuales denominadas «de flujo bidireccional», que los usuarios pueden comprar y vender con arreglo al tipo de cambio. Por lo que respecta a su uso en el mundo real, estas divisas virtuales son análogas a las demás divisas intercambiables, y permiten adquirir bienes y servicios tanto reales como virtuales. Las divisas virtuales se distinguen del dinero electrónico, tal como lo define la Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267, p. 7), en la medida en que, a diferencia de este dinero, en el caso de las divisas virtuales los fondos no se expresan en la unidad de cuenta tradicional, por ejemplo, en euros, sino en una unidad de cuenta virtual, como Bitcoin[84].

De hecho, el bitcoin se utiliza, con carácter principal, para los pagos entre particulares en Internet y en determinadas tiendas en línea que aceptan esta divisa (algunos comercios a la calle ya aceptan Bitcoin también como medio de pago[85]).

La segunda particularidad de este sistema, y tal como lo explicamos en la sección 3 más arriba es que para obtener y transferir la titularidad de los bitcoins se utiliza llamado "criptografía[86] asimétrica de clave pública". En este esquema, cada persona que quiere constituirse como titular

[80] Los tokens son una unidad de valor, emitida por una entidad privada, que tiene el valor que se le otorga dentro de una comunidad. Muchos de los pagos que realizamos a diario con soluciones digitales, están tokenizados. Las aplicaciones móviles para teléfonos digitales, los códigos de algunas páginas webs, que generan o validan claves criptográficas para proteger operaciones, no son más que una aplicación real de los Tokens.

[81] Johanna C. Faliero, Criptomonedas: La nueva frontera regulatoria del derecho informático. p. 65, Ed. Ad-Hoc.

[82] En virtud de lo manifestado, se dice que los bitcoin no tienen un valor intrínseco, aunque —conforme se verá más adelante— para su creación deba incurrirse en un costo equivalente al valor del tiempo de la persona que lo obtuvo a través del "mining", el valor del hardware que necesitó para ello, y la energía consumida. Ver, Kaplanov, Nikolei M., "Nerdy money:Bitcoin, the private digital currency, and the case against its regulation", 31 de marzo de 2012, disponible enhttp://ssrn.com/abstract=2115203 (accedido el 01.10.15).

[83] Gallego Fernández, *supra* nota 28.

[84] SENTENCIA Nº C-264/14 DE TRIBUNAL DE JUSTICIA, 22 DE OCTUBRE DE 2015, Högsta förvaltningsdomstolen (Tribunal Supremo de lo contencioso-administrativo, Suecia)

[85] https://www.lanacion.com.ar/economia/mas-comercios-aceptan-bitcoins-nid2244259

[86] La criptografía es la rama de las matemáticas que nos permite crear pruebas matemáticas que proporcionan altos niveles de seguridad. El comercio en línea y los bancos ya utilizan criptografía. En el caso de Bitcoin, la criptografía se utiliza para hacer imposible que alguien pueda gastar los fondos del monedero de otro usuario o que se pueda corromper la cadena de bloques. También se utilizada para encriptar un monedero, de manera que no se pueda utilizar sin una contraseña.

de bitcoins debe generar dos claves matemáticamente relacionadas, una de las cuales se hace pública y otra se mantiene en privado[87].

Otra particularidad de este sistema, y tal como lo explicamos más arriba, respecto de las criptomonedas en general, es que no existe una administración o autoridad central. Es decir, es descentralizado. Esta divisa virtual no tiene un emisor único y se crea, en cambio, directamente en el seno de una red mediante un algoritmo especial. El sistema de la divisa virtual Bitcoin permite que los usuarios que dispongan de direcciones Bitcoin posean y transfieran anónimamente dentro de la red Bitcoin en cantidades variables[88].

De esa manera, los bitcoins y sus transferencias se registran en una base de datos de carácter pública (por cuanto todos tienen acceso a ella) que se almacena en una red diseminada de puntos o "nodos", cada uno de los cuales está compuesto de hardware y software aportados por distintas personas que voluntariamente, pero a cambio de una contraprestación, participan en el sistema. Cada uno de estos nodos contiene una réplica de la base de datos en cuestión y procesa todas las transferencias de titularidad que van ocurriendo. De esta manera, cada vez que una persona ordena la transferencia de titularidad de un bitcoin, ello se informa a toda la red, para que todos los nodos analicen su legitimidad, y —de corresponder— la incorporen a su versión de la base de datos[89].

Como el Sistema Bitcoin es un sistema descentralizado con las características indicadas más arriba, ha surgido también una serie de intermediarios y negocios accesorios, cuyo conocimiento —al menos de los más relevantes— es fundamental para la mejor comprensión del esquema. En primer lugar, se habla de los "proveedores de billeteras", que ofrecen un servicio a los titulares de bitcoins consistente en el almacenamiento de las claves criptográficas necesarias para transferirlos[90].

Finalmente, los Bitcoin son anónimos o seudónimos, tal como explicaremos más adelante, porque los usuarios son identificados solamente por la clave pública y la prueba de su titularidad es la clave privada que ostentan en su billetera. En teoría no hace falta proveer datos personales ni ninguna otra forma de identificación para ser dueño de un bitcoin.

El escenario descripto anteriormente constituye un resumen general del sistema Bitcoin, que sirve como introducción al mismo, y a sus distintos aspectos tipificantes y/o rasgos distintivos, que voy a desarrollar en particular en los capítulos siguientes.

https://bitcoin.org/es/vocabulario#confirmacion

[87] Mora, *supra* nota 76.

[88] *Supra* nota 84.

[89] Mora, *supra* nota 76.

[90] *Ibíd*.

6. Anónima o Seudónima.

Como dije antes, una de las características importantes del sistema Bitcoin es que sus usuarios y tenedores de bitcoins pueden permanecer y operar en forma anónima. En realidad, sería más adecuado decir que Bitcoin es un sistema seudónimo porque la gente que lo opera lo hace a través de información que carga a la red, la cual puede ser genuina o ficticia.

Cuando se instala una aplicación cliente no es necesario introducir ningún dato personal y si, en vez de utilizar alguna de estas aplicaciones se opta por usar alguna de las webs que permiten operar en dicha red, a lo sumo se deberá especificar una dirección de correo electrónico que, no obstante, puede ser una dirección creada al efecto en alguno de los muchos servicios de correo gratuitos en los que tampoco es necesario introducir nuestros datos personales reales[91].

Es decir, se pueden crear con facilidad identidades totalmente ficticias para operar en el sistema Bitcoin, todo lo cual proporciona un considerable grado de anonimato a los usuarios de la red. Se puede decir, que la dirección de Bitcoin, en ese aspecto se asemeja a tener una cuenta de correo electrónico la cual puede ser creada utilizando cualquier tipo de información, no necesariamente veraz o relacionada a la real identidad de su titular.

De esa forma, los Bitcoins residen en lo que se conoce como direcciones Bitcoin, la propiedad de una determinada cantidad de Bitcoins se reduce a la capacidad de enviar pagos en la red desde la dirección Bitcoin con la que se asocia lo que, se controla a través de firmas digitales[92], como veremos a continuación.

Todas las transacciones Bitcoin se almacenan públicamente y permanentemente en la red, lo que significa que cualquiera puede ver los fondos y transacciones de una dirección Bitcoin. No obstante, como dije antes, la identidad del usuario que posee la dirección no es conocida a no ser que sea develada durante una compra o por otras circunstancias. Esta es una de las razones por la que las direcciones Bitcoin deberían ser utilizadas sólo una vez[93].

Precisamente, la identificación del usuario es su dirección Bitcoin, y no su nombre e identidad[94]. De esa forma, las "cuentas" Bitcoin no contienen en ellas el nombre de las personas y no necesariamente corresponden específicamente a individuos. **Cada saldo simplemente se asocia con el par de claves pública-privada generadas al azar y el dinero "pertenece" a cualquiera que pueda firmar con la clave privada cualquier transacción de esos fondos.** Las transacciones firmadas usando estas claves no incluyen los nombres de las personas que las realizan[95]. Quien posea la clave privada de un saldo, será el titular del bitcoin.

Cada persona puede tener muchas direcciones, cada una con su propio saldo, y esto puede hacer más difícil identificar qué persona tiene tal cantidad de dinero[96]. Incluso, los usuarios pueden utilizar una diferente para cada transacción, oscureciendo significativamente la traza de los activos ilícitos. También, los usuarios pueden emplear diversas herramientas y servicios, tales

[91] Gallego Fernández, *supra* nota 28.
[92] Faliero, *supra* nota 11, p. 73.
[93] https://bitcoin.org/es/debes-saber
[94] Faliero, *supra* nota 11, p. 76.
[95] https://www.bitcoinargentina.org/faqs/.
[96] *Ibíd.*

como el mezclador o tumbador, con el propósito de disfrazar la fuente de una transacción de Bitcoin y facilitar incluso más el anonimato[97].

En términos de funcionamiento, más allá de la utilización de criptografía, Blockchain en sí misma y la información que contiene, no se encuentran encriptadas. Para proteger la identidad de los usuarios de la red, su información IP nunca se almacena, y las claves de cifrado se utilizan en lugar de la información personal[98].

Como se puede ver, no es posible, *a priori,* conocer la identidad de las personas que participan en los registros[99] de Bitcoin. Esta queda encriptada y se esconde detrás de una serie alfanumérica: las transacciones pasan a ser seudónimas. Podemos conocer las transacciones, pero no la identidad de quienes la realizan. Una vez que se inscriben esas transacciones, no se pueden eliminar ni modificar. Solamente pueden ser leídas[100].

Sin embargo, Bitcoin no es enteramente anónima, porque – según sostienen algunos – sería posible rastrear la gran mayoría de las operaciones si se tienen elevados conocimientos de la red[101].

Tal como mencioné, en la red Bitcoin las transacciones son anónimas porque desconocemos la identidad del emisor y del receptor[102], pero el sistema no permite esconder las operaciones realizadas[103], por lo tanto, se podría averiguar la identidad de un usuario estudiando y rastreando las transacciones realizadas y publicadas en la red Bitcoin.

Precisamente a través del seguimiento del flujo de Bitcoins, la investigación y la utilización de información externa encontrada, se pueden develar las identidades anónimas de los usuarios[104]. Aunque la identificación de los usuarios no es una tarea fácil, se podría lograr a también a través de las siguientes medidas: a) las plataformas de intercambio pueden compartir la información de sus usuarios (como veremos más abajo), b) hay determinadas clases de monederos que permiten conocer el IP de su titular, y c) las transacciones que se encuentran registradas en Blockchain, son rastreables hasta su origen y de esa forma se puede saber quién se encuentra enviando y recibiendo bitcoins.

Más aún, los mineros de Bitcoin han comenzado un proceso de cartelización, acrecentando el porcentaje de control que poseen de la red.

Si estos carteles de mineros controlan la mayor parte del *hash rate*, entonces tendrían que brindar garantías de transparencia, y que no van a manipular las reglas del sistema, y para ello, lo básico es saber quiénes son, donde operan y en qué jurisdicción se encuentran para saber a qué reglas se encuentran sujetos y de que capacidad persecutoria tendrían los usuarios en caso de ser defraudados. A partir de ese momento, esos mineros se van a encontrar bajo la lupa de entidades

[97] Mezclador -o tumbador- es un anonymiser que oscurece la cadena de transacciones en las blockchain mediante la vinculación de todas las transacciones en la misma dirección BTC, y que las envía por medio de una serie de transacciones no reales complejas, semi-al azar, haciendo casi imposible vincular las direcciones con una determinada operación. Caso Bobinas Blancas, Por María Belén Linares,
[98] Faliero, *supra* nota 11, p. 76.
[99] Boar, *supra* nota 27, p. 13.
[100] *Ibíd*.
[101] *Ibíd*.
[102] Boar, *supra* nota 27 p. 92.
[103] Ibíd.
[104] Faliero, *supra* nota 11, pág. 76.

gubernamentales de la jurisdicción en la que operen y seguramente tengan que compartir información sobre sus usuarios, con dichas entidades, como hacen las entidades financieras para poder seguir operando.

De la misma manera, a los fines de comprar otras monedas fiduciarias con Bitcoins o intercambiarlas por otras criptomonedas ("*exchanges*"), los usuarios muchas veces tienen que recurrir a plataformas de intercambio que tiene sus sedes en Estados Unidos y/o Europa.

Los "*exchanges*", ofrecen servicios de intercambio a los usuarios, fijando tasas de cambio contra distintas monedas por las cuales transferirán o adquirirán bitcoins[105]. Estos "exchanges" sirven para canjear bitcoins por otras criptomonedas como Litecoin o para canjearlas por monedas fiduciarias como dólares o euros. Esas plataformas de cambio se encuentran sujetas al cumplimiento de normativa anti lavado del país donde operan, y, por lo tanto, deben registrar a sus usuarios y obtener sus datos personales para conocer el origen de los fondos y que estos puedan transaccionar.

De esa forma, este tipo de plataformas de cambio (exchanges), constituyen otra atenuación a la característica de anonimato del Bitcoin, y demuestra que en la práctica los usuarios del Bitcoin quienes no gozan de un completo anonimato.

En resumen, si bien Bitcoin comenzó como un sistema anónimo de intercambio de valores, con el correr del tiempo, esa característica se fue perdiendo y diluyendo, para pasar a ser seudónima, y a medida que obtenga mayor difusión y uso, llegará un momento en el que Bitcoin deje de ser –en los hechos- completamente anónimo.

[105]Mora, *supra* nota 76.

7. Criptografía y el Bitcoin.

La criptografía es el arte de escribir con clave secreta o de un modo enigmático[106]. Es la rama de las matemáticas que nos permite crear **pruebas matemáticas que proporcionan altos niveles de seguridad**[107], es decir, que nos permite transcribir con una clave aquello que en principio es público para mejorar su confidencialidad[108].

En el caso de Bitcoin, la criptografía se utiliza para hacer imposible que alguien pueda gastar los fondos del monedero de otro usuario o que se pueda corromper la cadena de bloques. También se utilizada para encriptar un monedero, de manera que no se pueda utilizar sin una contraseña[109].

Puntualmente, el Bitcoin utiliza técnicas criptográficas para verificar las transacciones, el procesamiento de pagos y el control del suministro de Bitcoins[110], y para dotar de seguridad al sistema.

Precisamente, para realizar transacciones no hay más que enviar un mensaje a la red Bitcoin utilizando para ello la aplicación cliente e indicando, al menos, el remitente, el destinatario y la cantidad de bitcoins a transferir. Para asegurar que el mensaje es auténtico e íntegro, es decir, para acreditar la identidad del remitente y que el mensaje enviado no ha sido modificado, se utilizan técnicas de firma electrónica mediante criptografía asimétrica o criptografía de dos claves[111].

De esa manera, el funcionamiento del Bitcoin se basa en dos esquemas criptográficos: la *firma digital* y la función de *hash*; el primero permite el intercambio entre las partes de una transacción, y el segundo, se utiliza para reforzar los registros de las transacciones en la Blockchain[112].

Las firmas digitales son un medio para autenticar mensajes electrónicos, entre un emisor y un receptor, de una manera segura: su autenticidad (el destinatario puede verificar que el mensaje provenía del remitente), no repudio (el emisor no puede negar el envío del mensaje), e integridad (que el mensaje no ha sido adulterado)[113].

Firmar digitalmente un documento implica realizar una operación matemática sobre él a través de la utilización de un programa informático, por lo que la firma digital dista cualitativamente de la firma ológrafa, permitiendo valores y atributos que llegan a ser superiores a esta segunda en términos de seguridad e inviolabilidad[114].

Para ello, las aplicaciones cliente generan pares de claves criptográficas compuestos, cada uno de ellos, **por una clave pública y una clave privada**, las cuales no son independientes, sino que se

---

[106] http://dle.rae.es/?id=BHcfHjo (accedido el 29.07.19)
[107] https://bitcoin.org/es/vocabulario (accedido el 29.07.19)
[108] Boar, supra nota 27.
[109] https://bitcoin.org/es/vocabulario (accedido el 29.07.19)
[110] Faliero, supra nota 11, p. 68,
[111] Gallego Fernández, supra nota 28,.
[112] Faliero, supra nota 11 p. 69, Ed. Ad-Hoc, citando a Crosby, Michael. Nachiappan, Pattanayak, Pradhan; Verma; Sanjeev, y Kalyanaraman, Vigesh: *Blockchain Technology. Beyond Bitcoin*, Sutardja Center for Entrepreneurship / Technological Technical Report, 16.10.2015.
[113] Faliero,, supra nota 11p. 69, Ed. Ad-Hoc. La negrita me pertence.
[114] Faliero, supra nota 11p. 71, Ed. Ad-Hoc.

encuentran ligadas matemáticamente. Las claves públicas son cadenas alfanuméricas de 26 a 35 caracteres que comienzan por un '1' o un '3', un ejemplo de clave pública sería: 1Hg7wA7JMuMtpXbPMLi6XXh1XwrKK4fwUC, y la clave privada que le correspondería sería: 5J1D73SKtkgjtBGUKPL6EASDbGCKJ226prTAPmnhkyByvpU5deC[115].

El protocolo que utiliza el Bitcoin emplea el esquema anterior para firmar los mensajes de transacción. En particular, las transacciones se firman con la clave privada y luego se transmiten a la red Bitcoin; todos los miembros del sistema pueden verificar que llegó una transacción del propietario de la clave pública al tomar el mensaje, la firma y la clave pública, y corriendo el algoritmo de verificación[116].

El proceso de firma electrónica en este tipo de sistemas, se lleva a cabo del siguiente modo: a) En primer lugar, al mensaje se le aplica una función *hash* criptográfica con el fin de obtener su huella digital o código *hash*. Por tanto, las funciones *hash* devuelven, para el elemento que se les haya pasado como entrada (texto, imágenes, video, etc.), un resumen cifrado consistente en una cadena alfanumérica de longitud fija, b) Existen numerosas funciones o algoritmos de *hash*, como las familias MD (MD2, MD4, MD5), SHA (SHA-0, SHA-1, SHA-2, SHA-3), RIPEMD (RIPE-MD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320), etc. [117]

En segundo lugar, a la huella digital del mensaje, así obtenida, se le aplica una segunda función criptográfica para firmarla con la clave privada del usuario remitente. El resultado obtenido es la firma electrónica del mensaje[118].

Esta segunda función criptográfica, por tanto, tiene dos entradas: la huella digital del mensaje y la clave privada del usuario y se caracteriza porque su resultado solo puede descifrarse (y así obtener nuevamente la huella digital del mensaje enviado) mediante la clave pública de dicho usuario[119].

A continuación, se encapsula en un solo fichero tanto el mensaje original, como la clave pública del remitente y la firma electrónica del mensaje y se envía al destinatario[120].

Por último, el destinatario, al recibir dicho fichero encapsulado usará la clave pública del remitente para descifrar la firma electrónica, incluida en el fichero, y obtener la huella digital o código *hash* del mensaje que calculó el remitente[121].

El destinatario también calculará la huella digital del mensaje original, aplicándole el mismo algoritmo que el remitente, y si esta última huella coincide con la obtenida al descifrar la firma electrónica, se habrá garantizado que el mensaje no ha sido modificado y que ha sido emitido por el titular de la clave privada que se ha utilizado para firmar electrónicamente el mensaje[122].

Bien utilizados, los métodos criptográficos utilizados garantizan que cada pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas tengan una misma pareja de claves. Por otra parte, una misma persona puede tener

[115] Gallego Fernández, *supra* nota 28.
[116] Faliero, *supra* nota 11 p. 76, Ed. Ad-Hoc.
[117] Gallego Fernández, *supra* nota 28.
[118] *Ibíd.*
[119] *Ibíd.*
[120] *Ibíd.*
[121] *Ibíd.*
[122] *Ibíd.*

más de una pareja de claves, lo que puede ser útil, por ejemplo, para separar y distinguir entre monedas virtuales con orígenes y propósitos distintos[123].

Hash. El *hash* es como una etiqueta que se le agrega a cada bloque. De esa forma, cuando se intenta minar un bloque se genera un hash (una cadena de dígitos) que podría ser la solución al siguiente bloque de la cadena de bloques[124]. Es decir, números aleatorios y letras derivadas de la clave pública mediante la aplicación de una función de *hash* (un proceso que toma un block arbitrario de información y devuelve un hilo de bits de un tamaño fijo)[125].

El sistema Bitcoin hace un amplio uso de este tipo de algoritmos, no solo para la firma de mensajes sino también para otro tipo de tareas como la generación de direcciones, la minería de bitcoins, etc.; siendo uno de los más utilizados el algoritmo SHA-256, perteneciente a la familia SHA-2[126]. El algoritmo SHA-256, es una especie de *Secure Hash Algorithm* (SHA-2), diseñado por la Agencia de Seguridad Nacional de Estados Unidos de Norteamerica (*NSA – National Security Agency*) y publicado por el Instituto Nacional de Estándares y Tecnología (*National Institute of Stanards and Techonology*) [127].

Cada bloque de Bitcoin posee un hash en su cabecera de tipo SHA-256, que implica que el mismo es de 256 bits, 64 caracteres (utiliza una representación hexadecimal), y debe comenzar con 18 ceros. Cada 2016 bloques la dificultad varia[128].

Los eslabones de la cadena se enlazan entre sí de una manera que hace prácticamente imposible su manipulación o alteración por un agente mal intencionado a través de un algoritmo criptográfico conocido como *hash* (funciones matemáticas que transforman esencialmente los datos en el *hash* en una salida única de longitud fija, creando una "huella única" digital de los datos subyacentes) que ordena cada bloque en Blockchain con referencia al *hash* del bloque anterior. Estos *hashes* no son fáciles de manipular, lo que asegura toda la cadena de bloques a medida que crece[129].

La función *hash* es una operación también matemática e informática, que se efectúa sobre un documento, de la cual se obtiene – un resumen numérico – que se encripta y relaciona con el documento, permitiendo verificar respectivamente al desencriptarla. Si es auténtico – es decir, si pertenece a quien dice pertenecer-, si es íntegro – es decir, que no haya sido alterado su contenido, y si pertenece a su autor- respondiendo a la garantía de no repudio de su contenido[130].

Precisamente, el *hash* del mensaje revela poco o nada sobre el mensaje, lo que es fundamental para las funciones hash y en lo particular se traduce en las siguientes propiedades: dada una

---

[123] *Ibíd.*
[124] https://steemit.com/mineria/@jahlexistafari/thb-que-es-la-mineria-de-fusion-o-merged-mining-thb (accedido el 29.07.19)
[125] Blundell-Wignall, A. (2014), "The Bitcoin Question: Currency versus Trust-less Transfer Technology", *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jz2pwjd9t20-en.
[126] Gallego Fernandez, *supra* nota 28.
[127] Faliero, *supra* nota 11, p. 72, Ed. Ad-Hoc, citando a: a) "Descriptions of SHA 256, SHA 384, and SHA-512" disponible en http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf, y b) Malortha, Yogesh: "Bitcoin Protocol: Modelo of Cryptographic Proof Based Global Crypto-Currency & Electronico Payment Systems", Griffis Cyberspace, Global Risk Management Network, EEUU.
[128] ¿Qué es el Hashrate o Hashpower en las criptomonedas? Publicado en, https://criptotario.com/que-es-el-hashrate-en-las-criptomonedas (accedido el 29.07.19)
[129] Manzur, Wolff y Robles, *supra* nota 10.
[130] Faliero, *supra* nota 11. p. 72. p. 72.

función *hash* es difícil encontrar un mensaje que dé el mismo hash por resultado; dado un mensaje, su variación implica que el hash varíe; y resulta muy dificultoso (aunque bien no imposible), encontrar dos mensajes diversos que de por resultado el mismo hash. Otra propiedad útil en términos de seguridad que provee la función hash es que, incluso, muy pequeños cambios en el mensaje son propensos a cambiar el hash significativamente[131].

Las funciones hash criptográficas tienen varias características importantes: a) Su cálculo es muy sencillo, en términos de tiempo y de capacidad de cálculo necesaria, pero, inversamente, la obtención de una entrada a partir de su código hash es muy difícil; b) Entradas iguales siempre producen códigos hash iguales y entradas diferentes siempre producen códigos *hash* diferentes, por lo que un determinado código hash identificará inequívocamente la entrada de la que proviene; y, c) por último, es imposible predecir cualquier código hash a partir de otros previamente capturados. En relación con ello, en los ejemplos anteriores se puede comprobar la gran disparidad que existe entre los distintos resultados por el simple hecho de quitar un punto final[132].

Cada registro es único, replicado y autentificado en una red informática y sincronizado para que todas las computadoras en las que está almacenado el Blockchain reflejen la misma información a medida que ésta se actualiza[133].

La tasa de hash o *"hash rate"* es **la unidad de medida de la potencia de procesamiento de la red Bitcoin**[134], y es lo que permite determinar la capacidad que tiene la red para procesar transacciones, o lo que es lo mismo, cuanto tardan los mineros en validar una transacción y en agregar un nuevo bloque a la cadena. La cantidad de intentos que puede realizar la red completa (o un minero) en un segundo se llama *hash rate* o *hash power*[135].

Cuanto más crece la red Bitcoin, y más mineros se incorporan el *hash rate* disminuye y hace falta más potencia y poder para poder procesar transacciones y minar bitcoins[136].

Como se puede apreciar, el sistema Bitcoin tiene un mecanismo complejo para intentar garantizar su inviolabilidad y su seguridad, y eso hace a uno de sus rasgos esenciales, que en cierto modo constituye la contracara del rasgo de anonimato, esto es: si bien los administradores y usuarios del sistema Bitcoin son anónimos, el sistema se presenta como inviolable en virtud de la criptografía. Es decir, la confianza en el sistema no deriva de la autoridad de quien la administra (como podría ser un banco central en el caso de una moneda fiduciaria), sino en la supuesta inviolabilidad del mismo, independientemente de quien lo administre.

En resumen, la criptografía empleada por el sistema Bitcoin: a) cumple la misma función que cualquier medida de seguridad que podría tener un billete de una moneda fiduciaria, como ser, tintas de variabilidad óptica, imágenes latentes, o hilos de seguridad, por citar algunos ejemplos, b) sirve para realizar transacciones en forma segura, y, c) constituye la herramienta que dota de confianza al sistema Bitcoin.

---

[131] I*bíd.*
[132] Gallego Fernandez, *supra* nota 28.
[133] Manzur, Wolff y Robles, *supra* nota 10.

[135] *Supra* nota 128.
[136] *Ibíd.*

8. Transferencia y Minado del Bitcoin.

La transferencia y el minado del Bitcoin son dos caras de una misma manera. Los usuarios de Bitcoin son quienes transfieren sus bitcoins y los mineros son los nodos (mineros) de Blockchain que validan esa transferencia, y reciben bitcoins como recompensa por ese trabajo. De esa forma se crean nuevos bitcoins, se construye la cadena de transferencia y comercialización de los mismos.

8.1 Transferencia del Bitcoin.

El funcionamiento del sistema Bitcoin se pueda comprender más acabadamente en el contexto de una transacción, a medida que está se propaga por la red[137].

Ser dueño de un bitcoin significa tener la habilidad de transferirlo a terceros, y de tener control sobre la billetera o monedero donde se guarda la clave privada.

Una transacción es una transferencia de valores entre monederos Bitcoin que será incluida en la cadena de bloques[138].

Si una persona (digamos, "A") quiere transferir la titularidad de un bitcoin a otra persona (digamos, "B"), entonces "A" debe utilizar su clave privada para ordenar la transferencia[139] y consignar la clave pública de "B" para identificar al destinatario de la misma. En este contexto, una vez finalizada la operación, se dice que "B" pasa a ser el nuevo titular del bitcoin referido, dado que el sistema sólo permitirá una nueva transferencia del mismo si ella es ordenada mediante la utilización de su clave privada.

La *clave privada*, es secreta y se utilizada para firmar las operaciones, proporcionando una prueba matemática de que la transacción está hecha por el propietario del monedero. La *firma* también evita que la transacción no sea alterada por alguien una vez ésta ha sido emitida. Todas las transacciones son difundidas entre los usuarios, y por lo general, empiezan a ser confirmadas por la red en los 10 minutos siguientes a través de un proceso llamado *minería*[140].

Haciendo uso de la relación matemática entre la clave pública y la clave privada, el receptor de la transferencia puede probar su identidad y aceptar la transacción. **Mientras tanto, el transferente reconoce la transferencia de esos bitcoins mediante la firma de dicha transacción con su clave privada, y de esa manera le informa a la red que los bitcoins que antes se encontraban en su cuenta ahora pertenecen a otra persona[141]. El resultado de ese intercambio se transmite a todos los nodos conectados a la red del sistema Bitcoin[142].**

De forma muy resumida, para realizar una transferencia a favor de otro usuario no hay más que difundir un mensaje en la red Bitcoin indicando la cantidad a transferir y el

---

[137] Joshua J. Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*. https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=6425&context=lalrev (ultimo acceso 30 de julio de 2019)
[138] https://bitcoin.org/es/como-funciona
[139] Mora, *supra* nota 76.
[140] https://bitcoin.org/es/como-funciona
[141] Doguet, supra nota 137.
[142] *Ibíd*, citando a Ari Altstedter, Bitcoins Create Truly Democratic Policy, Followers Say, CANADA.COM (Jul. 22, 2011) citando a Bruce Wagner).

destinatario. Con cada una de estas transacciones se realizan una serie de operaciones de verificación y, una vez superadas, se anotan en la copia del archivo contable del nodo que las hubiera verificado y se difunden a otros nodos, de tal forma que el *libro* de transacciones es mantenido por la totalidad de los usuarios[143].

Las transacciones en Bitcoin son irreversibles, porque el hilo digital no puede romperse[144], y una vez que han sido incorporada a la cadena no se puede eliminar, o sustraer de la cadena. Nadie puede prohibir o censurar las transacciones que han sido validadas[145]. Se pueden realizar de forma nacional o internacional desde cualquier lugar del mundo que tenga internet[146].

Una vez que se firma y se envía un mensaje de transacción, este llegará a su destinatario en segundos, no obstante, se tratará de una transacción no confirmada, es decir, una transacción que todavía no forma parte de ningún bloque en la cadena de bloques. Por tanto, cuando una transacción recibe la primera confirmación significará que se ha integrado en un bloque para formar parte de la cadena de bloques[147].

En el sistema Bitcoin no se mantiene una tabla de saldos en la que se van actualizando la cantidad de monedas que cada uno de los usuarios tiene disponibles en un momento dado. Por el contrario, el sistema lo que hace es guardar la totalidad de las transacciones que se van realizando, estableciendo enlaces entre ellas que relacionan las transacciones actuales con las anteriores[148].

De esta forma, para que un usuario: *X* pueda transferir una cantidad: *z* a otro usuario: *Y*, *X* debe tener a su favor, es decir, apuntado a su identificador o clave pública, un número de transacciones sin usar cuyo importe total sea, al menos, la cantidad *z*[149].

A las transacciones que apuntan al usuario *X*, y que van a ser utilizadas por este para hacer la transferencia al usuario *Y*, se les denominan entradas de esta última transacción y a las direcciones del usuario o usuarios a cuyo favor se hace la transferencia, en este caso la del usuario *Y*, se les denomina salidas[150].

Como se puede apreciar, los Bitcoins circulan de mano en mano y de manera libre e irrestricta dentro de la red, por iniciativa de sus titulares y con la asistencia de los nodos (mineros), quienes validan o rechazan cada una de las transacciones, certificando de esa manera su autenticidad.

[143] Gallego Fernandez, *supra* nota 28, La negrita me pertenece.
[144] Martin Mushkin Esq, Joseph Sahid and Joseph Taub, VIRTUAL CURRENCY IS HERE TO STAY BITCOIN IS THE LATEST EVOLUTION, Law Office of Martin Mushkin LLC, https://app.vlex.com/#WW/search/*/bitcoin/p4/WW/vid/503498990.
[145] Barreira Delfino, "Acerca de la Criptomonedas", Revista de Derecho Bancario y Financiero – Numero 43 – Noviembre de 2018, 28-11-2018 - IJ-DXLII-773.
[146] Boar, *supra* nota 27, p. 47.
[147] Gallego Fernandez, *supra* nota 28, p. 97 a 141.
[148] *Ibíd*.
[149] *Ibíd*.
[150] *Ibíd*.

8.2 Minado del Bitcoin.

La creación e introducción en el mercado de nuevos bloques de criptomonedas se lleva a cabo a través de la actividad de minado. Se lo llama así porque la tarea de nodos que verifican las transacciones de bitcoin se asemeja a la de un minero en busca algún metal precioso o un mineral, quien para ello insume tiempo y recursos y de vez en cuando tiene la suerte de encontrar algo de ese metal precioso o mineral.

El sitio web Bitcoin.org define la minería del Bitcoin como: El proceso de **realizar cálculos matemáticos mediante computadoras muy potentes para confirmar las transacciones en la red Bitcoin e incrementar la seguridad**. **Como recompensa por sus servicios, los mineros Bitcoin pueden cobrar los costos de transacción de las transacciones que confirman junto con bitcoins nuevos que se crean en cada bloque.** La minería es un mercado especializado y competitivo en el que los beneficios se reparten de acuerdo a la cantidad de cálculos que se hacen. No todos los usuarios de Bitcoin realizan minería y no es una manera fácil de hacer dinero. Sin mineros las transacciones no se confirman y el sistema cae[151].

De esa manera, el minado de bitcoins se realiza mediante la resolución de problemas matemáticos aleatorios y sin utilidad práctica generados por el protocolo. Cada problema matemático es un bloque. Hasta que el bloque no es resuelto, el protocolo no arroja a los mineros un nuevo bloque. Es decir, hasta que algún minero no resuelva el problema, no se pasa al siguiente[152], y así sucesivamente bloque por bloque.

Los bloques generados pueden contener tanto los datos de nuevos Bitcoins como de Bitcoins viejos. Los Bitcoins nuevos serán generados hasta llegar a su límite mientras que los viejos estarán en circulación para siempre, salvo situaciones muy particulares como su envío a billeteras sin clave privada, por ejemplo. El minero agrega en ese bloque la información sobre Bitcoins nuevos, si ello fuera posible, y sobre las operaciones con Bitcoins viejos[153].

Esta dependencia lineal entre los problemas resulta en el encadenamiento denominado cadena de bloques. Una vez que la respuesta al bloque es encontrada por alguno de los mineros mediante varios intentos de fuerza bruta no determinista, aquella es transmitida por el nodo que encontró la solución a los otros nodos a fin de obtener una confirmación de la respuesta. Luego comparte ese bloque con el resto de la red y, si el resto de la red está de acuerdo con la solución matemática obtenida, el bloque pasa a formar parte de la cadena[154].

En resumen, la minería es un sistema de consenso distribuido que se utiliza para *confirmar* las transacciones pendientes a ser incluidas en la cadena de bloques. Hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un acuerdo entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones, deberán ser empacadas en un *bloque* que se ajuste a estrictas normas de cifrado y que será verificado por la red, como expliqué en el capítulo anterior. Estas normas impiden que cualquier bloque anterior se modifique, ya que hacerlo invalidaría todos los bloques siguientes[155].

---

[151] Barreira Delfino, supra nota 145.
[152] *Andrés Chomczyk*, ¿Qué es un bitcoin? Un primer análisis sobre su situación legal en la Argentina, elDial DC1B46.
[153] *Andrés Chomczyk*, Status LegalActual de los Bitcoin en la Argentina, elDial DC1D79, 9/10/2014.
[154] *Andrés Chomczyk*, supra nota 152.
[155] https://bitcoin.org/es/como-funciona (último acceso 29/7/2019).

La minería también crea el equivalente a una lotería competitiva que impide que cualquier persona pueda fácilmente añadir nuevos bloques consecutivamente en la cadena de bloques. De esta manera, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para revertir sus propios gastos[156]. De hecho, dado su constante trabajo aseguran la red y la protegen de la falsificación[157].

En resumen, una de las principales funciones de los nodos de la red que actúan como mineros es la construcción de la cadena de bloques[158], revisando, publicando y validando transacciones de bitcoins constantemente. La idea detrás de la cadena de bloques es contar con un registro de la titularidad de todos los bitcoins en circulación[159].

8.2.1 ***Proof of Work.***

Pero ¿cómo se genera el consenso para la validación de transacciones, para la adición de un bloque determinado que contiene información sobre transacciones? Existen varias maneras de implementar ese mecanismo de acuerdos en una red punto a punto (peer-to-peer) en donde existe una igualdad absoluta entre todos los actores intervinientes.

Para evitar que un usuario transfiera (gaste) dos o más veces[160] el mismo bitcoin, la red mineros Bitcoin tiene que validar esa transferencia y evitar que dicho usuario vuelva a transferir nuevamente ese bitcoin[161]. **Para hacer eso, el sistema Bitcoin emplea un mecanismo de votación entre los distintos nodos de la red, quienes revisan las transacciones y emiten su voto para validarlas**. De esa forma, la validez y veracidad de las transacciones es determinada por la mayoría de los nodos quienes utilizando sus computadoras después de consumir mucha energía y tiempo resuelven un problema matemático, mencionado y explicado en las subsecciones anteriores y más arriba, y emiten su voto[162].

El arduo y costoso proceso de validación descripto se llama *proof of work*[163].

Proof-of-work es el proceso a través del cual se resuelve el problema de difícil solución (rompecabezas criptográfico) al que he hecho referencia en las subsecciones anteriores y en esta sección más arriba, resuelto por una cantidad considerable de poder computacional distribuido relacionado a la firma, y por lo tanto aprobación de cada bloque de transacción, incluyendo bloques aprobados anteriormente. En el sistema Bitcoin, el *proof of work* es para demostrar que **el usuario/nodo ha consumido un considerable poder de CPU para resolver el problema**[164].

La creación de Bitcoin requiere de una capacidad de hardware y energía que solo sería alcanzable a partir de una gran inversión inicial y una dedicación plena[165]. Para tener una

---

[156] *Ibíd.*
[157] Boar, *supra* nota 27, p.p. 26.
[158] Gallego Fernandez, *supra* nota 28, p. 97 a 141.
[159] *Andrés Chomczyk*, supra nota 152.
[160] Llamado problema del "doble gasto".
[161] Dowd, Kevin, BITCOIN WILL BITE THE DUST., Dowd, Kevin, The Cato Journal ISSN: 0273-3072, Vol. 35 Núm. 2, Marzo - Marzo 2015, ID vLex: 636717173.
[162] *Ibíd*.
[163] *Ibíd.*
[164] *Ibíd*.
[165] Boar, *supra* nota 27, p.13.

referencia, nuestras computadoras personales, no tienen la capacidad necesaria para dedicarse a la minería[166].

Como expliqué en subsecciones anteriores, el requerimiento de *proof-of-work* implica que cada nuevo *hash* debe empezar con un cierto número de ceros, para podes ser agregado a la cadena. La cantidad de ceros requerida para cumplir con el *proof of work* constituye la "dificultad" de la transacción[167]. Cuando un minero resuelve el problema mencionado, lo publica y transmite a otros mineros y los otros mineros fácilmente verifican esa solución[168]. El minero que resuelve el problema primero, se asegura el derecho de adjuntar el bloque a la cadena de bloques más larga. Una vez confirmado, el nuevo bloque de la cadena es copiado a cada nodo de la red[169].

Así, el procedimiento antes descripto se reinicia para confirmar todas las transacciones Bitcoin que ocurrieron mientras los nodos se encontraban resolviendo el bloque anterior[170].

Es decir, una vez verificada y realizada una transacción por un nodo, se difunde por el resto de la red para que sea nuevamente verificada, confirmada e incluida en la cadena de bloques por los mineros y almacenada en la copia local de cada nodo[171]. La validez se comprueba por cada nodo de la red, para todo el histórico de transacciones, al instalar la aplicación cliente y descargar la cadena de bloques completa existente en ese momento y, para cada nueva transacción, en el momento de realizar esta y respecto de las transacciones anteriores, o entradas, involucradas en la misma[172].

Como las transacciones se comunican progresivamente de nodo a nodo, no puede garantizarse que el orden en el que un nodo de la red recibe dichas transacciones es el mismo en el que fueron realizadas[173].

En resumen, las transacciones de bitcoins tienen como objeto la transferencia de los valores que figuran como "salidas" (outputs) en transacciones previas. En rigor, en las transacciones lo que se transfiere es la titularidad, entendida como la posibilidad de realizar nuevas transacciones sobre un monto determinado de los valores (bitcoins) asentados en el registro público. Cada transacción representa una orden dirigida a asentar en el registro público un traspaso de aquella titularidad. Esta orden es comunicada a casi todos los nodos de la red bitcoin en busca de un "consenso" sobre su validez, el cual es conseguido a través de su inclusión en un bloque y las sucesivas confirmaciones[174].

---

[166] *Ibíd*.
[167] Pflaum, Isaac, A BIT OF A PROBLEM: NATIONAL AND EXTRATERRITORIAL REGULATION OF VIRTUAL CURRENCY IN THE AGE OF FINANCIAL DISINTERMEDIATION, Vol. 45 Núm. 4, Junio 2014, Georgetown Journal of International Law.
[168] Derks, J., Gordijn, J. & Siegmann, A. Electron Markets (2018) 28: 321. https://doi.org/10.1007/s12525-018-0308-3.
[169] Narayanan, A, Bonneau J, Felten E, *et al* (2016) Bitcoin and cryptocurrency technologies. Princeton University Press, New Jersey.
[170] Doguet, supra nota 137.
[171] *Ibíd*.
[172] *Ibíd*.
[173] *Ibíd*.
[174] Eraso Lomaquiz, Santiago E., Las monedas virtuales en el Derecho argentino. Los Bitcoins, AR/DOC/4070/2015.

Aunque el sistema dificulta el fraude, como consecuencia de que la orden es comunicada a todos los nodos al mismo tiempo y que no puede garantizarse el orden en el que los nodos de la red reciben dichas transacciones, podría darse el caso de que ocurran ataques de doble gasto[175].

Efectivamente, un usuario malintencionado podría realizar una transacción y a continuación, antes de que esta fuese validada, desde otro dispositivo realizar una nueva transacción utilizando las mismas entradas que en la anterior. Debido a los diferentes tiempos de propagación en la red habrá nodos que recibirán la segunda transacción antes que la primera -y por ello considerarán esta última como inválida- y viceversa, con lo que no habría acuerdo en cuanto a que operaciones deben considerarse válidas[176].

La solución que se ha implementado en Bitcoin para mitigar el anterior problema es, precisamente, la cadena de bloques que no es, por tanto, más que un mecanismo para ordenar las transacciones. De esta forma cada bloque contiene más de una transacción y las transacciones se agrupan en bloques y estos se enlazan entre sí, formando la cadena de bloques[177].

Cada bloque tiene una estructura definida en la que, al menos, se habrá de incluir el identificador de bloque, el identificador o referencia al bloque anterior, el conjunto de transacciones que se agrupan en el propio bloque (cada una de las cuales incluirá, al menos, los datos que se han visto anteriormente, es decir: entradas, salidas, importe, identificador de transacción, etc.) y un número aleatorio (que recibe el nombre de *nonce*) cuya función se verá más adelante[178].

Por tanto, en Bitcoin se gestionan dos estructuras paralelas y con funciones diferentes. En primer lugar, el árbol de transacciones cuya función es determinar la titularidad de las monedas y, en segundo lugar, la cadena de bloques que tiene por objeto ordenar dichas transacciones[179].

Las transacciones incluidas en un mismo bloque se considera que se han producido al mismo tiempo, mientras que la referencia que cada bloque contiene al anterior permite ordenarlos uno tras otro en el tiempo[180].

Cualquier nodo puede agrupar transacciones que todavía no forman parte de ningún bloque -es decir, transacciones no confirmadas-, formar un nuevo bloque potencial y difundirlo al resto de nodos como propuesta de siguiente bloque en la cadena[181].

Dado que los distintos nodos de la red pueden realizar diferentes propuestas de nuevos bloques potenciales, es necesario establecer un criterio que permita decidir cuál de estos nuevos bloques potenciales debe ser considerado el siguiente bloque de la cadena[182].

Este criterio no puede ser el orden de recepción de las nuevas propuestas de bloques ya que, como se ha visto para el caso de las transacciones y como consecuencia de las diferentes

[175] Doguet, supra nota 137.
[176] *Ibíd*.
[177] *Ibíd*.
[178] *Ibíd*.
[179] *Ibíd*.
[180] *Ibíd*.
[181] *Ibíd*.
[182] *Ibíd*.

velocidades de propagación de la información entre los nodos de la red, ello podría dar lugar a decisiones contradictorias entre dichos nodos[183].

Al contrario, el criterio por el que se opta en Bitcoin es considerar válido el nuevo bloque propuesto que incluya la solución a una búsqueda matemática. Esta solución es el número aleatorio, que se ha mencionado anteriormente al exponer la estructura de los bloques[184].

Estas búsquedas matemáticas son realizadas por los nodos de la red que actúan como mineros y consisten, una vez más, en el cálculo de un hash. En este caso, el *hash* se calcula a partir de los datos que conforman cada nuevo bloque propuesto[185]. Este proceso básicamente adivina una cadena de caracteres compuesta por números y letras (*hash*) hasta que finalmente da con la correcta. Para llegar a ese particular *hash*, el minero debe variar el «nonce» (una pequeña parte del bloque de su cabecera). Este siempre comienza con cero y es incrementado cada vez hasta obtener el hash requerido. Debido a que para alcanzar el objetivo se varía el *nonce*, el procedimiento es impredecible, haciendo que las probabilidades del minero sean bastante bajas. Por eso que se requiere de muchos intentos para llegar al correcto[186]

En concreto, dicho cálculo, se lleva a cabo sobre la estructura del siguiente conjunto de datos: identificador del último bloque de la cadena, el conjunto de transacciones que se integran en el nuevo bloque propuesto sobre el que se realiza el cálculo y un número aleatorio o *nonce*[187].

Para que el nuevo bloque sea considerado válido y, por tanto, el siguiente bloque de la cadena de bloques, el *hash* calculado debe estar por debajo de un determinado valor o, dicho de otra forma, debe tener un número determinado de ceros al principio[188].

Si el *hash* no cumple las anteriores condiciones se cambia el número aleatorio utilizado por otro distinto y se vuelve a realizar el cálculo del *hash* y así sucesivamente hasta que se obtiene el código *hash* con las condiciones requeridas[189].

Teóricamente, de media serían necesarias miles de millones de operaciones de cálculo de *hash* como las anteriores para dar con la solución que valide una concreta propuesta de bloque, lo que, a un solo ordenador, le llevaría años. No obstante, el propio sistema se autorregula, teniendo en cuenta la potencia de cálculo de todos los nodos de la red Bitcoin que actúan como mineros, ajustando cada dos semanas la dificultad de la búsqueda para que el tiempo medio de validación de bloque se mantenga alrededor de los 10 minutos[190].

Este periodo de 10 minutos es un compromiso entre el tiempo de confirmación y la probabilidad de que se produzcan ramas o bifurcaciones en la cadena (que se verán a continuación). Un intervalo de tiempo más corto en la confirmación de los bloques, haría que las transacciones se ejecutaran más rápidamente, pero aumentaría la probabilidad de que se produjeran ramas en la cadena de bloques y viceversa[191].

---

[183] *Ibíd*.
[184] *Ibíd*.
[185] *Ibíd*.
[186] ¿Qué es el Hashrate o Hashpower en las criptomonedas? Publicado en, https://criptotario.com/que-es-el-hashrate-en-las-criptomonedas. (último acceso el 29/7/2019)
[187] *Ibíd*.
[188] *Ibíd*.
[189] *Ibíd*.
[190] *Ibíd*.
[191] *Ibíd*.

Con esta configuración, sin embargo, no se resuelven todos los problemas ya que es posible que dos o más mineros validen simultáneamente propuestas de nuevos bloques diferentes, dando lugar a varias ramas posibles en la cadena[192].

En este tipo de situaciones cabe preguntarse cuál de los distintos primeros bloques, de las diferentes ramas existentes, habrá de ser considerado como bloque anterior al intentar validar un nuevo bloque o, en otras palabras, en que rama deben integrarse los nuevos bloques. **La regla es que, si todas las ramas tienen el mismo número de bloques, cada minero seguirá validando bloques considerando como anterior el último de los bloques de la primera de las ramas que hubiera recibido. No obstante, en el momento en el que una rama sea más larga que las demás automáticamente se comenzará a minar sobre esta lo que, además, provocará que el resto de ramas se eliminen y que todas las transacciones que estaban incluidas en los bloques que integraban estas ramas más cortas y que, por tanto, eran consideradas transacciones confirmadas, pasarán a formar parte, nuevamente, del conjunto de transacciones no confirmadas y tendrán que ser incluidas en un bloque posterior que, a su vez, habrá de ser minado para poder integrarse otra vez en la cadena de bloques**[193].

8.2.2 Confirmación.

Para que el sistema funcione adecuadamente, necesitamos que la red se ponga de acuerdo sobre el orden en el cual las transacciones ocurrieron, de lo contrario no podría quedar claro quién es el dueño de que bitcoin[194]. **A eso se le llama "confirmación"**[195]. A los fines de alcanzar este objetivo, cada bloque del Blockchain incluye una punta del eslabón (bloque) anterior (de hecho, esta punta es solo un *hash* del bloque anterior) que puede ser trazado hasta el bloque original, el "bloque de Genesis", para terminar con una cadena linear de blockchain[196].

De esta forma, las criptomonedas emplean un mecanismo que garantiza que la mayoría de los participantes en la red acuerdan sobre la validez de cada una de las transacciones[197], a los fines de obtener las correspondientes confirmaciones y agregar otro eslabón en la cadena.

Las confirmaciones proporcionan seguridad a los destinatarios de las transacciones, al asegurar su titularidad sobre las monedas recibidas y los protegen frente a los ataques de doble gasto[198], tal como expliqué en la subsección anterior.

Esto aseguraría que, dado que todas las máquinas del mundo tienen la misma chance de resolver el problema en cada intento que hacen, la escritura y auditoría no esté concentrada en un único jugador, sino que es aleatoria, eliminando las chances de la corrupción de los mismos[199].

---

[192] Gallego Fernández, *supra* nota 28, p. 97 a 141.
[193] Gallego Fernández, *supra* nota 28, p. 97 a 141.
[194] Dowd, supra nota 160.
[195] Una confirmación significa que una transacción ha sido procesada por la red y es poco probable que sea revertida. Las transacciones son confirmadas cuando son incluidas en un bloque y por cada bloque siguiente. Incluso una única confirmación se puede considerar segura para transacciones pequeñas, aunque para transacciones más grandes como 1000 USD, tiene sentido esperar hasta 6 confirmaciones o más. Cada confirmación reduce *exponecialmente* el riesgo de que la transacción sea revertida. https://bitcoin.org/es/vocabulario#cadena-de-bloques.
[196] Dowd, Kevin, supra nota 160.
[197] Derks, J., Gordijn, J. & Siegmann, A. Electron Markets (2018) 28: 321. https://doi.org/10.1007/s12525-018-0308-3
[198] Gallego Fernandez, *supra* nota 28, p. 97 a 141.
[199] https://www.bitcoinargentina.org/faqs/

Una transacción Bitcoin, por lo general, es recibida en pocos segundos y empieza a confirmarse en los 10 minutos siguientes. Durante este periodo, la transacción puede considerarse auténtica pero aún puede ser revertida. Si no puede esperar a una confirmación, se puede pagar una pequeña tasa o usar un sistema para detectar transacciones inseguras. Para cantidades mayores a 1000 USD, se debería esperar a tener 6 confirmaciones o más. Cada confirmación disminuye *exponencialmente* el riesgo de revertir una transacción[200].

8.2.3 Remuneración.

El proceso de minado consume energía, tiempo y capital, pero prohíbe reportes de transacciones malicioso, libres de penalidades[201]. Para llevar a cabo un proceso de minado de Bitcoin, es imprescindible invertir en capacidad computacional para procesar eficazmente las transacciones, garantizar la seguridad de la red y conseguir que todos los participantes estén adecuadamente sincronizados[202].

Como contraprestación por esta tarea de minado, los mineros reciben en pago bitcoins. Precisamente, en el sistema Bitcoin la recompensa viene en una combinación de nuevos bitcoins y una tasa por transacción[203]. La creación de nuevos bitcoins para recompensar a mineros, es la forma de aumentar el número de bitcoins circulante.

Las comisiones de los usuarios se pagan para acelerar la confirmación de sus transacciones. En la actualidad, el pago de estas comisiones, si no se quiere adquirir prioridad para confirmar la transacción, no es obligatorio, pero en el futuro, cuando cese el sistema de recompensas o cuando estas dejen de ser rentables, las comisiones serán la única fuente de ingresos de los mineros, por lo que la realización de transacciones dejará de ser gratuita y, probablemente, la cuantía de dichas comisiones aumentará de forma significativa[204], las cuales pasarían a ser obligatorias y más elevadas que en la actualidad, lo que igualmente podría producir el abandono de usuarios[205].

Para recibir bitcoins como premios otorgados por el sistema de manera automática, el valor del bloque calculado por el minero debe coincidir con el valor generado por el sistema de Bitcoin[206].

Al comienzo de sistema bitcoin, un minero exitoso era remunerado con 50 bitcoins por cada bloque de la cadena validado. Sin embargo, después de 210.000 bloques validados la recompensa fue reducida a la mitad, esto es, a 25 bitcoins por bloque validado. Este proceso de reducción a la mitad de la retribución por minado continuará ocurriendo cada 4 años, y, por lo tanto, la producción de bitcoins en el tiempo se irá reduciendo gradualmente hasta llegar a cero, hasta llegar a un total de 21 millones de bitcoins[207].

[200] https://bitcoin.org/es/debes-saber.
[201] Shi, N. Financ Innov (2016) 2: 31. https://doi.org/10.1186/s40854-016-0045-6
[202] Barreira Delfino, supra nota 145.
[203] Dowd, supra nota 160.
[204] Gallego Fernandez, *supra* nota 28, p. 97 a 141.
[205] Gallego Fernandez, *supra* nota 28, p. 97 a 141.
[206] Andrés Rivas Herazo, supra 14.
[207] Dowd, Kevin, supra nota 160.

Lo interesante es que la dificultad de la minería aumenta a medida que más personas se unen a la red, por tanto, la necesidad de *hashpower* se incrementa. En otras palabras, se requiere de más intentos por segundos para encontrar la solución[208].

Un principio importante del sistema Bitcoin es que no asume que todos los mineros que componen la red actúan en forma honesta al validar las transacciones. Por lo tanto, para lidiar con posibles mineros deshonestos, el sistema Bitcoin estableció un mecanismo de castigos y recompensas. Este mecanismo funciona como una competencia para ver que minero aprueba primero una determinada transacción, y el costo de entrada a esa competencia es una cierta cantidad de energía que el minero deberá consumir con su computadora para poder validar una transacción. Las probabilidades de éxito de un minero son aproximadamente proporcionales a total de energía que tiene disponible para utilizar y consumir la computadora que va a intentar resolver el problema y validar la transacción. Un minero que emplea un 1% de consumo de energía para validar la transacción tiene un 1% de probabilidades de ganar. Cada tarea validación implica un considerable consumo de energía, y, por lo tanto, eso desalienta a mineros deshonestos o corruptos que pretendan validar transacciones que no son auténticas, porque el costo de la energía consumida es alto, simplemente porque no sería un actividad redituable. El concepto es que el proceso de minado es un proceso demasiado caro como para hacerlo sin la finalidad de obtener la recompensa, o, mejor dicho, para hacerlo con la sola finalidad de dañar o alterar al sistema[209].

La rentabilidad de las tareas de minado para los mineros depende en parte del costo de la electricidad y la eficiencia de la maquina utilizada para llevar a cabo las tareas de minado, las cuales pueden variar considerablemente[210]. Por lo tanto, la rentabilidad del minado depende del precio del Bitcoin. Si el precio del Bitcoin es superior al costo de la energía eléctrica entonces el proceso de minado va a ser rentable para el minero. Si el precio del Bitcoin baja, entonces esa rentabilidad se va a reducir.

Es decir, la seguridad del Bitcoin está en el incentivo económico y en los intereses alineados de los mineros[211], y no en el sistema, lo cual demuestra que no es inviolable, altamente manipulable y susceptible a ataques.

Por el contrario, creo que ese sistema de castigos y recompensas no blinda al sistema Bitcoin de este tipo de ataques o distorsiones, porque asume que toda la gente en su totalidad es racional, va a actuar en beneficio propio y buscar obtener una ganancia, descartando cualquier obrar irracional o mal intencionado, y/o beneficios que un participante de la comunidad de Bitcoin que pudiere perseguir otros intereses, como ser, alterar la misma, crear operaciones inexistentes, o boicotearla a pedido de algún competidor.

Por otra parte, si el minado del Bitcoin se termina monopolizando entonces el titular del monopolio va a poder manipular el sistema a su antojo.

---

[208] ¿Qué es el Hashrate o Hashpower en las criptomonedas? Publicado enhttps://criptotario.com/que-es-el-hashrate-en-las-criptomonedas.

[209] Dowd, supra nota 160.

[210] Dowd, supra nota 160.

[211] "The security of blockchains come from economic incentives, not from math. We cross our fingers and hope that a group of attacker nodes will choose to play by the rules." Peter Rizun, https://www.coindesk.com/after-the-fork-how-two-bitcoin-cash-blockchains-might-wage-war

De hecho, quien tenga mayoría de los nodos hasta podría minar bloques "vacíos" para ampliar la longitud de su cadena y hacer prevalecer su cadena, o para inundar una cadena de transacciones y con el fin de acaparar la capacidad de procesamiento de los mismos y haciendo más lento el tiempo que lleva validar una transacción (*Spam transactions*).

El mecanismo de minado es esencial para que el Bitcoin funcione, porque genera el incentivo para que los miembros de la comunidad Bitcoin validen de manera confiable las transacciones, eviten casos de doble gasto, y mantengan un sistema de control descentralizado, libre de intermediarios. Ello así, toda vez que el reducido costo de transacción del Bitcoin es el principal beneficio social de dicha moneda, y para el caso, de todas las criptomonedas[212].

[212] Blundell-Wignall, A. (2014), "The Bitcoin Question: Currency versus Trust-less Transfer Technology", *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jz2pwjd9t20-en.

9. Descentralizada o Distribuida. Merge Mining.

La mayor innovación de las criptomonedas es que no se requiere de un ente centralizado (como un banco central) que brinde confianza para realizar las transacciones[213]. En su lugar, el Bitcoin se apoya en la confianza de la comunidad o red que verifica cada una de las transacciones y mantiene la integridad del sistema[214]. Por eso se dice que uno de los rasgos salientes del Bitcoin es que es una moneda "descentralizada"[215].

En teoría, las criptomonedas vienen a resolver un problema de importancia: la transferencia segura de propiedad sin la necesidad de intermediarios o un tercero que garantice confianza[216]. Es decir, la premisa básica de las criptomonedas es establecer un medio de cambio basado en matemática inmutable y no sujeto al control o la manipulación de un gobierno[217], y de esa forma evitar lidiar con un banco central y poder transaccionar en forma directa, y sin intermediarios.

De esta manera, en teoría, la política monetaria del Bitcoin la fijaría la propia comunidad que opera y usa el sistema.

Precisamente, el Bitcoin necesita de una red de personas (físicas y/o jurídicas) para adquirir y brindar confianza a los usuarios. Asimismo, para poder validar las transacciones de bitcoins y crear más bitcoins es necesario que esa misma red de nodos (los mineros integrantes del blockchain) constantemente analice y determine la validez o no de cada transacción.

De esa forma, a diferencia de otras criptomonedas, el Bitcoin no tiene (en teoría) ni siquiera una entidad o persona jurídica designada que la administre.

Es decir, el Bitcoin surge y depende de una "memoria colectiva" que revise y legitime cada una de las transacciones; una red punto a punto, en la que los usuarios comparten sus resultados con otros usuarios, sin necesidad de intervención de ninguna entidad financiera ni banco central, porque es la comunidad de personas quien verifica las transacciones y evita que ocurran casos de doble gasto (double-spending).

La inexistencia de un banco central preparado para intervenir para estabilizar el precio, hace que el precio de las criptomonedas sea altamente volátil[218].

El sistema Bitcoin funcionará siempre y cuando la red se integre de un número suficiente de mineros que compitan entre sí. En cuanto los mineros individuales se asocien y operen en forma colusiva para constituir un jugador dominante o un grupo de mineros grandes se cartelice, entonces esos grupos dominantes van a tener control sobre el sistema y van a poder determinar cuáles transacciones son válidas y cuales no los son. En ese caso, los tenedores de bitcoin deberán esperar que ese grupo no abuse de su posición dominante[219], que operaría a modo de un banco central volviendo al modelo fiduciario de las monedas comunes y corrientes.

---

[213] *Ibíd.*
[214] Dowd, supra nota 160.
[215] Algunos autores sostienen que es distribuida en lugar de descentralizada porque todos los nodos están conectados sin depender de un nodo central (como ocurriría con una red descentralizada). Sin importar el concepto que se utilice, lo relevante de este aspecto es que el Bitcoin no depende de ninguna autoridad central para funcionar.
[216] Blundell-Wignall, supra 214.
[217] Mushkin Esq, supra 144.
[218] Blundell-Wignall, supra 214.
[219] Dowd, supra nota 160.

Esos incentivos son: a) reducción de costos de minado, y b) aumento de probabilidades de obtener confirmaciones realizando la misma cantidad de trabajo.

Es decir, para que el sistema Bitcoin funcione requiere de competencia entre los mineros, de lo contrario terminaría transformándose en un sistema similar al de las monedas tradicionales, pero con menos garantías, sin regulación, dotado de menor confianza (el "cartel" de mineros actuaría como una corporación anónima), y con la capacidad de que un solo participante (o un conjunto de ellos) puedan cambiar las reglas a su antojo de la noche a la mañana, determinando quien puede minar y quien no, y hasta establecer tasas u honorarios adicionales como contraprestación para autorizar y procesar transacciones.

Tal es así que, han existido casos de *merge mining* en los cuales los mineros se unen para obtener mejores resultados a un menor costo. Es más, cada vez hay más *pooles* de minería y más grandes que acaparan una mayor porción del *hash rate* de la red[220], y eso atenta contra la descentralización del Bitcoin.

Precisamente, se comenzó a diseñar y construir hardware y procesadores a medida para el minado de bitcoin[221] (*ASIC's: application-specific integrated circu*its), que han venido duplicando su capacidad de procesamiento, aproximadamente, cada 6 meses, alcanzando, en la actualidad, alguna de estas máquinas una capacidad de decenas de *tera-hashes* por segundo. Igualmente, surgieron *startups* que ofrecían la posibilidad de contratar capacidad de minado en la nube[222].

Todo ello ha conducido a la aparición de grandes *granjas* con miles de máquinas especializadas dedicadas exclusivamente al minado de bitcoins que, prácticamente, han eliminado la posibilidad de que los mineros domésticos u ocasionales puedan conseguir minar algún bloque[223].

La creciente complejidad técnica y, también, los crecientes recursos financieros, materiales y humanos necesarios para minar las monedas favorecen la aparición de superestructuras o grupos de mineros. Así, por ejemplo, durante el pasado mes de abril más del 70% del total de transacciones fueron minadas por grupos chinos de minado y, más del 70% de aquel porcentaje por solo dos de estos grupos. En tiempos más recientes, el 50,1% de la capacidad de minado mundial estaba en manos de únicamente 4 de estos grupos y, solamente una docena de ellos, reunía más del 87% de la capacidad total de minado[224].

Todos estos datos demuestran que, en realidad, Bitcoin no es tan descentralizada como se quiere hacer ver y, también, que sus usuarios han perdido el control del sistema[225].

Ese monopolio u oligopolio de mineros, o de un grupo dominante que acapare el 50% del esfuerzo computacional de la red Bitcoin, podría permitirles alterar el sistema, hasta ensayar un "cepo" de Bitcoin para los actuales usuarios si quisieran, o validar transacciones fraudulentas y excluir transacciones legítimas.

---

[220] *Ibíd.*

[221] Véase: https://www.bitcoinmining.com/bitcoin-mining-hardware.

[222] Por ejemplo: Eobot: https://www.eobot.com; Genesis Mining: https://www.genesis-mining.com; Ghash.IO: https://ghash.io; HashFlare: https://hashflare.io; HashNest: https://www. hashnest.com; MineOnCloud: https://mineoncloud.com; MinerGate: https://en.minergate.com; Minex: https://minex.io; NiceHash: https://www.nicehash.com; etc.

[223] Gallego Fernández, *supra* nota 28, p. 97 a 141.

[224] En la dirección: https://blockchain.info/es/pools timespan=4days se pueden consultar estos datos para las últimas 24 o 48 horas o para los últimos 4 días.

[225] Gallego Fernández, *supra* nota 28, p. 97 a 141.

Finalmente, ese monopolio u oligopolio o cartel, podría terminar en los hechos funcionando como una especie de banco central no gubernamental, y tener la entidad y aptitud suficientes para transformar al Bitcoin en una moneda virtual cuyo esencia y funcionamiento constituiría una réplica privada del sistema monetario fiduciario de cualquier país. Por otra parte, a los fines de comprar otras monedas fiduciarias con Bitcoins o intercambiarlas por otras criptomonedas, muchas veces hay que recurrir a plataformas de intercambio (o *exchanges*). Estas plataformas son intermediarios, es decir, son los terceros que el Bitcoin pretendía evitar o excluir de su operatoria para reducir el costo y el tiempo de cada transacción. Estos intermediarios, cobran comisiones por transacción como cualquier entidad financiera.

Por todo lo expresado anteriormente, digo que el Bitcoin no eliminó a los intermediarios completamente; por el contrario, solamente sustituyó unos por otros, es decir, sustituyó a los operadores bancarios tradicionales por los mineros[226], y adquirió de esa manera, más notas comunes a las monedas fiduciarias comunes y corrientes.

En resumen, si bien Bitcoin nació como una moneda virtual descentralizada o diseminada, poco a poco la misma va perdiendo ese rasgo, asemejándose cada vez más a una moneda tradicional, controlada y administrada por una entidad central.

[226] *Ibíd.*

10. Diferencia entre Dinero y Moneda.

Me parece importante distinción entre dinero y moneda, porque no es una mera diferencia semántica, su caracterización tiene efectos distintos.

Entre la moneda y el dinero existe una relación de género y especie, siendo el dinero aquella moneda dotada de curso legal por algún estado. Con prístina claridad explica Nussbaum que la afirmación anterior presenta ciertas excepciones. Sostiene el autor que *"[h]ay cosas que por una u otra razón no encuadran en el concepto general de la moneda, pero que en situaciones especiales pueden ser consideradas como dinero, ya sea por la fuerza de una particular orientación legislativa o en virtud de una decisión judicial"*[227].

En el plano jurídico sólo será dinero lo que el Estado diga que es dinero. Por ende, y en atención a la redacción actual del art. 765[228] del Cód. Civ. y Com., parecería que **sólo podría considerarse como dinero la moneda de curso legal en la República Argentina**[229]. De esa manera, las obligaciones dinerarias son aquellas cuyo objeto es la entrega de una suma de dinero[230], si fueren de dar una moneda extranjera, sería obligaciones de dar cosas porque no son dinero.

Subsiste entonces la incógnita sobre si corresponde considerar que la noción de "moneda" —y no dinero- se presenta como una calificación jurídica que incluya en forma exclusiva aquellas que tengan curso legal en algún estado o si, por el contrario, podría incluirse dentro de esta categoría los bienes que cumplan con las tres funciones de la moneda[231].

Al respecto, pueden esbozarse dos teorías principales sobre el concepto de moneda en el marco jurídico actual del derecho argentino. Por un lado, una postura amplia permitiría calificar como moneda a todo bien que sea susceptible de actuar como una medida de valor, unidad de cuenta y medio de pago, identificando así la naturaleza económica de la moneda con su calificación jurídica[232].

Sería posible considerar como moneda sólo a aquella que tenga curso legal en algún estado, sea en la República Argentina o en el extranjero. De esta manera, los términos "moneda que no sea de curso legal en la República" o "moneda sin curso legal" utilizados por el Código Civil y Comercial se identificarían con la noción de moneda extranjera[233].

Tal parecería ser la postura adoptada por el art. 30 de la Carta Orgánica del Banco Central que determina que "*son susceptibles de circular como moneda, cualesquiera fueran las condiciones y características de los instrumentos, cuando: i) El emisor imponga o induzca en forma directa o indirecta, su aceptación forzosa para la cancelación de cualquier tipo de obligación; o ii) Se emitan por valores nominales inferiores o iguales a 10 veces el valor del billete de moneda nacional de máxima nominación que se encuentre en circulación".* Esta norma eliminaría,

---

[227] Eraso Lomaquiz, supra 173.
[228] Concepto. La obligación es de dar dinero si el deudor debe cierta cantidad de moneda, determinada o determinable, al momento de constitución de la obligación. Si por el acto por el que se ha constituido la obligación, se estipuló dar moneda que no sea de curso legal en la República, la obligación debe considerarse como de dar cantidades de cosas y el deudor puede liberarse dando el equivalente en moneda de curso legal.
[229] Eraso Lomaquiz, supra 173.
[230] Lorenzetti, supra 100, Tomo I, p. 744.
[231] Eraso Lomaquiz, supra 173.
[232] *Ibíd.*
[233] *Ibíd.*

prima facie, parecería despejar toda duda respecto de lo que podría circular como moneda en el país, en tanto sólo abarcaría a los instrumentos que tengan curso legal o que sean emitidos por los valores nominales indicados en el texto citado. El requisito de la imposición o inducción del curso legal del instrumento por su emisor echaría por tierra la posibilidad de considerar a los bitcoins como moneda, en tanto no existe una autoridad central de emisión[234].

Al respecto, el Banco Central emitió un comunicado de prensa alertando al público sobre los riesgos que conlleva la utilización de las monedas virtuales. Sin perjuicio de la falta de carácter normativo de los comunicados de prensa, el Banco Central ha expresado que las monedas virtuales no son emitidas por aquel ni ninguna otra autoridad monetaria internacional, concluyendo así —acertadamente- en su carencia de curso legal y respaldo alguno por parte de una autoridad estatal [235]**.** El mencionado organismo ha expresado que se encuentra "analizando diversos escenarios para verificar que las operaciones con estos activos no se constituyan en un riesgo para aquellos aspectos cuya vigilancia está expresamente establecida en su Carta Orgánica" [236].

En adición a las dos teorías descriptas precedentemente, se presenta la posibilidad de esbozar una tercera alternativa ecléctica que defina a la moneda como todo bien —tanto material como inmaterial- susceptible de actuar como una medida de valor, unidad de cuenta y medio de pago que, a su vez, sea utilizado habitualmente como tal y cuya finalidad no sea complementaria —o secundaria- respecto de otra distinta sobre la cual se fundamente un régimen específico[237].

Adelanto, que adhiero a esta teoría, y que por ello considero que el Bitcoin es moneda y, por lo tanto, podría ser asimilado a moneda extranjera en cuanto al tratamiento en el derecho argentino.

Precisamente, la redacción actual del artículo 765 del Código Civil y Comercial de la Nación contempla dos tipos de monedas: i) aquellas que tienen curso legal en la República, y ii) aquellas que no tienen curso legal en la República. Con la redacción actual del citado artículo, en principio, sólo las primeras podrían ser calificadas como dinero. Las segundas, si bien son consideradas como cosas, también continúan siendo denominadas moneda (moneda-mercancía). Esta norma deja en evidencia la dicotomía existente entre las monedas que son consideradas dinero -por tener curso legal en nuestro país- y aquellas que no lo son[238].

Es decir, Bitcoin podría ser considerado moneda extranjera, pero no dinero de conformidad con lo dispuesto en el artículo 765 del Código Civil y Comercial de la Nación, y, por lo tanto, una obligación de dar Bitcoin debería pagarse con y es exigible en Bitcoin, y no con dinero.

Finalmente, el proyecto de reforma del CCyCN, modifica los arts. 765[239] y 766[240], manteniendo

---

[234] Eraso Lomaquiz, supra 173.

[235] *Ibíd.* Comunicación al público en general emitida por el Banco Central de la República Argentina a través del sitiowww.clientebancario.gov.ar, mayo de 2014. El Banco Central también alertó al público sobre la volatilidad del valor de las monedas virtuales, así como la posibilidad de que aquellas sean utilizadas para operaciones de lavado de activos y diversos tipos de fraude. Ver también, Banco Central de la República Argentina, Boletín de Estabilidad Financiera, Primer Semestre de 2014, pág. 91. La negrita y el subrayado me pertenecen.

[236] *Ibíd.*

[237] *Ibíd.*

[238] *Ibíd.*

[239] "Concepto. La obligación es de dar dinero si el deudor debe cierta cantidad de moneda, determinada o determinable, al momento de constitución de la obligación. Si por el acto por el que se ha constituido la obligación, se estipuló dar moneda que no sea de curso legal en la República, la obligación debe considerarse como de dar sumas de dinero."

el concepto amplio de dinero y todas las obligaciones que sean dar alguna moneda que sea no sea de curso legal en Argentina deberá considerarse de dar sumas de dinero. Es decir, si el Bitcoin es considerado moneda (aún sin tener curso legal), entonces para el derecho argentino sería también dinero, si es que se aprueba el proyecto de reforma.

Esto permite imaginar, que, en un futuro no muy lejano, el Bitcoin también podría ser considerado dinero para el derecho argentino.

11. Bitcoin y la Ley Argentina.

Determinar qué es Bitcoin para la ley argentina tiene importancia práctica porque permite saber que marco normativo va a regular su creación, su circulación, si es una actividad regulada o no, que impuestos se le debería aplicar, todo lo cual determinará en última instancia, quienes van a ser los usuarios de Bitcoin y su utilización masiva o sectorizada.

Si Bitcoin fuese considerado una moneda, entonces podría ser utilizado como medio de pago masivo, y eventualmente, ser utilizado en forma cotidiana para realizar todo tipo de transacciones. Por el contrario, si fuese considerado como un título representativo valor o una acción, el uso de Bitcoin quedaría más restringido a un uso comercial, y posiblemente especulativo, para personas de un mayor grado de sofisticación financiero, quienes estuvieren autorizados para operar por la entidad de contralo estatal correspondiente, y sus eventuales clientes quienes lo utilizarían a modo de inversión, restándole liquidez.

Determinar la naturaleza jurídica de Bitcoin también sería de utilidad para la Comisión Nacional de Defensa de la Competencia, a fin de que esta pueda determinar si existen cuestiones actividades distorsivas de la competencia, anticompetitivas, cartelizaciones, y/o actividades monopólicas por el obrar de los mineros de Bitcoin, o por el *merge minig*, o como ocurre con Libra donde Facebook, Google, y sus otros impulsores ya tienen una posición casi monopólica en algunos mercados[241].

12. Bitcoin No Es …

En primer término, me parece importante a los efectos de construir una teoría sobre qué es Bitcoin, desarrollar una teoría sobre lo que no es, a saber:

a. **Bitcoin No es Dinero ni Moneda de Curso Legal**. Bitcoin no es dinero ni moneda de curso legal, y parecería que tampoco pretende serlo[242]. Es más, dada su naturaleza anárquica parecería ser que solo pretende ser aceptado y utilizado en forma masiva, manteniéndose por fuera del sistema financiero, sin tener aspiraciones a ser una moneda de curso legal ni dinero.

El primer argumento por el cual se podría decir que Bitcoin no es una moneda de curso legal es que, a modo de confesión, la propia página web de Bitcoin España dice que *"el Bitcoin no es una moneda oficial[243]"*.

---

[240] "Obligación del deudor. El deudor debe entregar la cantidad correspondiente de la especie designada tanto si la moneda tiene curso legal en la República como si no lo tiene."

[241] https://www.coindesk.com/facebooks-libra-cryptocurrency-bad-for-privacy-bad-for-competition. (último acceso 29/7/2019).

[242] Esto teniendo en cuenta las disposiciones del CCyC tal cual se encuentran redactadas en la actualidad.

[243] https://bitcoin.org/es/debes-saber (último acceso 29/7/2019).

En igual sentido y reforzando el concepto expresado en la propia página web de Bitcoin España, la página web de Bitcoin Argentina define Bitcoin como una moneda digital de emisión descentralizada sin curso legal[244], y posteriormente, lo reduce solo a *"un sistema de pago electrónico P2P"*[245].

El otro argumento por el cual mucha gente considera que el Bitcoin no son monedas de curso legal (ni una moneda de ninguna naturaleza, para el caso), es que no reuniría la totalidad de las características típicas de una moneda, esto es: unidad de cuenta, reserva de valor, y un medio de cambio, pero como veremos más adelante, esto no es tan así.

Desde una mirada más práctica parecería ser que la razón más relevante de rechazar a las criptomonedas como dinero (o moneda de curso legal) es que los estados desean mantener un cierto monopolio sobre el sistema de pagos. Todos tienen que pagar sus impuestos, y, por lo tanto, cualquier banco que reciba dichos pagos deberá poder hacer el posterior *clearing* con el banco del estado, habitualmente el banco central. A tal fin, el gobierno solamente aceptaría moneda de curso legal, que es la palanca sobre el sistema financiero que asegura que el gobierno pueda afectar las tasas de interés de toda la economía. El banco central no aceptaría Bitcoin en proceso de *clearing*. Sin importar cuan aceptados sea el Bitcoin entre sus entusiastas, de ninguna manera podría tener impacto en la habilidad del gobierno de conducir la política monetaria, porque al fin del día todos tienen que pagar sus impuestos con moneda local de curso legal en el país[246].

Más aún, las monedas de curso legal son representadas por los billetes físicos se transmiten de mano en mano, o digitalmente, y en forma inmediata. Contrariamente, cada bitcoin se transmite solo digitalmente, y las transferencias no son inmediatas, porque tienen demoras de por lo menos de 10 minutos para validar cada transferencia.

Justamente, porque su valor es altamente volátil, pareciera ser que no cumple una función de reserva de valor, esto es capaz de guardar parte de un patrimonio actual para poder recuperar de manera prácticamente igual en el futuro. El depósito de valor hace la función de ahorro en la economía, tiene que ser estable y ser imposible de falsificar para mantener la confianza[247].

Si bien el argumento de la volatilidad de su valor parecería ser un argumento coyuntural, no hay certeza de que su valor respecto de monedas como el Dólar se vaya a estabilizar en algún momento, de hecho, desde que fue creado, el precio del Bitcoin experimentó subas muy pronunciadas y caídas del 50% del valor o más, después de alcanzar cada pico de valor.

Bitcoin, en sentido estrictamente normativo y tradicional, al momento no constituye moneda (dinero), ya que carece de curso legal y no son emitidas por una autoridad pública de carácter central, como lo es el Banco Central[248].

Desde la perspectiva de la Constitución de la Nación Argentina, en el artículo 75 inciso 6 estableció que es facultad exclusiva del Congreso Nacional "*establecer y reglamentar un banco federal con facultad de emitir moneda, así como otros bancos nacionales*". De esa manera la

[244] https://www.bitcoinargentina.org/faqs/ (último acceso 29/7/2019).
[245] *Ibíd.*
[246] Blundell-Wignall, supra 214.
[247] Boar, *supra* nota 27, p. 140.
[248] Faliero, *supra* nota 11, p.125, Ed. Ad-Hoc. La negrita me pertenece.

Constitución de la Nación Argentina delegó la emisión monetaria y su control exclusivamente en el Banco Central de la República Argentina[249].

El artículo 30 de la Carta Orgánica (Ley 24.144 y modificatorias) dispone que: "*el Banco es el encargado exclusivo de la emisión de billetes y monedas de la Nación Argentina y ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, bancos u otras autoridades cualesquiera, podrán emitir billetes ni monedas metálicas ni otros instrumentos que fuesen susceptibles de circular como moneda*".

Una interpretación restrictiva de esa norma permitiría considerar como moneda solamente a los instrumentos que sean emitidos por autoridades, conforme el giro final de la primera parte del articulo 30, dejando de lado a los particulares;[250] como son los mineros de Bitcoin.

Es así, que una nueva tecnología nos lleva a releer definiciones en dos normas centrales y fundacionales del sistema jurídico: la Constitución Nacional y la Ley N° 24.114 y sus modificatorias (la "Carta Orgánica del BCRA"). Una lectura sistemática de ambas solo nos permite concluir que es imposible darle el carácter de moneda de curso legal a los bitcoins[251], al menos de moneda de curso legal y forzoso en la República Argentina.

El primer requisito para que un instrumento sea tratado como dinero es que cuente con curso legal, es decir, aceptación forzosa. El curso legal, o aceptación forzosa, es una característica que resulta contradictoria con la naturaleza de Bitcoin. El curso legal se caracteriza por ser un elemento que dota al instrumento de fuerza para cancelar una obligación, sin importar si el acreedor quiere aceptar tal instrumento como forma de pago. La exigibilidad de Bitcoin nace de la voluntad de las partes, y no de la ley[252],su exigibilidad es contractual.

Con relación al segundo requisito, creo que no es de aplicación a los bitcoins puesto que los mismos no emiten valores nominales que guarden relación alguna con la moneda nacional. El valor nominal del que habla el art. 30 es aquel que se encuentra consignado en el título, impuesto por el emisor y que se encuentra atado a toda la existencia del instrumento. En el caso de Bitcoin, estos carecen de valores nominales. Bitcoin solo tiene valor de mercado, aquel que es fijado por el libre juego de la oferta y la demanda al momento de ser empleado[253].

Asimismo, el 28 de junio de 2014 el Banco Central de la República Argentina emitió un comunicado de prensa sobre Bitcoin. Recordamos que tal comunicado de prensa no tiene efectos jurídicos por sí solo, pero nos muestra la postura del BCRA al respecto y nos permite orientar la interpretación de la normativa existente al respecto [254].

En ese comunicado, el BCRA alertó a los usuarios sobre los riesgos de las monedas virtuales, al afirmar que, al no ser emitidas por el BCRA ni por otras autoridades monetarias internacionales,

---

[249] http://elbitcoin.org/situacion-legal-de-bitcoin-en-argentina./ de *Andrés Chomczyk, 10/10/13. (último acceso 29/7/2019). El subrayado me perteneces.*
[250] *Ibíd.*
[251] Andrés Chomczyk, Reflexiones sobre el incipiente marco legal de la industria fintech en Argentina, Revista de Graduados de Derecho de la Universidad Austral - Número 3 - Junio 2017, 28-06-2017, IJ-CCCLXXVI-623.
[252] El proyecto de reforma del código civil y comercial de la nació establece en su artículo 766: *"Obligación del deudor. El deudor debe entregar la cantidad correspondiente de la especie designada tanto si la moneda tiene curso legal en la República como si no lo tiene."* Si el Bitcoin fuere considerado moneda extranjera, entonces, el pago en Bitcoin sería exigibile por ley.
[253] Chomczyk, supra 252.
[254] *Ibíd.*

"no tienen curso legal ni poseen respaldo alguno". Así la existencia y uso del "Bitcoin" quedan convalidados, no involucrando alguna conducta ilegal[255].

En tal sentido, el comunicado reconoce la existencia y uso de los bitcoins; en ningún lugar del mismo se dispone la prohibición del uso ni se considera que el uso de bitcoins es una conducta ilegal. La única advertencia que da el BCRA es "que las llamadas "monedas virtuales" no son emitidas por este Banco Central ni por otras autoridades monetarias internacionales, por ende, no tienen curso legal ni poseen respaldo alguno" [256].

La consecuencia más importante de esto es que el BCRA no se considera como la autoridad encargada de regular Bitcoin, en la medida que no entren en juego "aspectos cuya vigilancia está expresamente establecida en su Carta Orgánica" [257], es decir, porque no lo considera moneda.

Otra consecuencia, no menor e inclusive más importante que la señalada, es que al no ser una moneda en el sentido que entiende la normativa aplicable, es imposible hacer cuadrar a las criptomonedas, los bitcoins entre ellas, dentro del Sistema Nacional de Pagos[258], porque el estado no acepta Bitcoin para el pago de impuestos.

Actualmente, en nuestro entorno la mayoría de la doctrina coincide en considerar que los bitcoins son, en cuanto a su naturaleza jurídica, bienes. Esta resulta ser la conclusión lógica a la cual cabe arribar en tanto los bitcoins, así como el resto de las monedas virtuales, son representaciones digitales de valor que, como tales, son intangibles[259].

En tal entendimiento, en diciembre de 2017 la Comisión Nacional de Valores ("CNV") emitió una advertencia en relaciona las "Ofertas Públicas de Monedas Virtuales y Tokens" en las que refiere a las emisiones de monedas virtuales como *"inversiones especulativas de alto riesgo"*, aclarando que "*el token digital emitido puede representar una acción en una empresa, un bono prepago para servicios futuros o, en algunos casos, no ofrecer ningún valor discernible"*, pero no como una moneda.

Es más, en esa misma advertencia, la CNV manifestó que de acuerdo *"a lo dispuesto por el Capítulo 6, Título V, del Libro tercero del Código Civil y Comercial de la Nación y el artículo 2° de la Ley de Mercado de Capitales N° 26.831, dependiendo de las particularidades de cada caso y de cómo cada ICO es estructurado, podríamos encontrarnos ante valores negociables cuya emisión por oferta pública en la República Argentina debe ser materia de autorización por parte de ésta Comisión."* La CNV se inclinaría más a tratar las criptomonedas como valores negociables y no como monedas, y posiblemente esa definición responda a ciertas características del Bitcoin sumado al sesgo con el que la CNV mira/analiza las transacciones influenciada por su función y ámbito de acción, que es el mercado de capitales y la necesidad de proteger a los inversores y proteger a ese tipo de consumidores.

Por su parte, a los efectos impositivos, la Ley 27.430 trataría a las monedas digitales de la misma forma que trata a los títulos de valores, y/o acciones, bonos, participaciones sociales y "demás valores", o como inversiones. Es decir, a los efectos impositivos parecería que la AFIP tampoco

[255] Barreira Delfino, supra nota 145.
[256] Chomczyk, supra 252.
[257] Chomczyk, supra 252.
[258] Chomczyk, supra 252.
[259] Barreira Delfino, supra nota 145.

considera que las criptomonedas son dinero o moneda (ni de curso legal ni extranjera ni de ningún tipo).

Precisamente, el inciso b) del artículo 90.4. de la LIG indica que las operaciones de enajenación de monedas digitales emitidas en moneda nacional con cláusula de ajuste o en moneda extranjera estarán gravadas al 15% cuando las obtengan personas humanas residentes en el país y pueda afirmarse que generan renta de fuente argentina. El mismo inciso refiere a las operaciones con acciones, títulos y demás valores, para los cuales tiene sentido la referencia a la moneda de emisión y su eventual cláusula de ajuste. Sin embargo, esta referencia respecto de las monedas digitales podría hacer inaplicable la norma puesto que las criptomonedas no se emiten en ninguna moneda, aunque comúnmente se comercialicen en dólares. Respecto a la fuente de la ganancia, las operaciones de compra y venta de criptomonedas, así como su dación en pago se registran en Blockchain que se reproduce en cada nodo de acceso, por lo que difícilmente pueda afirmarse que la operación ocurre en una jurisdicción en particular[260].

Posiblemente, la AFIP también pretenda tratarlo como un título de crédito o un bono para poder incluirlo en su órbita de recaudación, y ampliar la misma, aplicándole una categoría existente.

En el plano internacional, la *Financial Crimes Enforcement Network* (FinCEN) de Estados Unidos se ha expedido en reiteradas ocasiones respecto de las monedas virtuales. El mencionado organismo ha sostenido que los bitcoins no cumplen con los requisitos necesarios para encuadrar dentro de la definición de moneda (*currency*). Concretamente, la FinCEN requiere que, para ser considerado como una moneda, un objeto debe (i) ser designado como moneda de curso legal, (ii) circular y (iii) ser habitualmente utilizado y aceptado como un medio de intercambio en el país de emisión. **Asimismo, este organismo ha concluido que aquellas personas que realicen un intercambio habitual de monedas virtuales por monedas "reales" no se encontrarán sujetas a las regulaciones sobre cambio de moneda extranjera ya que los bitcoins no poseen curso legal en ningún país**[261].

Por su parte, en el año 2014 el Internal Revenue Service ("IRS") -autoridad fiscal norteamericana- emitió la Nota Nro. 2014-21 en la cual expone el tratamiento que corresponde otorgar a las operaciones con criptomonedas. El criterio del IRS parte de las opiniones de la *Securities & Exchange Commision* ("SEC") -autoridad de contralor de los mercados de capitales de ese país- quien previamente había afirmado que Bitcoin y otras criptomonedas son un *comodity*. **Sobre esa base, el criterio de la SEC indica que las criptomonedas son bienes y su venta o dación en pago puede implicar la realización de una ganancia sujeta al Impuesto a la Renta.** Sin embargo, la calificación de la ganancia como de capital o no dependerá de si las monedas se mantienen en cartera por un plazo mayor al año[262].

Finalmente, la Sala de lo Penal del Tribunal Supremo de España considera que B**itcoin** no es dinero, ni puede tener la consideración legal, a los efectos de responsabilidad civil, al considerar que se trata de un activo inmaterial de contraprestación o de intercambio en cualquier transacción

[260] Martina Caunedo, "Impuesto a las Ganancias en Operaciones de Criptomonedas", http://abogados.com.ar/el-impuesto-a-las-ganancias-en-las-operaciones-con-criptomonedas/22658, leído 11/12/18.
[261] Eraso Lomaquiz, supra 173, citando: Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, 2013.
[262] Martina Caunedo, supra 261.

bilateral en la que los contratantes lo acepten[263]. Los argumentos de dicha conclusión son los siguientes: a) se almacena en forma criptográfica, b) su valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta, es decir, **no existe por tanto un precio mundial o único del bitcoin.**

En resumen, Bitcoin no es dinero ni una moneda de curso legal para la ley argentina, y pareciera que tampoco lo sería para países como Estados Unidos y España.

b. No Es una Acción. Bitcoin no es una acción o cuota porque no representa el capital social de ninguna sociedad, su titularidad no confiere derechos políticos de ninguna naturaleza, no tiene dividendos, y no otorga a su tenedor un derecho contractual u obligación de recibir efectivo u otro activo financiero.

c. No es una Cosa Material. El Bitcoin no es una cosa material porque es un software, basado en un registro virtual. Contrariamente al hardware -elemento físico de los sistemas de tratamiento de la información-, el software es el elemento inmaterial[264], sin perjuicio del soporte físico en el que se almacena o ejecuta.

Por ello, el Bitcoin podría ser considerado un bien, esto es, una cosa mueble inmaterial amparada por el derecho de propiedad intelectual, en los términos del artículo 16 del Código Civil y Comercial de la Nación. Bitcoin no es una cosa tangible, porque no tiene representación física. Es más, como los bitcoins se registran en Blockchain, podría decirse que son una bien inmaterial registrable.

En sentido contrario, y en un artículo más que interesante, cuya lectura recomiendo, Andrés Chomczyk, manifestó que "[…] los bitcoins son objetos materiales en cuanto los mismos se encuentran representados de un modo que resulta tangible al ser humano. Si bien en este caso, la relación resulta más complicada de comprender que las cosas "tradicionales", la misma está presente; el bitcoin puede ser percibido por las personas en cuanto el mismo se concretiza en algo, ya sea una dirección privada asociada a cierta cantidad de bitcoins en una billetera o bien las líneas de código que representan el bloque de la cadena que acaba de ser minado. Si bien, se trata de un grado de materialidad que la mayoría de las personas no están acostumbrados a percibir no por ello debe ser menospreciado". Chomczyk también sostiene que "[…] hoy en día, se está igualando las categorías de documentos y firmas digitales a sus contrapartes físicas"; Chomczyk manifestó que, en el caso de los bitcoins, éste debe ser el mismo camino[265].

Sin perjuicio de considerar que el razonamiento de Chomczyk es lúcido, claro y muy bien articulado, considero que clasificar a Bitcoin como una cosa material sería casi ir contra la propia naturaleza del Bitcoin, porque sería casi como pretender asimilarlo a billetes del circulante físico que el propio Bitcoin pretende superar y reemplazar, y por cuya oposición se define.

En resumen, Bitcoin sería un bien inmaterial susceptible de apreciación pecuniaria asimilable a una moneda y no una cosa material, ni dinero.

---

[263] https://confilegal.com/20190705-el-tribunal-supremo-dice-que-el-bitcoin-no-es-dinero/, publicado el 5 de julio de 2019. Sentencia 998/2018 de 20 de junio de 2019. (último acceso 29/7/2019).

[264] 84.559/2003 – "A&CISA c/Buenos Aires Software S.R.L. y otro s/ordinario" – CNCOM – SALA C – 10/10/2008, citando la Revista de Derecho Privado y Comunitario, Tomo 2003-3, Editorial Rubinzal- Culzoni, pág. 111.

[265] *Andrés Chomczyk*, ¿Qué es un bitcoin? Un primer análisis sobre su situación legal en la Argentina, elDial DC1B46.

d. No es Título Valor. Bitcoin no son títulos valores porque no constituyen ni incorporan una obligación incondicionada e irrevocable de pago. Bitcoin no es una obligación de pago, es un medio de pago en sí mismo, un valor actual, y un medio para transferir dinero fiat en caso de que su titular desee permutarlo. La tenencia en sí misma no tiene como génesis ni objeto la obligación a un tercero a pagarle dinero al titular del bitcoin. Por otra parte, los bitcoins no devengan intereses.

Adicionalmente, a diferencia de los títulos valores, los bitcoins no tienen soporte cartular o físico, porque el registro de los mismos es virtual y a través de un software.

e. No es un Cheque Electrónico. Por razones similares, Bitcoin tampoco puede ser considerado un cheque electrónico, tanto más porque no tiene un banco girado de donde está la cuenta de donde salen los fondos para pagar la promesa incondicionada de pago, que contiene el mismo.

Si bien el cheque electrónico y los bitcoins circulan de manera puramente virtual, el bitcoin no contiene ninguna promesa de pago ni está asociado a ningún tipo de cuenta bancaria. Adicionalmente, el bitcoin no se transfiere por endoso, siempre se transmite electrónicamente por cesión de la clave privada del titular la cual se asocia a la clave pública del receptor del mismo. En tal entendimiento, si bien existe una cadena de transferencias registradas en Blockchain, similar a una cadena de endosos, esas transferencias no hacen que los transferentes anteriores tengan responsabilidad alguna por los incumplimientos del último cedente del bitcoin (no hay solidaridad). El bitcoin es seudónimo, y en los cheques electrónicos debe lucir el nombre del librador, como mínimo.

13. Bitcoin es una Moneda Virtual sin Curso Legal.

En fallo Miller v. Race dictado un tribunal inglés, resolvió que hay monedas que no son de curso legal, pero son tratadas como dinero, como efectivo, en el curso ordinario de sus negocios por vía del consentimiento general de la gente[266]. Eso les da el crédito y el curso del dinero, a todos los fines y propósitos[267], llegando en algunos casos a considerar como dinero a lo que fuere que el consentimiento común hubiere fijado o asignado como un signo denotando cierto valor[268]. Vale decir, moneda termina siendo lo que el común de la gente demanda o termine utilizando como un medio de cambio habitual.

De hecho, en el sobre fines del siglo 17 la jurisprudencia inglesa reconoció que las notas *goldsmiths* libradas por los bancos fueron siempre considerados por los comerciantes como dinero en efectivo[269], aún en el caso de que no tengan curso legal y los acreedores podían rechazar los pagos con ese tipo de documentos y reclamar el pago en dinero[270]. Era dinero creado por particulares, sin ningún tipo de esquema central, como Bitcoin.

[266] Miller v. Race, (1758), 1 Burr. 452 at 457, 97 E.R. 398 at 401 (K.B.)
[267] *Ibíd.*
[268] *Ibíd.*
[269] Tassell and Lee v. Lewis (1695), 1 Ld. Raym. 743 at 744, 91 E.R. 1397 at 1398 (K.B.).
[270] *Ibíd.*

Más aún, en Moss v. Hancock[271] el juzgado resolvió que **dinero es todo lo que pasa libremente de mano en mano dentro de una comunidad para la cancelación final de deudas, aceptada en forma igual sin discriminar el carácter o crédito de quien la ofrece en pago y sin la intención del receptor de consumir la misma.**

Nuestra constitución nacional, la única autoridad capaz de emitir moneda de curso legal es el Banco Central. Por ello, las criptomonedas como el Bitcoin no son consideradas monedas de curso legal en términos estrictos, ya que no son emitidas por la autoridad gubernamental idónea[272], por el contrario, uno de los rasgos característicos de las criptomonedas es su emisión descentralizada y la falta de respaldo de cualquier banco central.

Sin embargo, y siguiendo la línea de Moss y Miller (sentido amplio de lo que es moneda) y analizándolo con más detenimiento el artículo 30 de la Carta Orgánica (Ley 24.144 y modificatorias) que cité en el capítulo anterior advertimos que el mismo pareciera dejar abierta la posibilidad de que exista una moneda privada, que tenga validez y circulación dentro de la Argentina

Precisamente, el artículo 30 de la Carta Orgánica (Ley 24.144 y modificatorias) establece que: "*el Banco es el encargado exclusivo de la emisión de billetes y monedas de la Nación Argentina y ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, bancos u otras autoridades cualesquiera, podrán emitir billetes ni monedas metálicas ni otros instrumentos que fuesen susceptibles de circular como moneda*".

Como se puede apreciar, el artículo 30 de la Carta Orgánica en su primera parte pareciera referirse exclusivamente a la moneda de curso legal en la Argentina, y circunscribir su monopolio de emisión de monedas de la nación argentina solamente en relación a, y dentro de la órbita de las entidades públicas *("ningún órgano del gobierno nacional [...]"*, *"u otras autoridades cualesquiera"*), omitiendo hacer referencia a los privados que no fueren bancos, como podrían ser los mineros de Bitcoin. El artículo podría haber establecido expresamente que la prohibición de emisión de moneda también abarcaba a privados, diciendo: "[…] *ningún otro órgano del gobierno nacional, ni los gobiernos provinciales, ni las municipalidades, bancos u otras autoridades cualesquiera, ni ninguna persona y/o persona jurídica, podrán emitir billetes ni monedas*", pero no lo hizo.

Dicha interpretación del artículo 30 de la Carta Orgánica del Banco Central tiene su fundamento en el principio de legalidad establecido en el artículo 18 de la Constitución Nacional, el cual establece que lo que la ley no prohíbe se encuentra permitido: Si la prohibición de crear y emitir monedas de la Nación Argentina establecida en el artículo 30 de la Carta Orgánica del Banco Central no mencionó y/o incluyó expresamente a los particulares, y/o entidades privadas tampoco es dable que la misma sea extendida a estos por vía de la interpretación.

Ello así, en virtud de que tal interpretación resultaría contrario al principio de legalidad consagrado en el artículo 18 de la Constitución Nacional, el cual nace de la necesidad de que haya una norma que mande o prohíba una conducta, para que una persona pueda incurrir en falta

[271] [1899] 2QB 111, 116, citado en https://www.torys.com/insights/publications/2018/06/is-cryptocurrency-money-and-why-does-it-matter.
[272] Faliero, *supra* nota 11, p. 65, Ed. Ad-Hoc.

por haber obrado u omitido obrar en determinado sentido, y que además se establezcan las penas a aplicar[273].

Precisamente, el principio de legalidad (art. 18 de la Constitución Nacional) exige priorizar una exégesis restrictiva dentro del límite semántico del texto legal, en consonancia con el principio político criminal que caracteriza al derecho penal como la última ratio del ordenamiento jurídico[274], Es más, el principio de legalidad en materia sancionatoria exige que la conducta sancionada esté definida de forma explícita y precisa por las normas aplicables[275], cosa que no ocurre en este caso.

En una línea de pensamiento similar, la UIF emitió en el año 2014 la resolución 300, siguiendo las directivas del GAFI definió las criptomonedas como: *"la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En este sentido las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción."*

Este parecería ser el criterio adoptado por la Unidad de Información Financiera (la "UIF") mediante la Resolución Nº 300/2014. Mediante esta norma la UIF adoptó una definición para las llamadas 'monedas virtuales', siguiendo los criterios sentados por el Grupo de Acción Financiera Internacional[276]. En tal sentido, la resolución define a las 'monedas virtuales' como "*la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En este sentido las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción"*[277].

La definición nos da varios elementos para trabajar al respecto y que, a nuestro criterio, ayudan a reforzar nuestra postura sobre la calificación jurídica de Bitcoin en nuestro país. En primer lugar, consideramos acertado el tratamiento como una representación digital de valor; en este sentido, se reafirma la naturaleza de bien inmaterial susceptible de apreciación pecuniaria que sostuvimos antes. Ahora, la definición es insuficiente en cuanto al ámbito de uso; una simple mirada a diferentes fuentes disponibles en Internet basta para darse cuenta de la cantidad de negocios "reales" existentes que operan con bitcoins para refutar que los bitcoins solo sean usados en comercio digital, sin perjuicio que este haya sido uno de los ámbitos donde mayor proliferación han tenido[278].

[273] Expte. Nº 18593/2005 – "B.A. c/EN- M° Justicia resol 22/04 s/proceso de conocimiento" – CNACAF – SALA – III – 29/06/2012, elDial.com - AA78EA.
[274] Causa Nº 28.185/2010 - "EN – FIA c/ EN – Mº Justicia s/ proceso de conocimiento" – CNACAF – SALA II – 24/09/2014, elDial.com - AA8AF0, Publicado el 28/10/2014.
[275] Causa 27.550/12 - "Aceitera General Deheza S.A. (TF 27.079-A) C. DGA" - CNACAF – SALA III - 12/02/2013, elDial.com - AA7EAA.
[276] Eraso Lomaquiz, supra 173.
[277] *Ibíd.*
[278] *Ibíd.*

Respecto de las funciones, aquellas consignadas por la UIF nos parecen acertadas para determinar las utilidades de las monedas virtuales. En igual sentido puedo expedirme sobre la ausencia de curso legal. Sin embargo, y estimo necesario hacer la aclaración, el hecho que hoy en día ninguna moneda virtual tenga curso legal no impide que en el futuro ello pueda modificarse y algún Estado pueda darle tal característica. Lo mismo puede decirse con respecto a la emisión; que ningún Estado emita moneda virtual en este momento, no prohíbe de forma alguna que un Estado puede ingresar en la 'minería'. Recordamos que la definición únicamente resulta aplicable para la interpretación de la normativa dictada por la UIF[279].

Es decir, la UIF define a las criptomonedas como una moneda, pero sin curso legal en la Argentina, como ocurre con cualquier moneda extranjera.

En el plano internacional, ha habido entidades gubernamentales que han destacado Bitcoin puede considerarse moneda, pero no moneda de curso legal, ya que no son un medio obligatorio para cancelar deudas u obligaciones.

En tal entendimiento, cabe destacar que Bitcoin, **aunque no lo sea**, cumple funciones de la moneda de curso forzoso: es utilizado como medio de intercambio de bienes y servicios, como medida de cuenta y como depósito de valor (European Central Bank, 2012, p. 16)[280].

En ese mismo sentido la FATF (Financial Action Task Force), un organismo internacional que lucha por la prevención del terrorismo y el blanqueo de capitales, también le asigna al Bitcoin las funciones de una moneda de curso forzoso, aclarando que no tiene curso legal al definirla como *"una representación digital de un valor que puede ser comerciado por Internet con las funciones de medio de pago, unidad de medida y guarda de valor, pero sin tener valor legal en ninguna jurisdicción"*[281].

La sentencia dictada por el Tribunal Europeo en la causa "**Hedqvist**" (2015), los miembros del tribunal entendieron que no corresponde gravar las operaciones de cambio de criptomonedas por cuanto la compraventa de "**divisas, billetes de banco y monedas que sean medios legales de pago**" está exenta del impuesto. Es así que el Tribunal Europeo consideró que las criptomonedas deben ser tratadas como divisas, billetes o monedas. Este encuadramiento ha tenido un fuerte impacto en lo que respecta a la aplicación del Impuesto al Valor Agregado por parte de los países miembros de la Unión Europea, con algunas excepciones tales como España y Francia, quienes continúan gravando las operaciones de intercambio y dación en pago de criptomonedas[282].

Más aún, recientemente el estado de Wyoming, EEUU, se encuentra analizando un proyecto de ley[283], que en su punto a) (iv) establece que, si los activos digitales son utilizados como medio de cambio, reserva de valor, o unidad de cuenta, y que no tenga curso legal en EEUU, entonces serán considerados como monedas virtuales. Posteriormente, en la sección 34-29-102, el proyecto de ley clasifica a las monedas virtuales como propiedad intelectual que será considerada dinero.

[279] *Ibíd.*
[280] ECB/2012/16, https://www.ecb.europa.eu/ecb/legal/pdf/l_24520120911en00030012.pdf
[281] Boar, *supra* nota 27, p. 133.
[282] Martina Caunedo, supra 261.
[283] Digital Assets Existing Law, STATE OF WYOMING, SENATE FILE NO. SF0125.

El proyecto de ley mencionado tiene la finalidad de que los bancos del estado de Wyoming, EEUU puedan tener y custodiar activos digitales, como criptomonedas[284]. Asimila a las criptomonedas al dinero, según función que el activo digital tenga.

De hecho, Alemania fue el primer gobierno en avalar Bitcoin como moneda privada, a través del su Ministerio de Finanzas quien reconoció a dicha criptomoneda como una unidad de cuenta [285] Si bien dicho reconocimiento no le confiere a Bitcoin el nivel de legitimidad que se le asigna a una moneda respaldada por un país, y permite su uso para transacciones privadas[286] . La única limitación que tiene en el mercado comercial, donde una empresa debe obtener un permiso de la Autoridad Federal de Supervisión Financiera (BaFin) alemana para usar Bitcoin como medio de pago en una transacción comercial[287].

De este modo, Bitcoin parece ser considerado como una moneda comunitaria, que es un subproducto del sistema de permute que permite a algunas comunidades simplificar el proceso de permute estableciendo su propia versión del dinero[288].

Un tribunal en EEUU definió a los Bitcoin como una moneda virtual, libre de soberanos (virtual, sovereign-free currency)[289]. Ello, por cuanto los bitcoins cumplirían, en más o en menos, con las tres condiciones económicas que debe tener una moneda, a saber: (a) Constituyen un medio de cambio; (b) permiten el almacenamiento de valor; y (c) funcionan como unidad de medida[290]. Está opinión no es compartida por muchos economistas.

Si la devaluación fuese determinante para definir que califica como moneda y que no lo es, entonces el Peso argentino, o el Bolivar venezolano, dos monedas que en los últimos años han sufrido devaluaciones considerables y pronunciadas, tampoco podrían ser consideradas moneda. Por lo tanto, ese no parecería ser un argumento válido para decir que Bitcoin no es moneda.

Más aún, si se tiene en cuenta que existe un número limitado de Bitcoin, todo lo cual impide que una emisión masiva del mismo y que pierda valor.

Si bien, Bitcoin se ha usado mayormente para inversión o especulación, no es su único uso ni su única función. De hecho, hay cajeros automáticos de Bitcoin y es aceptado como medio de pago en algunos comercios. El Bitcoin se puede cambiar por dinero físico o por otras criptomonedas o utilizarse como medio para transferir dinero.

---

[284] *Ibíd.*

[285] Charles Arthur, Bitcoin Now 'Unit of Account' in Germany, GUARDIAN (Aug. 19, 2013, 6:01 PM), http://www.theguardian.com/technology/2013/aug/19/bitcoin-unit-ofaccount-germany.

[286] *Ibíd.*

[287] Trading in Bitcoins, BaFIN (June 17, 2014), http://www.bafin.de/ SharedDocs/Veroeffentlichungen/EN/Jahresbericht/2013/jb_2013_II_9_2_trading_in_ bitcoins.html.

[288] Vivian Doumpa, Community Currencies and Bartering Models Take Root in Greek Cities, POP-UP CITY (May 14, 2013), http://popupcity.net/community-currenciesand-bartering-models-take-root-in- greek-cities.

[289] 857 F.3D 334 (6TH CIR. 2017), 16-6291, UNITED STATES V. BROWN.

[290] Se ha dicho que los bitcoins tienen tres cualidades útiles a estos efectos: Son "difícil de ganar, limitadas en su emisión, y fácil de verificar", cf. https://en.wikipedia.org/wiki/Bitcoin (accedido el 01.10.15). Esta afirmación no está exenta de conflicto. Si bien para algunos el bitcoin tiene el potencial de cumplir estos roles más eficientemente que las monedas tradicionales, algunos críticos postulan que el sistema no sería más que un "esquema Ponzi", cf. Plassaras, Nicholas,"Regulating digital currencies: Bringing bitcoin within the reach of the IMF", 7 de abril de 2013, disponible enhttp://ssrn.com/abstract=2248419 (accedido el 01.10.15). Sobre el particular, según el Banco Central Europeo (supra nota 3), los bancos centrales del Eurosistema no reconocen que los bitcoins cumplan con las condiciones económicas del dinero, ya que según sostienen— no tienen el suficiente nivel de aceptación entre el público en general, y ostentan una muy alta volatilidad; aunque reconocen que no pueda descartarse que se estabilice y sea más aceptado en el futuro, o que surja otra moneda virtual que la supere en estos aspectos.

Como se puede ver, existen argumentos de sobra para considerar a Bitcoin una moneda, y, de hecho, como vimos, algunos países de la Unión Europea (Alemania) y entidades gubernamentales de Estados Unidos ya lo han hecho.

14. Bitcoin es Asimilable a una Moneda Extrajera en la Argentina.

Habiendo determinado que Bitcoin es moneda y que no es moneda de curso legal en la Argentina, ahora corresponde determina cual debería ser el tratamiento legal que debería tener el Bitcoin.

Como dijimos anteriormente, en la Argentina, la emisión del dinero y las cuestiones atinentes a su circulación son facultad exclusiva y excluyente del Congreso de la Nación (art. 75, inc. 6 y 11 de la Constitución Nacional), quien delegó en el Banco Central de la República Argentina su emisión y control.

En la actualidad, el *peso* tiene *curso forzoso,* ya que es una moneda irrecusable como medio de pago e *inconvertible,* en razón de la derogación (por la ley 25.561, que se mantiene vigente) del sistema de convertibilidad establecida en el año 1991 por la ley 23.928[291].

En cuanto a la moneda extranjera, cabe decir que no es dinero en nuestro país y carece, por ende, de curso legal. Ello quiere decir que la única moneda que tiene aptitud para ser impuesta como medio de pago es el peso; el único medio de pago con poder cancelatorio es el peso[292].

Nuestro ordenamiento no da una definición expresa sobre este concepto jurídico de moneda extranjera. En la Carta Orgánica del BCRA nos encontramos con que este puede mantener una parte de sus activos externos en moneda extranjera, junto con otros elementos. Dadas las disposiciones previamente vistas, podríamos considerar como moneda extranjera a aquellos instrumentos emitidos por las autoridades públicas autorizadas a tales efectos en cada Estado extranjero[293], o cualquier otro instrumento que fuere considerado moneda (aunque no fuere de curso legal) en un país determinado, como vimos en el caso de Alemania, Inlgaterra y en algunos estados de EEUU.

Es decir, en general, nos encontramos con una concepción tradicionalista de las monedas, en donde solo se admiten como tales a aquellas que son emitidas por una autoridad central[294], **o, mejor dicho, aquellas que tuvieren curso legal en algún país, y por eso, tendemos a excluir del concepto de moneda a todas aquellas que no tuvieren curso legal en algún país determinado**.

En consecuencia, de la interpretación podría concluirse que no sería de aplicación la Ley 18.924 y todo el régimen relativo a las operaciones cambiarias. Es decir, no sería necesario constituirse como, por ejemplo, una casa de cambio para negociar de forma habitual bitcoins ni tampoco sería necesario solicitar autorización a la AFIP para comprar bitcoins a fin de demostrar que se cuenta con capacidad contributiva para ello[295].

---

[291] Lorenzetti, supra 100, Tomo V, p. 123, Rubinzal Culzoni Editores.
[292] *Ibíd.*
[293] http://elbitcoin.org/situacion-legal-de-bitcoin-en-argentina./ de *Andrés Chomczyk, 10/10/13. (último acceso 31/07/2019)*
[294] *Ibíd.*
[295] *Ibíd.*

Por el contrario, si el Bitcoin fuere considerado moneda (no necesariamente moneda de curso legal), se le debería aplicar la ley 18.294 y todo el régimen operativo relativo a las operaciones cambiarias, porque el artículo 1[296] de dicha ley refiere a "monedas" en sentido lato, sin aclarar si son de curso legal o no.

Sin embargo, cabe recordar el fallo de la justicia británica Miller v. Race[297], el fallo USA v. Brown, la normativa de Wyoming, EEUU, junto con otros antecedentes legales citados en el capítulo anterior, en los cuales las autoridades gubernamentales y jueces decidieron considerar como moneda a todo lo que fuere que el consentimiento común hubiere fijado o asignado como un signo denotando cierto valor, como ocurre con el Bitcoin.

Precisamente, a veces la legitimación de la moneda no solo proviene desde el punto de vista de la legislación monetaria, como la que cite anteriormente, sino también de la voluntad de las partes.

De esa manera, al igual que en Miller v. Race[298] y USA v. Brown, en la República Argentina nada impide que la exigibilidad de la moneda extranjera sea impuesta por una obligación, porque las partes utilizan la divisa extranjera como medio de pago y le dan una función dineraria a una cosa que (según la ley) no es dinero. **La legitimación proviene de la obligación y no de la legislación monetaria**[299], como ocurre con el Bitcoin

Al igual que ocurre con el Bitcoin, la obligación que tiene por objeto una prestación en moneda extranjera presenta el problema del pago. Conforme con el régimen del CCyCN, la regla es que el deudor tiene la opción de liberarse dando el equivalente en moneda de curso legal[300]. Al tener el Bitcoin un valor de mercado público y en dólares, el deudor podría pagar el valor del mismo entregando los Pesos equivalentes al valor del Bitcoin. Esta regla tiene las siguientes excepciones: a) Que las partes hayan pactado expresamente el pago en moneda extranjera y la renuncia a la opción (arts. 958, 959, en materia de contratos; 1121, inc. a, en los contratos de consumo); y b) que esté previsto expresamente otra solución (ej.: contratos bancarios)[301].

Es decir, la moneda extranjera no tiene carácter dinerario como lo preveía la Ley 23.928, sino que es una cosa no dineraria: de allí que el Código Civil y Comercial de la Nación en su artículo 765 establece que si la obligación se pacta en tal denominación se considera como de dar cantidades de cosas[302], que con el Bitcoin serían cosas inmateriales registrables.

Rectamente interpretada la norma 765 del Código Civil y Comercial de la Nación, que coordina con el art. 766, no impide *"que la moneda extranjera sea impuesta por una obligación, porque las partes utilizan la moneda extranjera como medio de pago y le dan una función dineraria a una cosa que no es dinero*[303]*. En la especie de modalidad de contratación, que la doctrina*

[296] Ninguna persona podrá dedicarse al comercio de compra y venta de monedas y billetes extranjeros, oro amonedado y cheques de viajero, giros, transferencias u operaciones análogas en divisas extranjeras, sin la previa autorización del Banco Central de la República Argentina para actuar con Casa de Cambio, Agencias de Cambio u Oficina de Cambio.
[297] Miller v. Race, (1758), 1 Burr. 452 at 457, 97 E.R. 398 at 401 (K.B.)
[298] *Ibíd.*
[299] Lorenzetti, supra 100, Tomo V, p. 123.
[300] Lorenzetti, supra 100, Tomo V, p. 125.
[301] *Ibíd.*
[302] Expediente N° 30694/2013/CA2 – "Gago Daniel Amilcar c/ Gargiulo, Gustavo Fabian s/Ejecutivo" – CNCOM – 10/03/2016
[303] *Ibíd.*

denomina como de "uso esencial de la moneda extranjera", el cumplimiento in natura resulta ser esencial pues, si se diera otra cosa se desnaturalizaría la obligación[304].

En ese sentido, el Bitcoin se asemejaría a una moneda extranjera para el derecho argentino, y, por lo tanto, debería recibir el mismo tratamiento legal.

Más aún, la afirmación de que el Bitcoin no estaría asociado a un estado extranjero no me parece exacto, ni que sea suficiente para excluirlo del concepto de moneda extranjera, toda vez que los productores (mineros) del Bitcoin se encuentran radicados en distintos países del mundo, y sus servidores y/o proveedores de internet se encuentran en esos países, siendo ello, suficiente punto de contacto para asignarle al Bitcoin una nacionalidad, o varias nacionalidades extranjeras, o simplemente para descartar la nacionalidad Argentina (lo cual la transformaría por descarte en extranjera).

Por todo ello, considero que a los fines del derecho argentino y en lo relativo a cuestiones cambiarias, exigibilidad de pago de obligaciones, y cuestiones impositivas Bitcoin puede ser asimilado a una moneda extranjera, y consecuentemente, deberían aplicar las normativas cambiarias a su compra y venta, como ocurre con el Dólar, lo que implicaría un tratamiento impositivo distinto al que le asignó la AFIP, y todo lo atinente a moneda de pago sería regulado por los artículos 765 y 766 del Código Civil y Comercial de la Nación.

[304] *Ibíd.*

"Beware of geeks bearing formulas."
Warren Buffet.

"Fortunes are bound to be made as cryptocurrencies become more widespread media of exchange."
Diego Zuluaga[305]

15. Conclusión.

A veces las discusiones sobre la naturaleza jurídica pueden estar guiadas por fines pragmático y no filosóficos. La discusión sobre la naturaleza jurídica de Bitcoin no es una discusión meramente semántica, todo lo contrario, es una discusión sobre el futuro, y cuál va a ser actitud que vamos a tomar como sociedad ante este nuevo fenómeno.

Por ello, y por todos los argumentos expresados a lo largo de este trabajo, es que creo que Bitcoin es asimilable a una moneda extranjera, y que: a) su adquisición y circulación debe analizarse a la luz de la normativa cambiaria del BCRA, b) la exigibilidad de obligaciones contraídas en Bitcoin debe resolverse de acuerdo a lo normado por los artículos 765 y 766 del Código Civil y Comercial de la Nación, y c) la AFIP debería darle el mismo tratamiento impositivo que a las monedas extranjeras.

Obiter dictum, sería interesante que podamos ampliar esta discusión y avanzar en un encuadre oficial para poder acompañar los cambios tecnológicos y que los mismos no nos tomen por sorpresa, o, lo que sería peor, la naturaleza jurídica del Bitcoin termine siendo determinada por la coyuntura, como podría ser la necesidad del estado Argentino de recaudar mayores impuestos para sus arcas, o eventualmente, en razón de alguna restricción cambiaria, o la mayor injerencia que pudiere tener la CNV o alguna agencia o ministerio estatal, en algún momento dado. Adoptar una posición oficial sobre la naturaleza del Bitcoin puede servir para trazar una hoja de ruta para eventualmente, determinar la naturaleza jurídica de otras criptomonedas, y tecnologías que se desarrollen en el futuro.

Soy consciente de que resulta difícil clasificar a las criptomonedas (en este caso el Bitcoin) en una naturaleza jurídica específica. Las criptomonedas evolucionan constantemente y tienen características distintas que hacen que puedan ser un título de valor, una acción, un *comodity* o una moneda. El error es pensarlo como algo estático, mirar lo que es hoy y no lo que puede ser[306].

Posiblemente, y a modo de autocrítica a este trabajo, mi error sea tratar de pensar el Bitcoin como una moneda tradicional, y tratar de encasillarlo en una definición de moneda extranjera. Por ahí, el enfoque correcto pasaría por generar una nueva clasificación, para un activo intangible digital que representa una moneda comunitaria y apátrida, propia de un mundo globalizado y cuyas fronteras parecerían ser cada vez más difusas gracias a Internet.

---

[305] The Price of Not Knowing the Value of BitcoinM, *By Diego Zuluaga* articulo publicado en https://www.cato.org/publications/commentary/price-not-knowing-value-bitcoin

[306] *"ICOs, these things can transform. They may start their life as a security from a capital-raising perspective but then at some point (…) turn into a commodity." CFTC Commissioner Brian Quintenz.*

No descarto que Bitcoin merezca la creación de una nueva clasificación, y una nueva mirada. Analizarlo con bajo la lupa de los esquemas tradicionales, puede que solamente nos sirva para llegar a conclusiones que no atiendan a la naturaleza y finalidad del Bitcoin, y que deban ser modificadas en el corto plazo.

No hay que perder de vista que Bitcoin no nació de una autoridad gubernamental, o de una entidad financiera específica. Bitcoin nació de un conjunto de usuarios de la Internet que querían crear un sistema financiero nuevo, disruptivo del sistema tradicional y anárquico, y, por lo tanto, parecería que no puede (¿quiere?) ser encasillado una categoría legal preexistente, todo lo cual resulta un argumento adicional para crear una nueva clasificación de moneda.

En ese sentido, es importante tener en cuenta que el uso de monedas espurias o seudo monedas no emitidas por el gobierno nacional se encuentra permitido por la ley, y ha ocurrido en la argentina y en el mundo con anterioridad. La fuerza vinculante y la exigibilidad de esas operaciones no proviene de la ley, proviene de la voluntad de las partes.

Lo novedoso es que Bitcoin es una moneda virtual (sin soporte físico), y que su transferencia y tenencias se encuentran registradas en un registro virtual mundial, dotado de seguridad por la criptografía. Es decir, lo novedoso es la estructura 100% virtual, su calidad de moneda mundial y la posibilidad de no tener que pagar costos de intermediación para su transferencia.

Por el momento, y dado el poco uso que tiene para transacciones cotidianas de comercio, la función principal de Bitcoin constituye la de ser un sistema para transmitir dinero (al menos hoy), y nada más.

Sin embargo, creo que Bitcoin llegó para quedarse y va a tener un rol protagónico en la economía del futuro, pero para ello no va a poder subsistir como fue originalmente pensado, porque es anárquico y tiene que tener un orden, someterse a normativa de transparencia y estar regulado, más aún si pretende interactuar en el mercado o tener un mercado transparente.

Algo de eso estamos viendo ahora con "LIBRA", la moneda virtual de Facebook, la cual parecería ser una versión evolucionada del Bitcoin, porque tiene muchos de los rasgos de Bitcoin (por ej. Utilizar Blockchain, ser una moneda virtual, privada, y en un futuro descentralizada o diseminada) y otras características destinadas a superar dudas, cuestiones, y puntos oscuros de Bitcoin, como ser un valor subyacente estable atado a ciertos activos (dinero y títulos) de países y empresas de reconocida solvencia (similar a un *stable coin*), y tener una fundación compuesta por empresas privadas multinacionales de primera línea (CALIBRA), sometidas a regulaciones gubernamentales (no sería anónima), destinada a crear la LIBRA en un primero momento y administrarla.

Por su parte, los bancos empezaron a aceptarlo con matices, Francia con su PACTE Law permite a los bancos abrir cuentas para criptomonedas sujeto a regulación, y a entidades financieras tomar mayores inversiones en criptomonedas, en sentido similar, JP Morgan manifestó que pretende tener su propia criptomoneda.

Todo lo mencionado nos demuestra que las criptomonedas llegaron para quedarse, y van a tener un rol protagónico en el sistema financiero de un futuro no tan lejano.